10 Mar 2021

Hardware Management Console (HMC)

Contents

Hardware Management Console (HMC)

The Hardware Management Console (HMC) is a feature on IBM Z® (Z) and IBM LinuxONE (LinuxONE) that provides an interface to control and monitor the status of the console or the Support Element (SE).

Learn how the HMC applies many of its functions as described in the introductory material and explains how the tasks are used for the console and selected systems.

Introduction

Introduction

You can expand this section for an overview of the Hardware Management Console (HMC).

What's new in version 2.15.0

This information reflects the licensed internal code for the Hardware Management Console Application, Version 2.15.0. You can tell if your Hardware Management Console has this version installed from the title bar on the Hardware Management Console workplace window or by pointing your mouse over **HMC Version** in the top of the work pane window. New enhancements to the version code are described in this section.

There might be other changes to the licensed internal code that are not described here. For more information, see the PDF files available on Resource Link® (http://www.ibm.com/servers/resourcelink).

The following information summarizes the new and changed features for Version 2.15.0.

Supported character sets

The console only supports Single-Byte Character Sets (SBCS) for data entry.

Audit support for remote syslog

The HMC 2.15.0 release provides a new option for audit support. Previously, Hardware Management Console (HMC) users might use the **Audit and Log Management** task or **Customize Scheduled Operations** task to offload xml and html formatted audit logs, security logs, and console events.

Now, you are able to consolidate a wider variety of logs, such as: security logs, audit logs, console events, hardware messages, BCPii logs, and Web Services API logs. In addition, it offloads directly to centralized servers that use established and industry-common syslog protocols, which can include any syslog enabled log consolidation tool. This eliminates the need for your own automation and goes directly to the consolidation point. The intent of the central logging instance is to collect all relevant messages across the enterprise immediately when they are created by each system to avoid a later removal of these messages and deleted traces of security incidents. (For more information about allowing a syslog enabled endpoint to forward syslog messages to your server, see the documentation that is provided for your syslog enabled log consolidation tool.)

A new HMC task, **Manage Syslog Servers**, is available to configure to forward selected consolidated syslog entries from the HMC or managed Support Elements (SE) to customer-controlled syslog servers. Currently, for the HMCs own remote syslogging configuration, you must configure each additional HMC uniquely or use the **Configure Data Replication** task. For each SEs remote syslogging configuration, any previous SE configurations are shown with the previous customization settings and can be altered if required.

This task allows you to add a syslog server, specifying a host name or IP address and a port where the server is listening for syslog messages. For each server, you can also specify which consoles should send syslog messages to it, and what types of messages each console should send.

Forwarding connectivity from the HMC and SE work differently although they are configured similarly. For each configured remote syslog server on the HMC, the HMC must have connectivity directly to the server. For each configured remote syslog server on the SE, there must be a managing HMC that has connectivity to that server. In this case, if there is such an HMC, the SE discovers it automatically and proxies the forwarding connectivity through it. If an SE cannot locate an HMC with connectivity or if an HMC does not have connectivity for its own logs, then a rolling buffer of logs is kept for forwarding when connectivity is restored. This exploits buffering capability that is built into remote syslog.

Manage System Time support for Precision Time Protocol

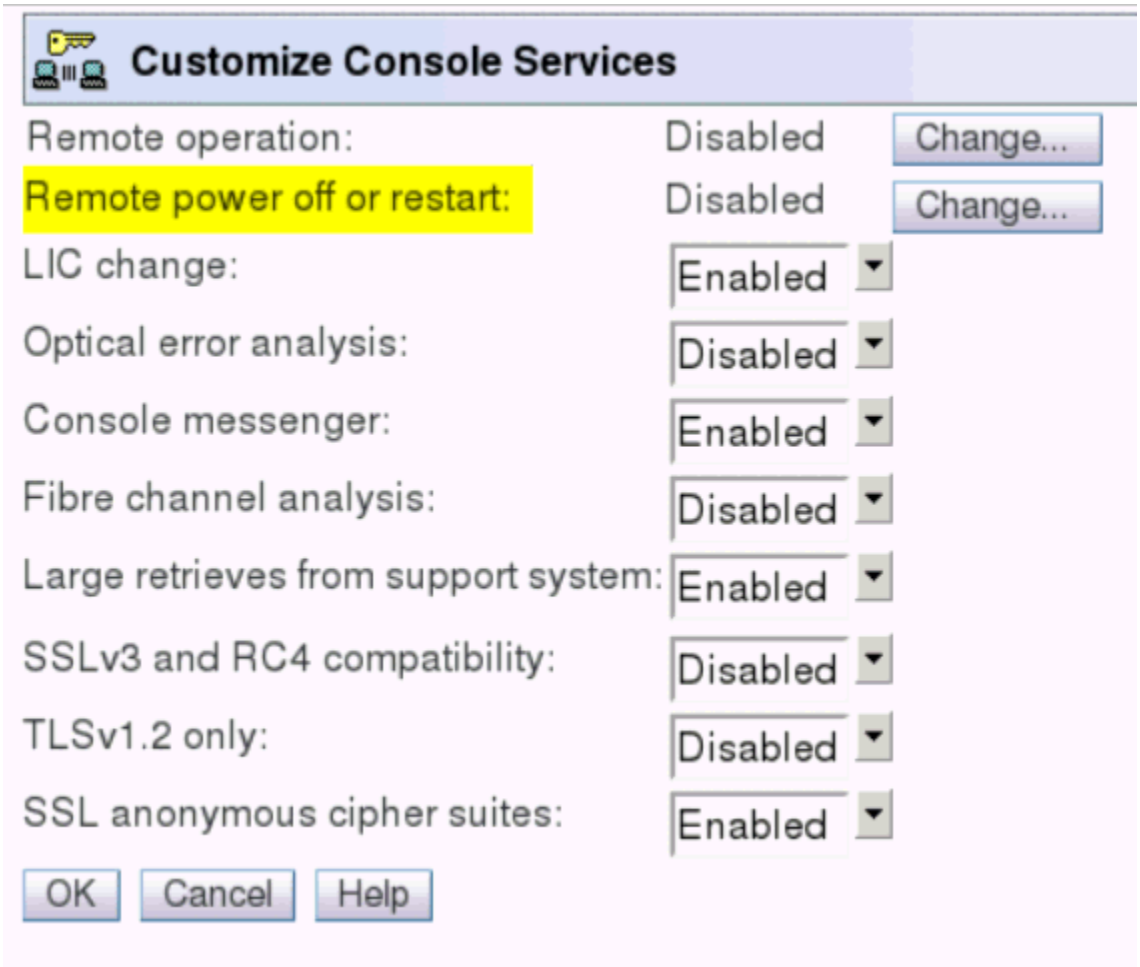
In addition to the Network Time Protocol (NTP), Precision Time Protocol (PTP) can now be used as an External Time Source (ETS) for Server Time Protocol (STP) for an Coordinated Timing Network (CTN). The advantage to using PTP is that its connections are significantly more accurate than NTP connections.

The HMC **Manage System Time** task has been updated to support PTP. For example, the **Configure External Time Source** action now allows you to specify **PTP** or **PTP with PPS (Pulse Per Second)** as the External Time source. **NTP** and **NTP with PPS (Pulse Per Second)** continue to be supported as External Time Sources as well.

Shutdown or Restart task has been renamed

The **Shutdown or Restart** task has been renamed to **Power Off or Restart**.

Additionally, the **Remote restart** option that is available from the **Customize Console Services** task has been renamed to **Remote power off or restart**. This option is available for the SYSPROG and SERVICE user IDs or any user ID that is assigned system programmer or service roles.



This task includes a section which describes the steps to enable remote power off at the Hardware Management Console (HMC), Support Element, or Hardware Management Appliance (HMA). Note that

each console setup must be done locally and before remote power off is required. Only users that have been assigned system programmer or service roles can perform these steps for remote users.

Secure Execution feature

A new feature called Secure Execution for Linux is enabled when the feature code is installed. An LPAR opts-in to use the Secure Execution support. Secure Execution protects data confidentiality and integrity when running multiple Linux virtual machines in a logical partition. The **Image Details** task displays the status is On/Off of Secure Execution for a specific logical partition. The **System Details** task indicates whether Secure Execution for Linux feature is enabled or disabled on the system and whether the required Global key or Host key is installed.

Adapter Details task

A new **Adapter Details** task replaces the **PCHID Details** task to include Detail information about a selected adapter. All references to PCHIDs and channels are now called adapters to stay consistent with industry standard.

Manage Key Manager Connections task

The **Manage Key Manager Connections** task enables you to establish connections between one or more endpoint-security-enabled systems (CPCs) and key managers in order to secure the connections between the systems and Fibre Channel storage devices.

Using **Manage Key Manager Connections**, system administrators can:

- Connect systems to key managers to enable the system Fibre Channel endpoint security capabilities.
- Manage security certificates to effectively secure connections.
- Establish system policies (the default security behavior for connections and certificate expiration) to meet datacenter security needs.

Manage Key Manager Connections also includes a number of sub-tasks ("Actions") for tasks such as connecting systems to key managers, editing certificates, exporting and importing certificates, and so on. Here are some examples:

- An administrator can use the **Connect system to key managers** action to choose systems, connect them to key managers, and then export the systems' certificates to the specified key managers. (The systems will obtain the shared keys that are used to secure the endpoints of the Fibre Channel connections from the key managers.)
- The **Edit certificates** action allows a system administrator to change the expiration date of an expiring self-signed certificate.
- Using the **Create certificate signing request** action, an administrator can replace a system's self-signed certificate with a CA-signed certificate. The administrator first uses the **Create certificate signing request** action to submit the self-signed certificate to a certificate authority (CA) for signing. Then, after the CA-signed certificate is generated, the administrator uses the **Import signed certificate** action to replace the system certificate.

The graphical format of the **Manage Key Manager Connections** user interface offers a clear view of the topology. The interface is simple to understand and intuitive. Textual guidance, placed directly on the panels, provides easy access to additional information.

The **Topology view** enables you to get information about your systems, key managers, and the connections between them, quickly and easily. Rectangular icons represent the systems and key managers, and lines that extend between them represent their connections. Hovering or clicking on one of these elements produces a pop-up window that displays additional details.

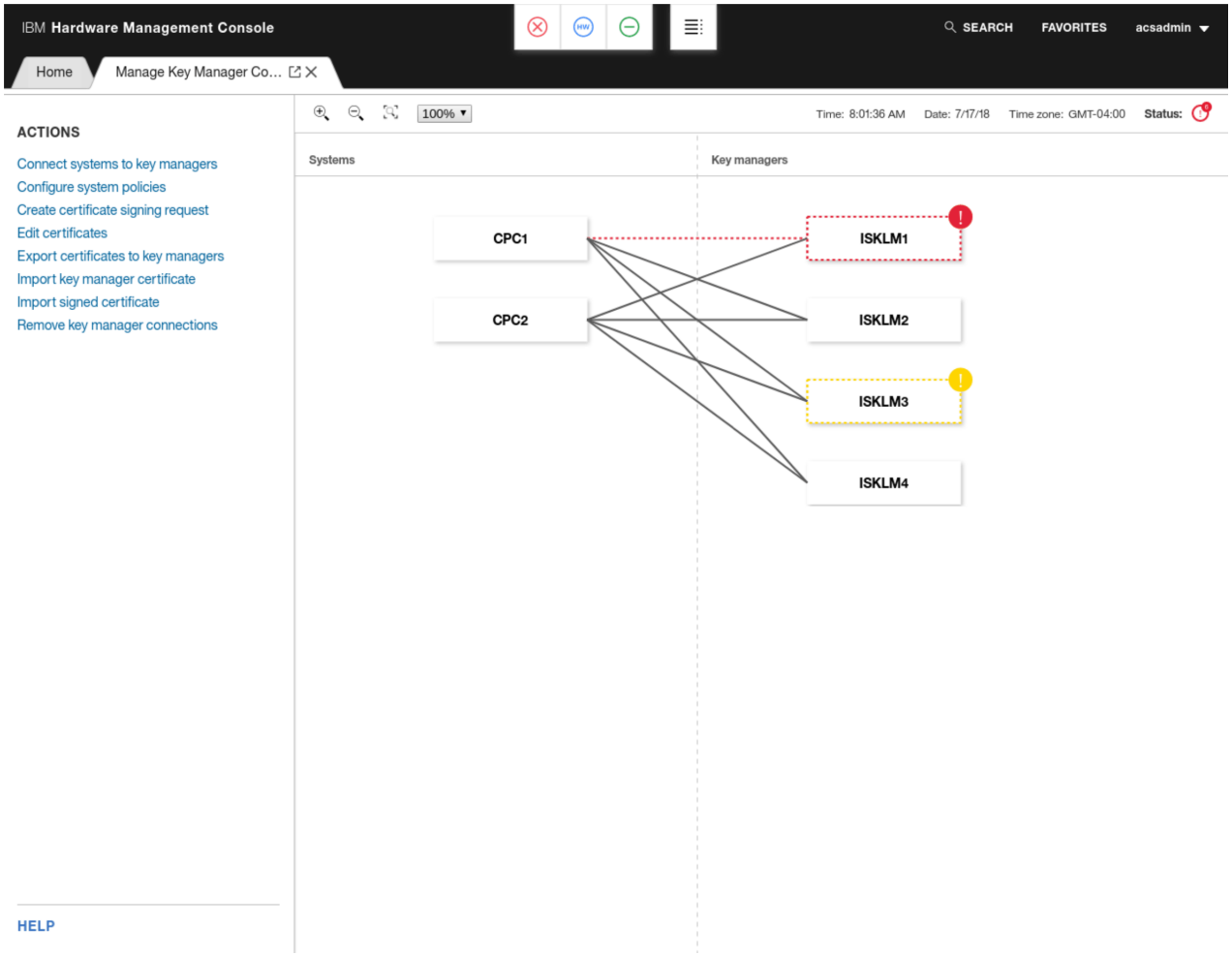


Figure 1. The Manage Key Manager Connections main window (Topology view)

The **Manage Key Manager Connections** interface displays status in a visual format. With a glance at the main window's toolbar, a managed system's general status is easily discernible. Systems with errors or warnings are visually highlighted in the topology's graphical display, and more specific details are available with a single click. The **Topology toolbar** also includes a **Status** icon, which is displayed in green, red or yellow to indicate the overall state of the topology at any given time.

The **Manage Key Manager Connections** task is available on the HMC.

New Manage Key Manager Connections action: View adapter security

The **View adapter security** action of the **Manage Key Manager Connections** task, provides users with a single place from which they can view the security capabilities of the Fibre Channel endpoints of their FICON Express adapters, instead of needing to check each PCHID individually.

For each FICON Express adapter, users can view the following details:

- PCHID that is assigned to the adapter
- Type of adapter
- Status of the adapter
- Security capabilities of the adapter (whether the hardware is capable of having authenticated and/or encrypted connections)

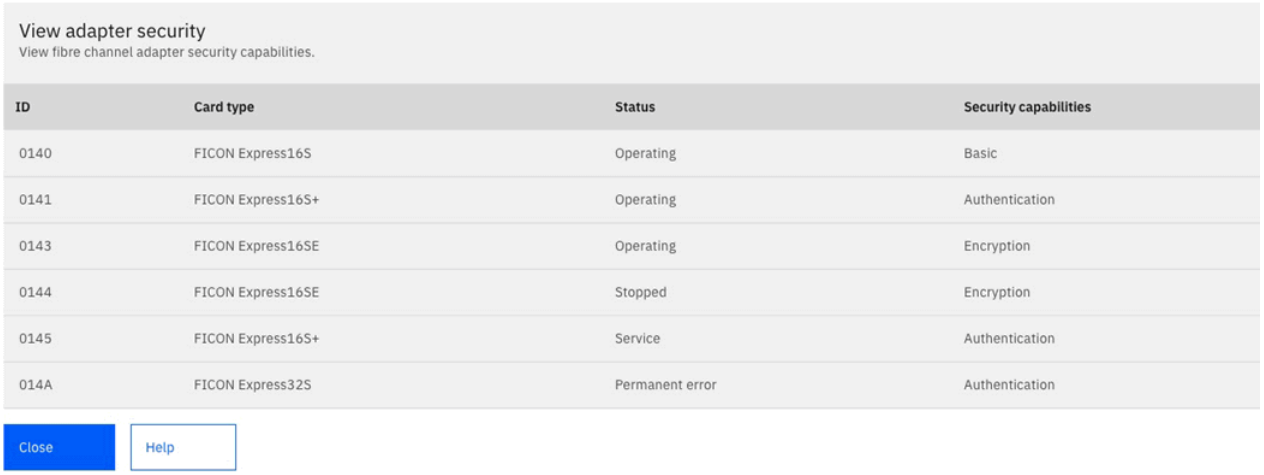


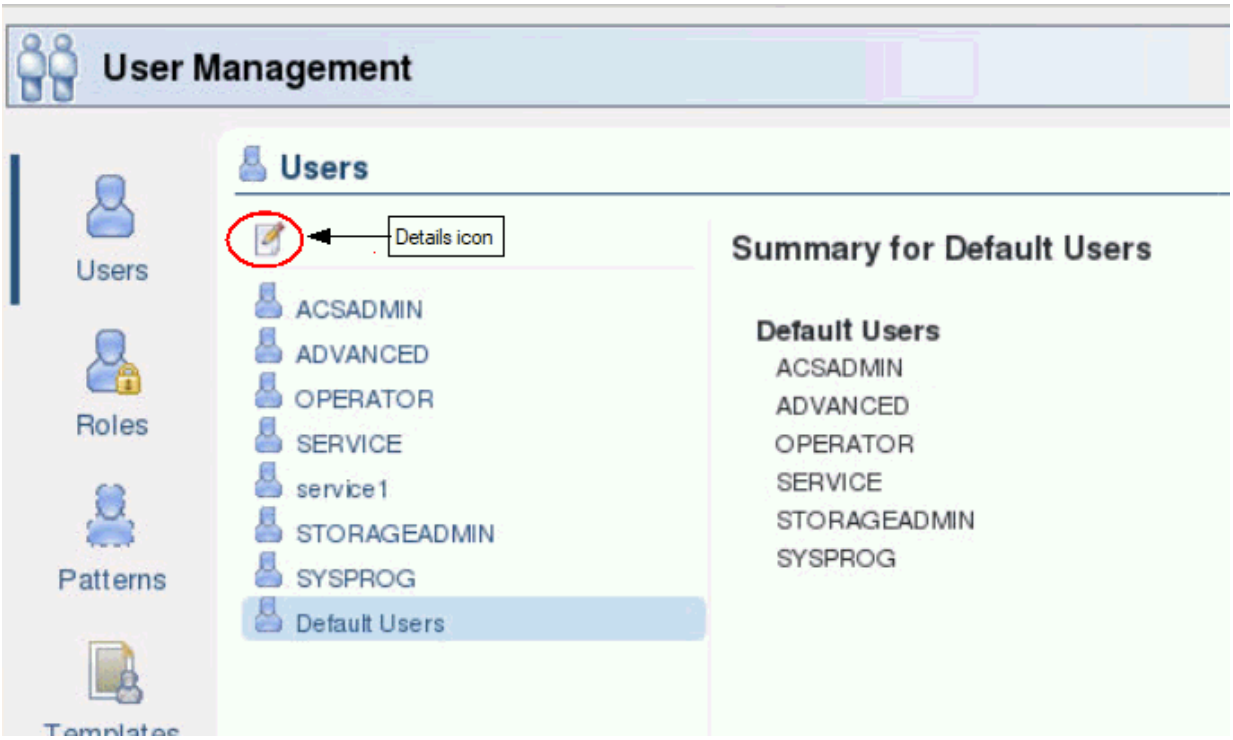
Figure 2. The Manage Key Manager Connections View adapter security action

User Management task updates required by the state of California, US

The *California Senate Bill No. 327* (as of 1 January 2020) requires all default users to change their passwords at the time of initial logon. The **User Management** task adds additional function to accomplish this function. The only users that can access the additional function are SERVICE or a user that is assigned a role with Manage Users task permission.

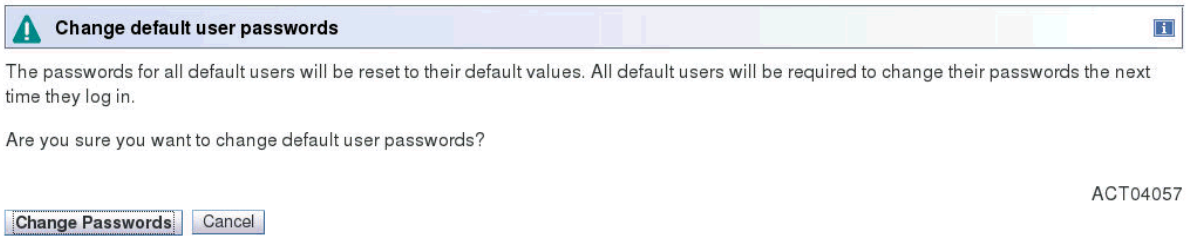
To force the default user IDs to change their passwords on their next login:

1. Log on with SERVICE or a user that is assigned a role with permission to manage users.
2. Go to the **User Management** task. You can see from the **Users** navigation, a new option is displayed, **Default Users**.
3. If you are logged in as a user that is assigned a role with Manage Users task permission, select **Default Users**, which displays the list of default users the password change affects.

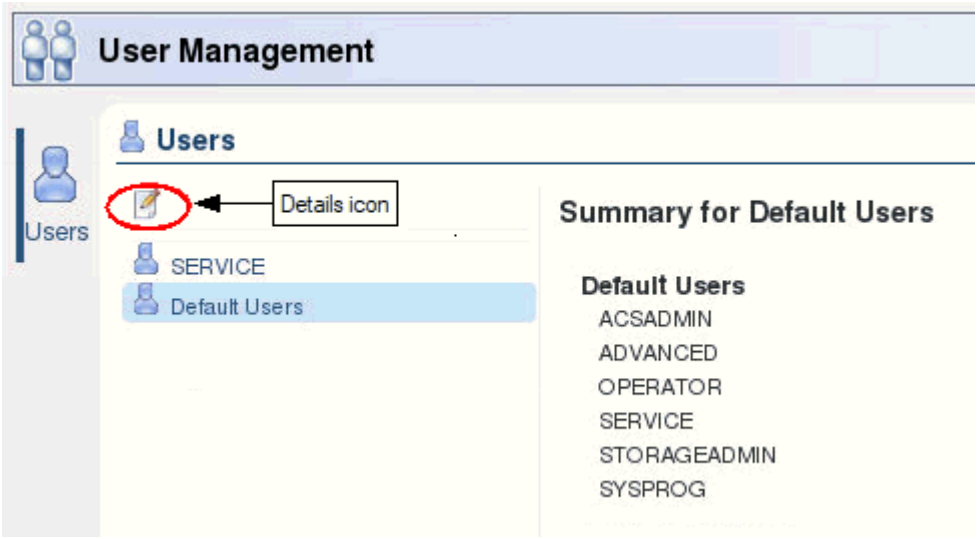


   a. Click the **Details** icon. The Change default user passwords window is displayed.

b. Click **Change Passwords** to reset all system defined user passwords back to their defaults and force those user IDs to change their password the next time they logon.

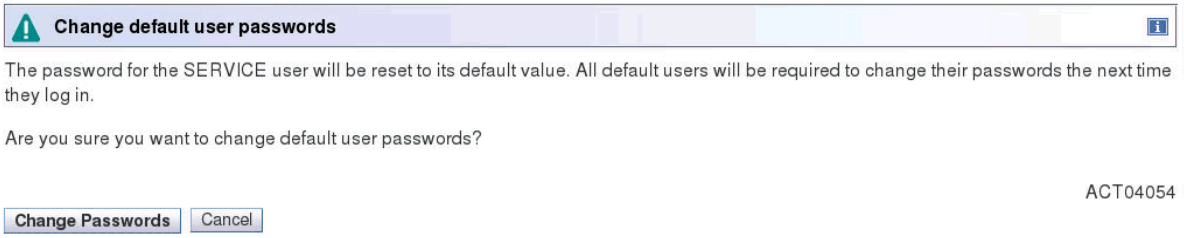


4. If you are logged in as SERVICE, select **Default Users**, displays the list of default users the action affects.

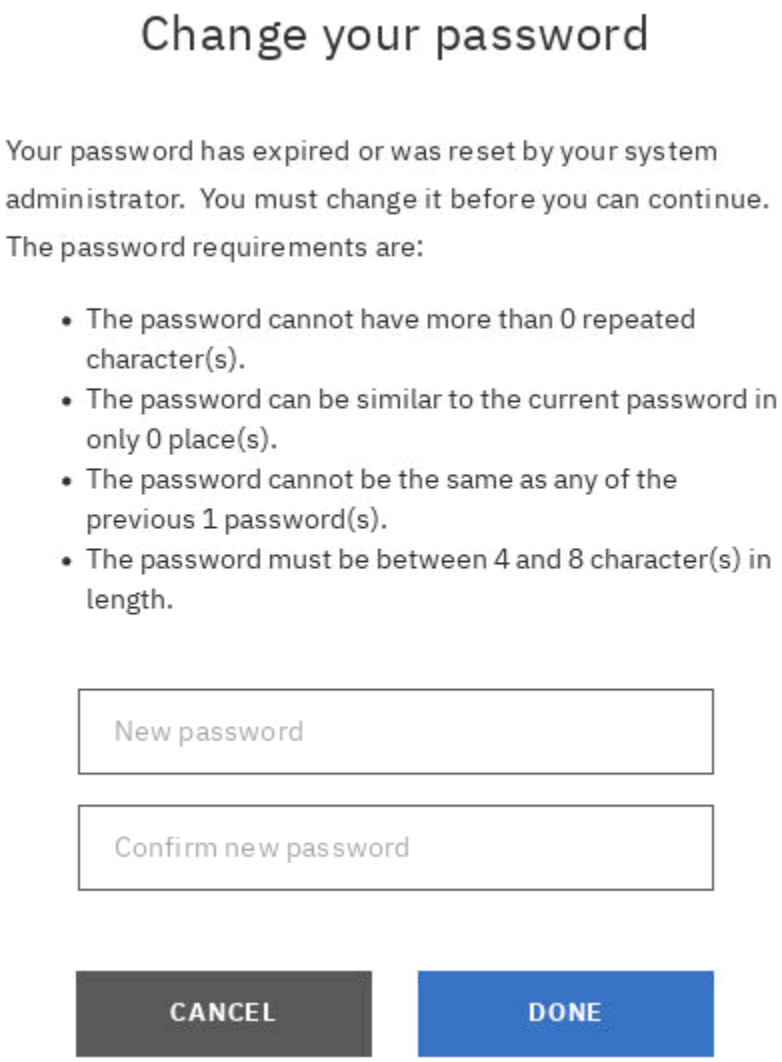


a. Click the **Details** icon. The Change default user passwords window is displayed.

b. Click **Change Passwords** to reset only the SERVICE user's password back to its default and force all the other system defined default users to change their passwords the next time they logon.



As a result of the previous change passwords function, the following prompt is displayed after the default user ID initially logs on.



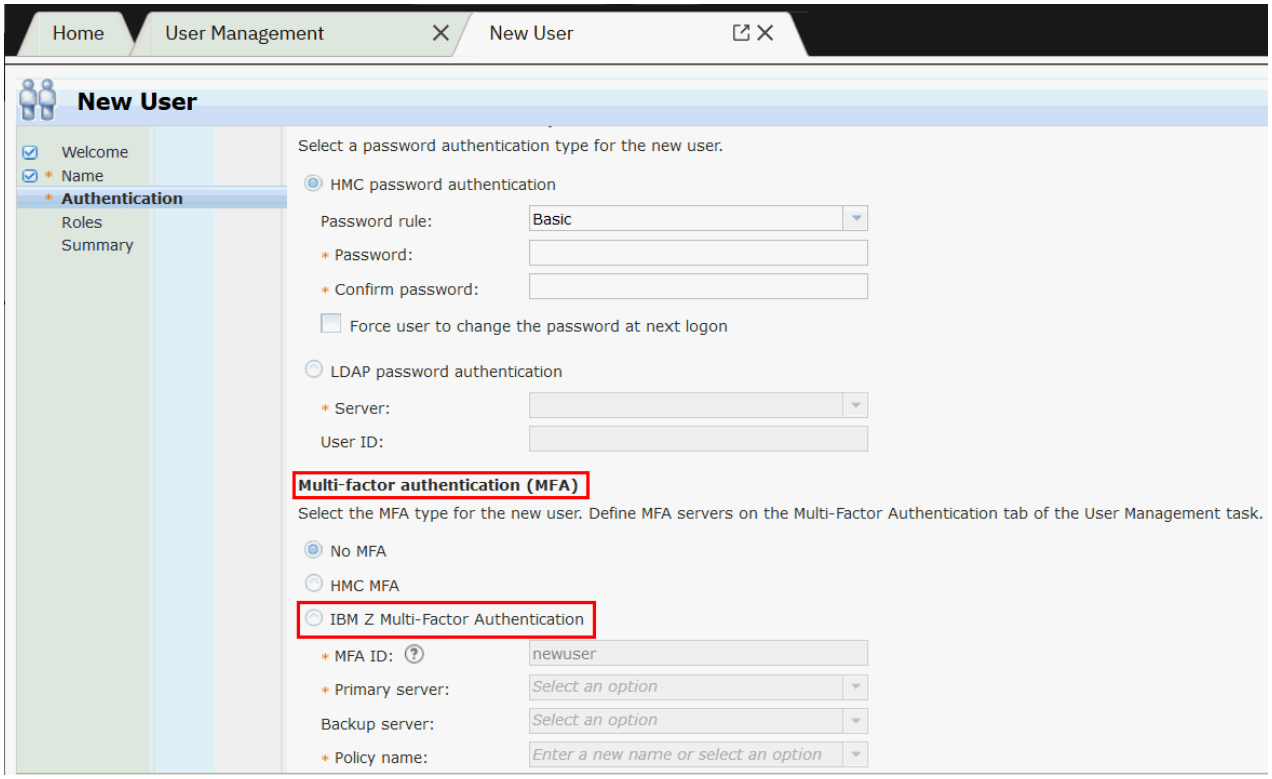
IBM Z Multi-Factor Authentication application

The Hardware Management Console (HMC) Version 2.15.0 now provides a centralized multi-factor authentication that uses a server connection to the IBM Z® Multi-Factor Authentication application. RSA SecurID authentication that is provided through the new centralized server is now supported when logging onto the HMC.

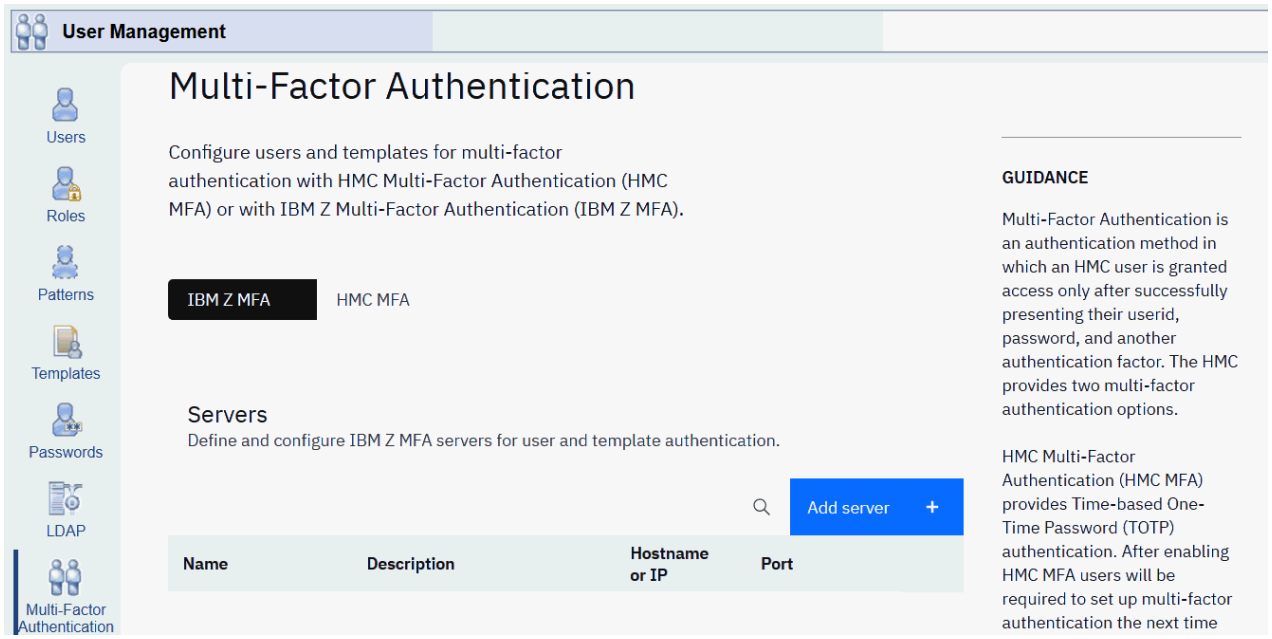
The **User Management** task is updated to incorporate the changes that are required to apply this new enhancement.

The access administrator can assign IBM Z Multi-Factor Authentication to users and templates.

When the access administrator adds new users and templates or when they are updating existing users and templates, a new Multi-factor authentication (MFA) section of the task displays the new **IBM Z Multi-Factor Authentication** option. See the following figure for an example of the task window.



The Multi-Factor Authentication navigation icon of the **User Management** task is updated to include a new user interface and also provides the new **IBM Z MFA** option. This option allows the access administrator to specify the IBM Z MFA server and manage the users and templates for IBM Z Multi-Factor Authentication. See the following figure for an example of the task window.



Dynamic Partition Manager (DPM) updates

The following DPM releases are available with HMC/SE Version 2.15.0.

DPM Release 4.3 (R4.3)

DPM R4.3 provides system or storage administrators with a simplified interface to configure access to FCP tape libraries in the storage area network (SAN). Administrators use the **Configure Storage** task to create a *tape link*, which defines the attributes of a connection that one or more partitions can use

to access one FCP tape library in the SAN. When you submit your request to create a tape link, DPM automatically generates the host world wide port names (WWPNs) and zoning instructions that storage administrators use to fulfill the tape link request.

The following summary describes the updates to various tasks for FCP tape support.

Configure Storage
Administrators can manage FCP tape storage through the following subtasks.

Connect to Storage and Storage Cards
At least one system adapter must be configured as FCP before you can request a tape link. You can configure the protocol of installed storage cards through **Connect to Storage** and **Storage Cards**.

Request Tape Link or Create Tape Link
Depending on the authorization of your user ID, select either **REQUEST TAPE LINK** or **CREATE TAPE LINK** to define the attributes of a tape link. Creating a tape link can be as easy as providing a name for the tape link, and checking the default value for the number of connecting paths. In this case, the storage administrator selects the tape library and the system adapters to use for the tape link.

If you want additional control over the resources for a tape link, you can use this task to select specific partitions to which DPM attaches your tape link; set the maximum number of partitions that share the tape link; select a tape library; and select the system adapters. You also can use this task to manage FCP tape libraries in the DPM environment.

Storage Overview and Tape Link details
Storage Overview provides a table that lists each tape link and its attributes. By selecting a table entry, you can open the **Tape Link details** page to view more information about a specific tape link. Through this page, you also can modify or delete the tape link; resend the zoning instructions for tape link that is incomplete or in a pending state; and view a history of the actions that users have taken for this tape link.

Manage Adapters
Through the Connections section of **Adapter Details**, you can view the Tape Links table, which lists any tape links that are associated with the target adapter.

New Partition task (basic and advanced modes) and Partition Details task
You can use the **Storage** section of these partition management tasks to select one or more tape links to attach to, or detach from, a specific partition. If any attached tape links are using adapters that become degraded, you can view those tape links in the **Status** section of the **Partition Details** task.

DPM Release 4.2 (R4.2)
DPM R4.2 delivers support for IBM® Adapter for NVMe1.1 features, which are available on IBM LinuxONE (LinuxONE) systems only. Non-Volatile Memory Express (NVMe) storage adapters use the PCI Express (PCIe) protocol to provide high-speed storage within a system. Each NVMe adapter consists of two pieces of hardware: an IBM-supplied carrier card installed in a system I/O drawer, and the solid state drive (SSD) that customers purchase. IBM service representatives install the NVMe SSDs in the carrier cards after the system is delivered to the customer site.

The following tasks are updated to support the use of NVMe storage adapters. Note that the HMC Web Services API provide equivalent NVMe support.

Configure Storage task
Administrators can manage NVMe storage through the following subtasks.

Connect to Storage and Storage Cards
Through these subtasks, you can view NVMe adapters in the visual display of system frames and I/O drawers, and view specific details about each adapter; for example, you can tell whether the carrier card has an SSD installed. You cannot use these tasks to reconfigure NVMe storage adapters; reconfiguration requires properly removing the carrier card and its SSD from the drawer and reinstalling them in a different physical location, as instructed by a service representative.

Request Storage
Through this task, you can create a storage group containing one or more available NVMe SSDs that are installed in carrier cards. You can define these SSDs as either boot or data volumes.

Storage Overview and Storage Group details
Through **Storage Overview**, you can view a list of all NVMe storage groups, and select one storage group to modify or delete. Through Storage Group details, you can view details about a specific storage group, such as a list of SSDs that are defined as volumes for the group; the partition, if any, that is using the group; and the history of changes related to the group. You can also modify or delete the NVMe storage group.

Dump task
Through this task, you can select an SSD volume in an NVMe storage group as the boot volume for a dump program. The NVMe storage group must be attached to the partition for which you want to request the dump. NVMe namespace management is not supported, so you can boot programs only from namespace ID=1.

Manage Adapters task
Through the **Adapters** tab and **Adapter Details**, you can view information about NVMe storage adapters only when NVMe SSDs are installed in carrier cards in the system I/O drawers. Adapter details for the installed SSDs include current operating status, allocation, card type, location, capacity, and manufacturer information.

New Partition task (basic and advanced modes) and Partition Details task
Through these partition management tasks, you can attach one or more NVMe storage groups, and select an SSD volume in an attached NVMe storage group as the boot volume for an operating system or hypervisor. Note that only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared.

- NVMe namespace management is not supported, so you can boot programs only from namespace ID=1.
- Unlike FCP and FICON storage groups, which sometimes require you to enter Linux commands to make those storage groups available to the operating system, NVMe storage groups are automatically detected by the operating system.

In addition to the NVMe support, DPM R4.2 also delivers performance improvements that significantly reduce the time required to discover logical units (LUNs) during storage management task processing.

DPM Release 4.1 (R4.1)
DPM R4.1 delivers the following enhancements to HMC tasks.

System Details task
The **General** section of the **System Details** task displays a new field, Secure Execution, which indicates whether the IBM Secure Execution for Linux® feature is enabled on this system. This indicator is also available on the **Systems** tab on the HMC **Systems Management** view, but the Secure Execution column on that tab is not displayed in the predefined default table view. To display the Secure Execution column, select the **Manage Views** icon in the work pane table toolbar to customize the table view.

For this feature to be enabled, a global key and host key must be installed on the Support Element. IBM either installs the required global and host key bundles on a new machine before delivery, or electronically sends them to your company for the service representative to import to an already installed system.

Partition Details task
The **General** section of the **Partition Details** task displays a new field, Secure Execution, which indicates whether the operating system that runs on a partition is configured for secure execution, which isolates and protects any guests that run on a hypervisor by restricting host access to guest workloads and data.

Configure Storage task
For FICON connections, the Connect Adapter Ports dialog has enhanced search functions to help you locate the adapter ports that connect a system to a switch or storage subsystem.

DPM Release 4.0 (R4.0)

DPM R4.0 delivers the following enhancements to HMC tasks.

Configure Storage task

- An exportable cabling plan that you can use to physically connect the system to storage area network (SAN) hardware. The cabling details file is in Comma Separated Values (CSV) format that you can view in a spreadsheet application.
- Updated displays and improved navigation aids for viewing the storage adapter cards that are installed in a multi-frame system.
- User interface enhancements that simplify tasks related to creating and managing storage groups:
  - Resolving volume device number conflicts between base and alias volumes in a FICON storage group.
  - Viewing and copying volume details that administrators need to configure a partition's operating system to access storage.
  - Selecting one or more ranges of logical control units (LCUs) when configuring system connections to storage devices.
- The **Resend Request** option on the Storage Group details page. This option creates a modification request that identifies actions for a storage administrator to perform to change the fulfillment state of the storage group to Complete. This option is enabled only when the storage administrator has not yet completed all storage configuration tasks that are required to fulfill the most recent creation or modification request for the storage group.

New Partition and Partition Details tasks

- A new option, **Permit ECC key import functions**, that enables applications running on the partition to generate and manage Elliptic Curve Cryptography (ECC) protected keys through the CP Assist for Cryptographic Functions (CPACF) feature. This option is available only on systems that support the ECC algorithm. When creating a new partition, users can specify this option only through the advanced mode of the **New Partition** task.
- A new option, **Secure Boot**, through which administrators can request DPM to verify the software signature of the Linux operating system that is to run in a partition. If the software signature does not match the signature from the distributor, the boot process ends. This option is enabled only when:
  - The partition has a partition type of Linux.
  - The system that hosts the partition supports the Secure Boot for Linux function.
  - The administrator selects a boot volume in an FCP storage group as the boot source for the Linux operating system.

HMC Mobile Settings task updates

Depending on the HMC/SE version that you are using, you can limit HMC Mobile app users to read-only access through either the User actions section or the Read-only access option of the **HMC Mobile Settings** task. The User actions section, which replaces the Read-only access option starting with HMC/SE Version 2.15.0, not only provides a read-only setting but also includes settings for more granular access control. Through the User actions section, you can use the **Actions are enabled** setting to enable or disable user actions.

- When user actions are disabled, the app is in read-only mode.
- When user actions are enabled, the display includes a table of actions that users can perform through the app and, for each action, a list of users or templates with authorization to perform the action. You can edit actions in this list to grant permission to all users and templates, to no users or templates, or to only specific users and templates. Note that these users and templates also must have the equivalent task permissions assigned through the HMC **User Management** task.

For more information about the User actions section, see the online help for the **HMC Mobile Settings** task.

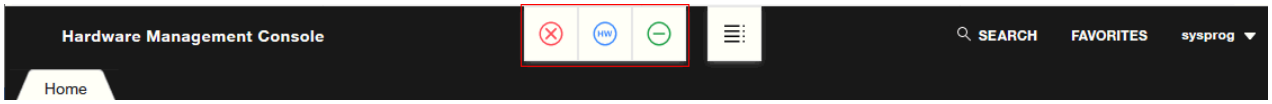
Tree style user interface updates

The following tree style user interface changes are part of Version 2.15.0:

Window Size

New for Version 2.15.0, the window size is saved for each user. When you remotely log on to the HMC and resize your window, that window size is remembered the next time you log on remotely.

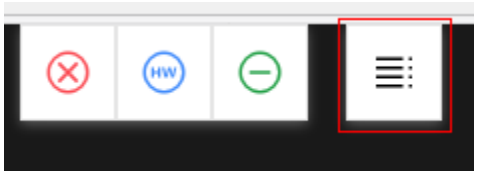
Status Bar



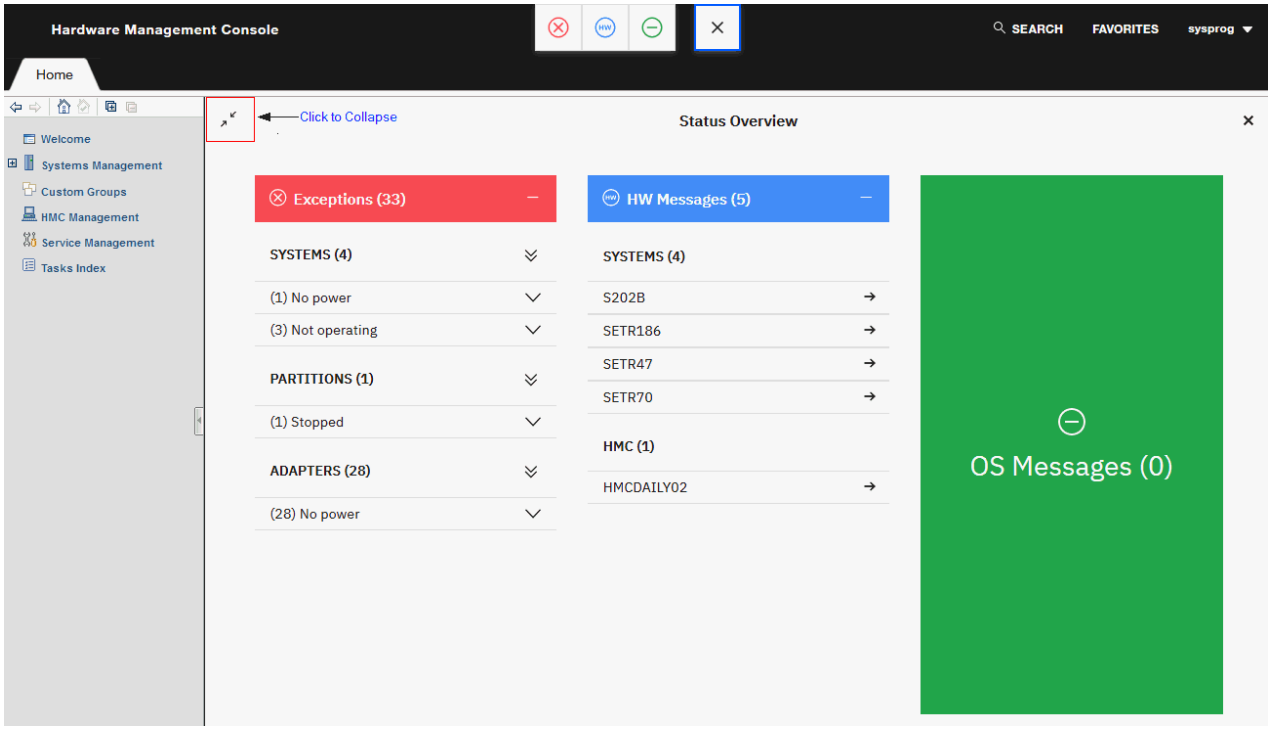
The status bar moved from the Home tab to the masthead. The three icons represent exceptions, hardware messages, and operating system messages. When no objects exist with a given status icon, then the icons are green to convey a positive status. When objects exist with a status icon other than green they are represented by red for exceptions, blue for hardware messages, and purple for operating system messages.

You can select each of the buttons to see all the objects with unacceptable status, hardware messages, or operating system messages.

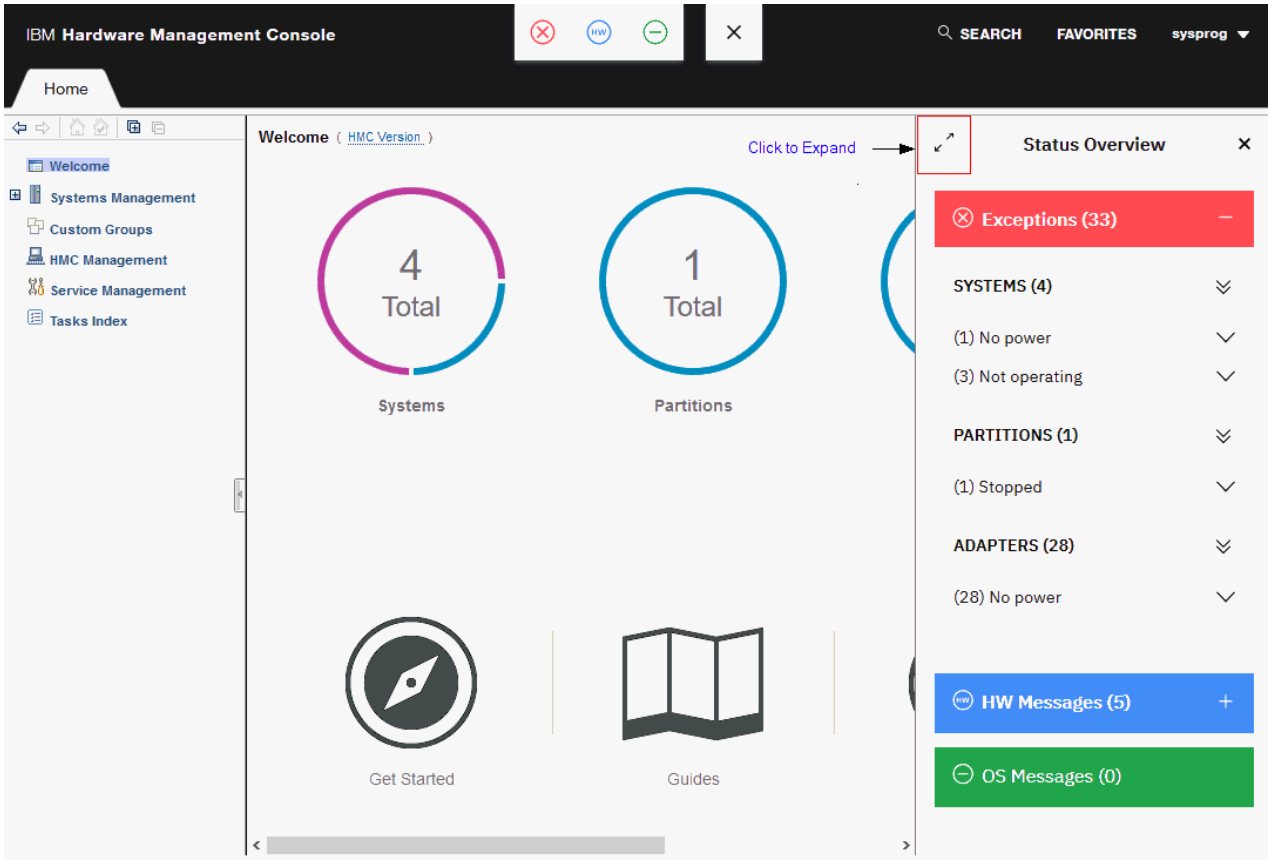
Status Overview



The status overview now shows detailed status information that can be expanded into the Home tab work area.

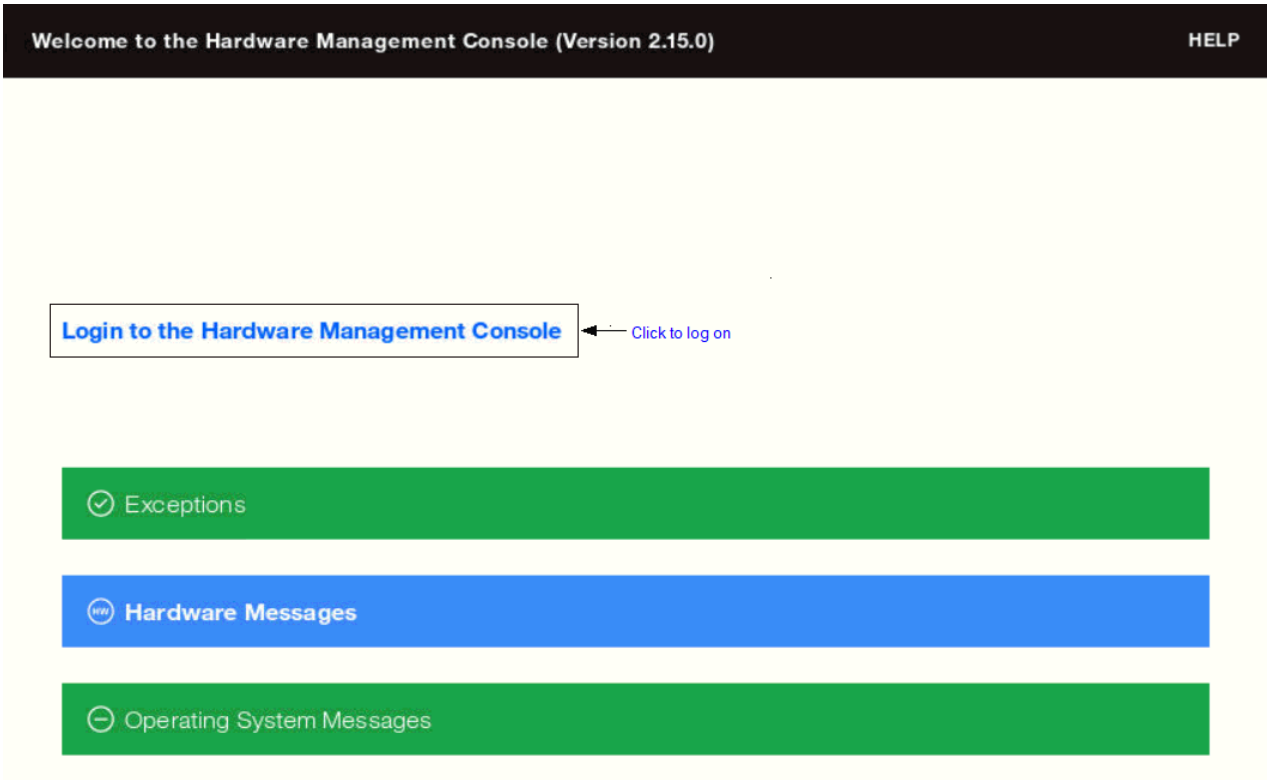


The status overview can also be viewed off to the side of the window that uses the new Collapse or Expand Status Overview icon.



Welcome page

The Welcome page displays the new status bars, a new location for the HELP button, and you can log on to the Hardware Management Console by selecting **Login to the Hardware Management Console**.

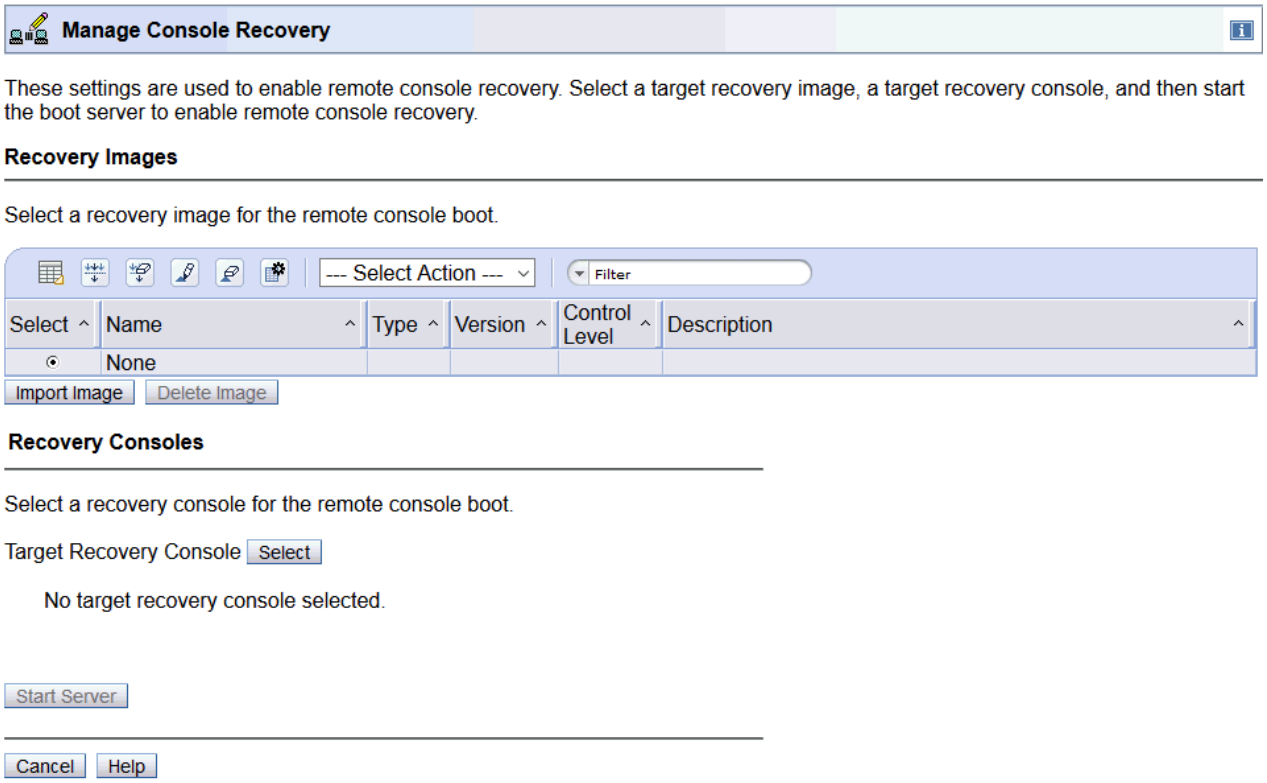


DVD drives no longer available

The DVD drives for the IBM z15™ (z15™) hardware are no longer available on the Hardware Management Console.

Note: If you upgrade your IBM z13® (z13®) or IBM z14® (z14) Hardware Management Console hardware to run Version 2.15.0 code, tasks that use the DVD will generally continue to recognize the DVD media.

With the removal of DVD drives, some tasks (such as: initial installs, EC upgrades, and hard disk restore operations) are going to load images by using a USB flash memory drive or through a network. A new task, **Manage Console Recovery**, allows the Hardware Management Console (HMC) to load a selected target system with a selected recovery code load image remotely over the network. Following is an example of the **Manage Console Recovery** task window.



IBM Z Hardware Management Appliance

The IBM Z Hardware Management Appliance provides Hardware Management Console (HMC) and Support Element (SE) functions within the CPC frame, eliminating the need for separate HMCs outside of the frame.

The IBM Z Hardware Management Appliance feature code #0100 can be ordered to provide the HMC and SE functions to be contained within redundant physical servers inside the CPC frame. When you order the IBM Z Hardware Management Appliance feature, it logically provides Primary and Alternate Support Elements and two peer Hardware Management Consoles on two physical servers in the CPC frame. This eliminates the need for having to manage a separate physical server or servers for one or more HMCs outside of the frame. For the user interface experience, you must use remote browsing controls from your own workstation into the HMC within the IBM Z Hardware Management Appliance.

If you have multiple systems, you will not need to order the Hardware Management Appliance feature for all systems. The recommendation is that you need to consider having the IBM Z Hardware Management Appliance features on one or two CPCs, but the rest of the CPCs do not need to include Hardware Appliance features. (Those CPCs would have redundant Support Elements.)

The IBM Z Hardware Management Appliance feature is optional. Physical HMCs (both mini-tower and rack mounted) are still available features you can use.

Virtual Support Element Management task

A new task is being introduced for version 2.15.0, the **Virtual Support Element Management** task. This new task allows you to open and manage the graphical console of the Support Element on the IBM Z Hardware Management Appliance. The task allows you to view, start and stop, and install a virtual Support Element on the IBM Z Hardware Management Appliance.

Server requirements for supporting FTP, SFTP, or FTPS

Use the following guidelines for a Linux operating system server supporting FTP, SFTP, or FTPS.

FTP (File Transfer Protocol)

- Recommend vsftpd 2.0 or higher
- Server must support passive FTP data transfers
- Client firewalls may need to be configured to allow the passive data connection to occur

SFTP (SSH File Transfer Protocol)

- Recommend openssh 4.4 or higher
- Only user name and password client authentication is currently supported
- Client key authentication is not supported

FTPS (FTP Secure)

- Recommend vsftpd 2.0 or higher
- Server must support passive FTP data transfers
- Server must support explicit FTPS connections
- Client firewalls may need to be configured to allow the passive data connection to occur

Logging on to the Support Element with a Hardware Management Console user name

When you log on to the Support Element with a Hardware Management Console user name, the following scenarios are considered.

- When the Support Element does not have a user name that matches the Hardware Management Console user name, the Support Element attempts to match to the Hardware Management Console user name based on the user name and password that is provided on the Support Element log on prompt. The Support Element user name is created dynamically with permissions based on the Hardware Management Console user name.
  - If a single Hardware Management Console user name matches both the user name and password on the Support Element, then this user name is logged on to the Support Element.
  - If multiple Hardware Management Console user names match both the user name and password on the Support Element, then the matching user names are compared based on properties such as permissions or settings.
    - If all matching user names have the same properties, then the user name from the Hardware Management Console that most recently targeted the Support Element is used.
    - If at least one user name has different properties, then a user name cannot be chosen and that user name cannot log on to the Support Element.
- As you attempt to log on to the Support Element with a Hardware Management Console user name and password, the appropriate audit logs are displayed.

Single Object Operations task update

If a user ID is created on a Hardware Management Console Version 2.15.0 and that user ID is not on the targeted Support Element Version 2.15.0, then a new user ID is created dynamically for the Support Element. The Support Element user ID, that is created, is based on the HMC user ID (including the HMC name) and similar permissions as the user ID on the Hardware Management Console. Thus, the naming convention that is previously used in the following table does not apply to Support Element Version 2.15.0. The user ID does not persist after the single object operation and it does not appear in tasks such as **User Management**. Also, since the user settings for these users are initially created from the Hardware Management Console **User Settings** task, this task is only available on the Hardware Management Console for these users and is not available on the Support Element.

Table 1. Association between Hardware Management Console task roles and Support Element Version 2.14.1 and prior target object user IDs

Hardware Management Console Task Roles (descending order of "most powerful")	**Support Element Version 2.14.1 and prior target object user IDs** **Note: These user IDs cannot be modified.**
Access Administrator Tasks	SooAcsadmin
Service Tasks	SooService
System Programmer Tasks	SooSysprog
Advanced Operator Tasks	SooAdvanced
None of the above	SooOperator

Miscellaneous changes

The following miscellaneous changes are part of Version 2.15.0:

- The **Load** task and **Customize/Delete Activation Profiles** task now support NVMe devices to perform loads from select partition in General, Linux Only, and z/VM operating modes.
- The **Manage Syslog Servers** task now supports the option to secure SSL connections between the Hardware Management Consoles and the syslog servers. You also have the option to enable logging for a specified server.
- The Hardware Management Console Version 2.15.0 support provides n-2 system levels only (IBM z13® and IBM z14®). IBM z14 (HMC Version 2.14.1) is the last system to support four generations of systems (n through n-4).
- The Hardware Management Console Version 2.15.0 no longer supports IBM zBX Model 004, IBM zBX Model 003, or IBM zBX Model 002.
- The **User Management** task allows you to enable or disable HMC multi-factor authentication (MFA) for users and templates with the new **HMC MFA** option.
- New customizable data types include:
  - Last User Logon Data - restores the enterprise wide data of the newest log on information, replicating automatically from the replica to the primary.
  - Remote Syslog Server Data - contains configuration data specified in the **Manage Syslog Servers** task for the syslog servers that the Hardware Management Console sends audit and event information to, including which data types are sent.
  - User Interface Customization Data - restores the user interface customization data.
- The Change LPAR Group Controls scheduled operation is added to the **Customized Scheduled Operations** task.
- A new **Customize/Delete Activation Profiles** task control is added to the Security page. The Elliptical Curve Cryptography (ECC) key import setting for CPACF allows the control enablement of digital signatures when the logical partition is activated.
- A new **Customize/Delete Activation Profiles** task control that is called Enable Secure Boot for Linux is added to the image Load page. When enabled, this new feature checks the signature(s) of the software being loaded to ensure that the signature matches that used by the distributor.
- A new Removable Media or FTP Server window is added for **Perform Model Conversion** task and **Reassign Hardware Management** task.
- The following Support Element tasks can now be accessed from the Hardware Management Console:
  - Advanced Facilities

  - Change LPAR Cryptographic Controls
  - Channel PCHID Assignment
  - Channel Problem Determination
  - Configure On/Off
  - Cryptographic Configuration
  - Cryptographic Management
  - Display Adapter ID
  - Enable/Disable Dynamic Channel Subsystem
  - FCP Configuration
  - FCP NPIV Mode On/Off
  - Input/Output (I/O) Configuration
  - Manage PCI System Services
  - Network Traffic Analyzer Authorization
  - Query Channel Crypto/Configure Off/On Pending
  - Query Coupling Facility Reactivations
  - Redundant I/O Interconnect Status and Control
  - Release I/O Path
  - Reset Error Thresholds
  - Service On/Off
  - Service Required State Query
  - Show LED
  - Storage Information
  - Update PCI Adapter Internal Code
  - View Internal Code Changes Summary
  - View LPAR Cryptographic Controls
- The **Manage Power Service State** task has been updated to now support Bulk Power Adapters (BPAs) in addition to Power Distribution Units (PDUs).
- The **Monitor System Events** task has been updated to clarify the Dynamic Partition Manager (DPM) event monitors.
- The **Configure Storage** task has been updated to document how to optimize second-level virtualization and share FCP disks across partitions. This task is available only on a Dynamic Partition Manager (DPM)-enabled system.

Introduction to the Hardware Management Console

The Hardware Management Console (HMC) communicates with each Central Processor Complex (CPC) through the CPC's Support Element (SE). When tasks are performed at the Hardware Management Console, the commands are sent to one or more Support Elements which then issue commands to their CPCs. CPCs can be grouped at the Hardware Management Console so that a single command can be passed along to as many as all of the CPCs defined to the Hardware Management Console. One Hardware Management Console can control up to 100 Support Elements and one Support Element can be controlled by 32 Hardware Management Consoles. Refer to Figure 3 on page 19 and Figure 4 on page 20 for typical Hardware Management Console configurations.

The following concepts and functions of the Hardware Management Console are described in further detail:

- “Remote operations” on page 36
- “Remote support facility” on page 43

- “LDAP support for user authentication” on page 45
- “IPv6 support” on page 45
- “Context sensitive help” on page 46
- “Disruptive tasks” on page 47
- “About activation profiles” on page 48
- “USB flash memory drive” on page 50
- “Server requirements for supporting FTP, SFTP, or FTPS” on page 15.

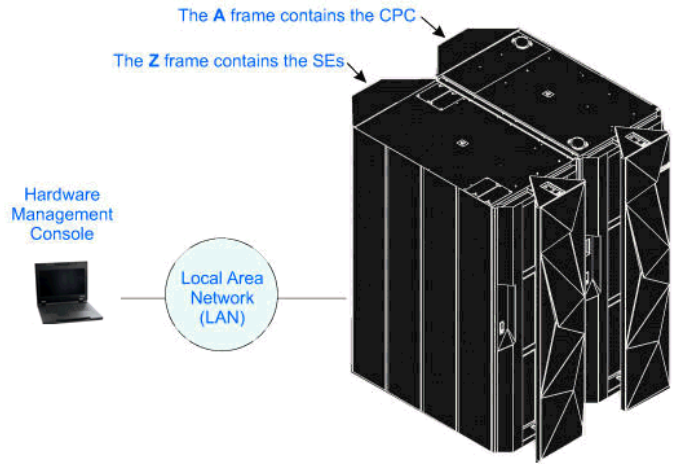


Figure 3. Hardware Management Console configuration in a single CPC environment

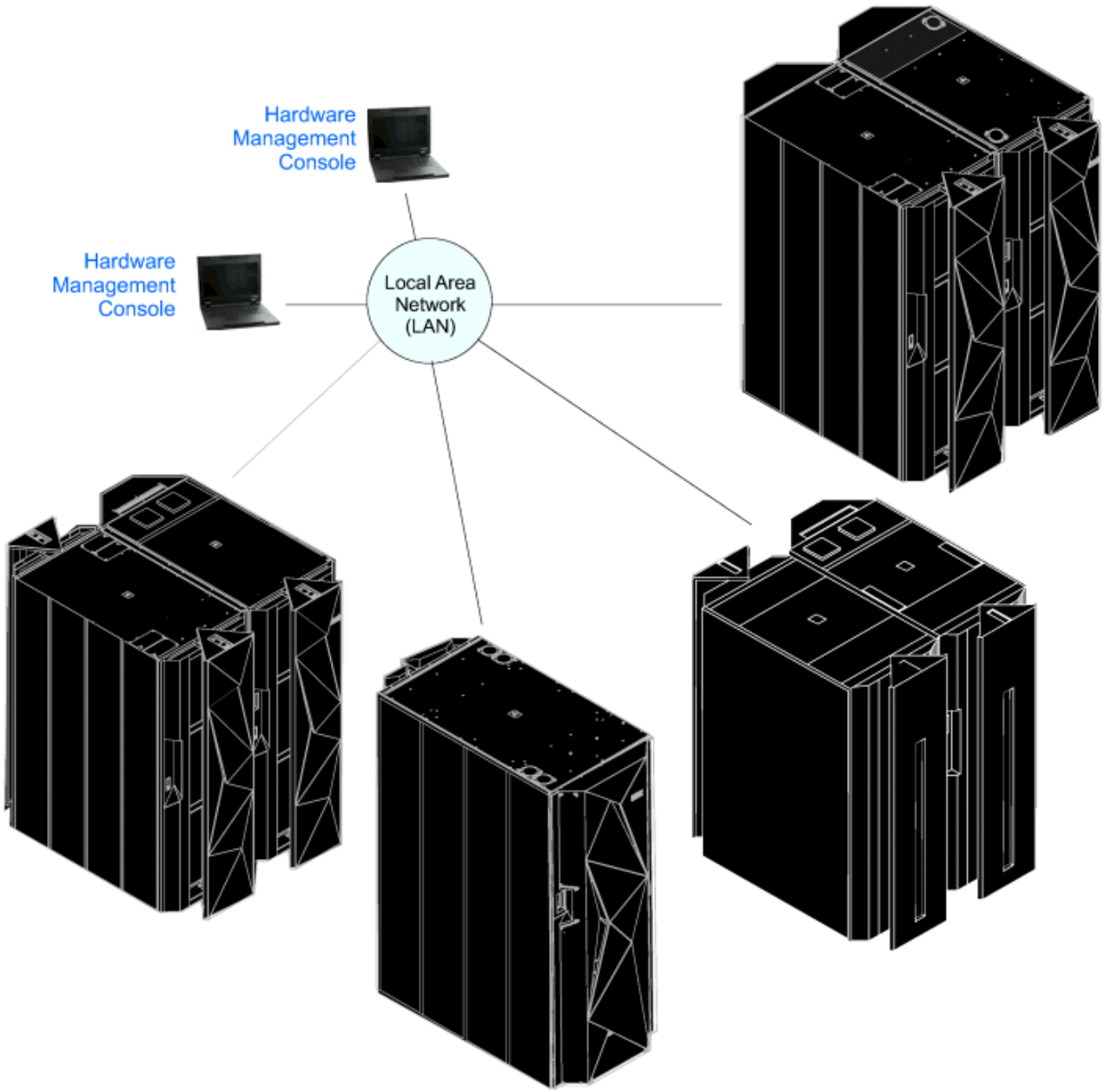


Figure 4. Hardware Management Console configuration in a multiple CPC environment

The Hardware Management Console (HMC) assists you when navigating through the user interfaces and describes the tasks that you can use on the console and for selected systems. It reflects the licensed machine code for the HMC Application, Version 2.15.0. You can tell if your HMC has this version that is installed by looking at the title bar on the workplace window or by hovering your mouse over **HMC Version** from the Welcome pane. You can use the Hardware Management Console for the following processors:

- IBM z15™ (z15™)
- IBM LinuxONE III (LinuxONE III)
- IBM z14® (z14)
- IBM LinuxONE Emperor II (Emperor II) and IBM LinuxONE Rockhopper II
- IBM z13 (z13) and IBM z13s® (z13s®)
- IBM LinuxONE Emperor (Emperor) and IBM LinuxONE Rockhopper (Rockhopper)

If you have an IBM Z (Z) or IBM LinuxONE (LinuxONE) system, your processor operates only in logically partitioned (LPAR) mode.

Notes:

- The task windows and user interface screens that are represented in this information are general samples. They may or may not represent the exact windows that are displayed for your user ID or version.
- The terms *system*, *server*, *object*, and *CPC* are used interchangeably through out this documentation.
- In the IBM Z or LinuxONE environments, the term *CPC* consists of an IBM Z or a LinuxONE. The term *zCPC* refers to the physical collection of main storage, central processors, timers, and channels within an IBM Z or a LinuxONE.
- Tasks can be performed remotely, unless stated otherwise.

Not all code enhancements that are described may be available on your Support Element. Locate the version of code that is installed in your Support Element by looking at the title bar on the workplace window or click **SE Version** from the Welcome pane.

Note: The *Support Element Operations Guide* is no longer available. The information has been incorporated into the console help information.

Related publications

An IBM publication that you might find helpful follows. You can access the portable document format (PDF) files from Resource Link (www.ibm.com/servers/resourcelink) under the **Library** section.

- *IBM Dynamic Partition Manager (DPM) Guide*, SB10-7176, includes information for Linux administrators and systems administrators who use the HMC to create and manage partitions on an IBM Z mainframe that has Dynamic Partition Manager (DPM) mode enabled.

Turning on the Hardware Management Console

First, turn on the Hardware Management Console by setting both the display and system units to the *On* position. You will then see the Initialization is in progress window.

When initialization is complete, the Welcome to the Hardware Management Console window is displayed as shown in Figure 5 on page 21.

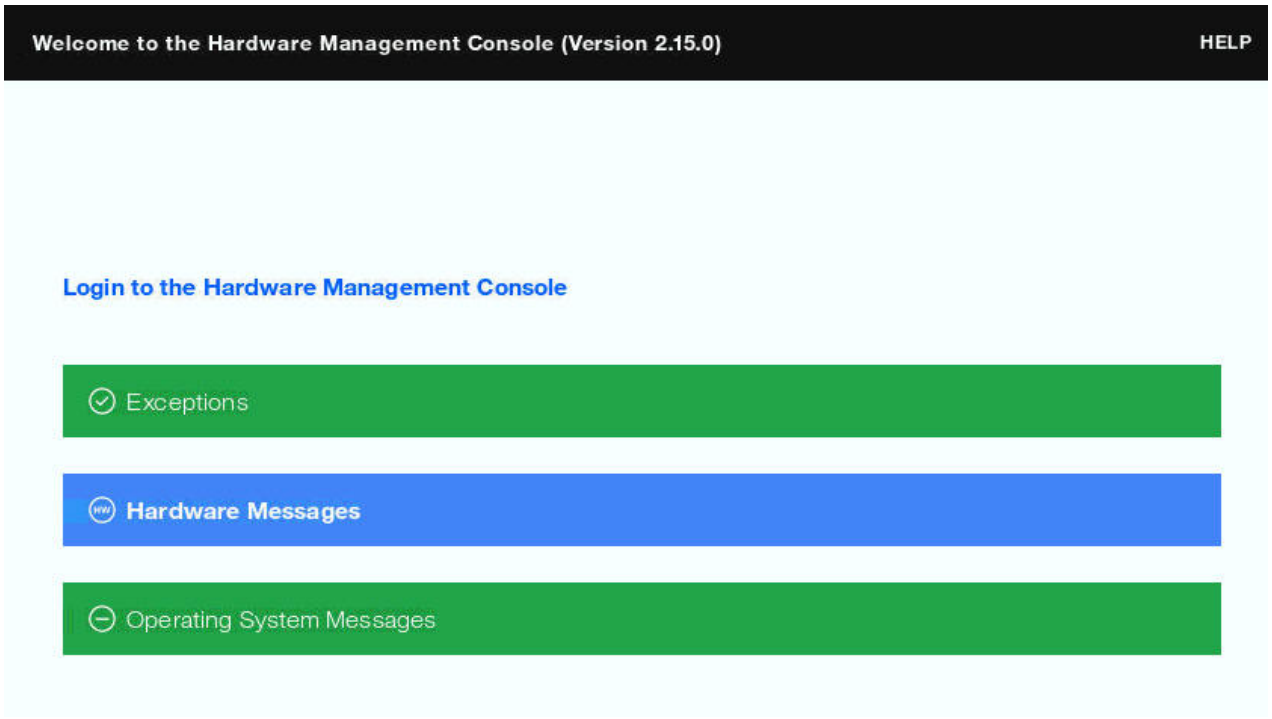


Figure 5. Hardware Management Console welcome window

The Welcome window includes links for logging on to the Hardware Management Console and to the online help. It also includes status indicators and message icons. The status indicator reflects the current overall status of the defined CPCs and images. The message indicators alert you to any hardware or operating system messages. If any of these icons do not display a green bar, you are alerted that a message was logged that might require your attention.

Logging on to the Hardware Management Console

To log on to the Hardware Management Console, click **Login to the Hardware Management Console** from the Welcome window.

The Logon window is displayed as shown in Figure 6 on page 22.

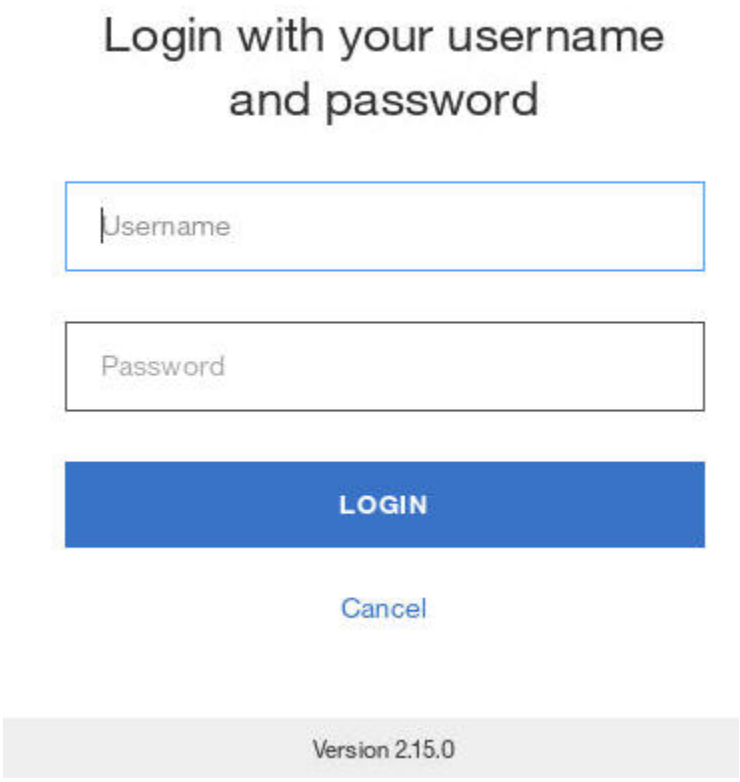


Figure 6. Hardware Management Console log on window

Default user IDs and passwords are established as part of a base Hardware Management Console. The Access Administrator **should assign new user IDs and passwords for each user and change the default user IDs as soon as the Hardware Management Console is installed** by using the **User Management** task. The predefined default user roles, user IDs, and passwords are:

```
Access Administrator    ACSADMIN      PASSWORD
Advanced Operator       ADVANCED      PASSWORD
Operator                OPERATOR      PASSWORD
Service Representative  SERVICE       SERVMODE
Storage Administrator   STORAGEADMIN  PASSWORD
System Programmer       SYSPROG       PASSWORD
```

Note: Letter case (uppercase, lowercase, mixed) is not significant for the default user IDs or passwords.

Attention: In the state of California, US, the use of default passwords are no longer allowed. The first time a default user ID logs on to the console, the default password must be changed. A prompt is displayed requiring the password change. This is initiated in the **User Management** task by SERVICE or a user that is assigned a role with Manage Users task permission.

To log on, enter one of the default user ID and password combinations, the user ID and password combination that is assigned to you by your Access Administrator, or your LDAP user ID (see "LDAP support for user authentication" on page 45). Then, click **Logon**.

Note: If you are accessing the Hardware Management Console remotely and depending on the browser you are using, the entry fields and the **Logon** button may initially be hidden until the Logon window has completely loaded. Use the online help if you need additional information by clicking **Help** from the Logon window.

After you log on, the Hardware Management Console workplace window is displayed. If enabled, the Tip of the Day window is displayed.

The Hardware Management Console workplace window allows you to work with tasks for your console and CPCs (servers). Not all tasks are available for each user ID. See "Tasks and default user IDs" on page 23 for a listing of all tasks and the default user IDs associated with the tasks.

If at any time you do not know or remember what user ID is logged on to the Hardware Management Console, click the user ID on the task bar.

Tasks and default user IDs

This section lists the tasks that you can perform that use the Hardware Management Console and the predefined default user IDs that are initially associated with that task. However, you can create customized users that would allow you to have unique user IDs and multiple roles. The management of these roles is performed by using the **User Management** task. The **User Management** task also provides the ability to define which roles are to be associated with each specific user ID.

Attention: In the state of California, US, the use of default passwords are no longer allowed. The first time a default user ID logs on to the console, the default password must be changed. A prompt is displayed requiring the password change. This is initiated in the **User Management** task by SERVICE or a user that is assigned a role with Manage Users task permission.

Table 2 on page 23 lists the tasks that can be performed on the console and the corresponding predefined default user IDs that can perform these tasks.

Table 3 on page 26 lists the tasks that can be performed on the objects and the corresponding predefined default user IDs that can perform these tasks.

Note: For tasks that are applicable for systems on which IBM Dynamic Partition Manager (DPM) is enabled, see the "DPM task and resource roles" on page 31.

Table 2. Hardware Management Console tasks and default user IDs

Tasks	**Default user IDs**				
	OPERATOR	**ADVANCED**	**SYSPROG**	**ACSADMIN**	**SERVICE**
Analyze Console Internal Code					X
Archive Security Logs			X	X	X
Audit and Log Management			X	X	X
Authorize Internal Code Changes			X		X
Backup Critical Console Data			X		X
Block Automatic Licensed Internal Code Change Installation				X	
Certificate Management			X	X	X
Change Console Internal Code		X	X		X
Change Password	X	X	X	X	X
Configure 3270 Emulators			X		

Table 2. Hardware Management Console tasks and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	**ADVANCED**	**SYSPROG**	**ACSADMIN**	**SERVICE**
Configure Backup Settings		X	X	X	X
Configure Data Replication				X	
Configure IDAA Call-Home			X		X
Console Default User Settings				X	
Console Messenger	X	X	X	X	X
Copy Console Logs to Media					X
Create Welcome Text				X	
Customize API Settings				X	
Customize Automatic Logon				X	
Customize Console Date/Time	X	X	X	X	X
Customize Console Services			X	X	X
Customize Customer Information			X		X
Customize Network Settings				X	X
Customize Outbound Connectivity			X		X
Customize Product Engineering Access				X	
Customize Remote Service			X		X
Customize Scheduled Operations			X	X	X
Domain Security				X	X
Enable FTP Access to Mass Storage Media			X		
Fibre Channel Analyzer	X	X	X	X	X
Format Media	X	X	X	X	X
HMC Mobile Settings				X	
Installation Complete Report					X
Logoff or Disconnect	X	X	X	X	X
Manage Console Recovery					X
Manage Coupling Facility Port Enablement					X
Manage Print Screen Files	X	X	X	X	X
Manage Product Engineering Access Control File					X
Manage Remote Connections	X	X	X	X	X
Manage Remote Support Requests	X	X	X	X	X
Manage SSH Keys				X	X
Manage Syslog Servers				X	
Manage Web Services API Logs			X	X	

Table 2. Hardware Management Console tasks and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	**ADVANCED**	**SYSPROG**	**ACSADMIN**	**SERVICE**
Monitor System Events			X		
Network Diagnostic Information	X	X	X	X	X
Object Locking Settings		X	X	X	X
Offload Problem Analysis Data to Removable Media	X	X	X	X	X
Perform a Console Repair Action					X
Power Off or Restart	X	X	X	X	X
Reassign Hardware Management Console					X
Rebuild Vital Product Data					X
Remote Hardware Management Console	X	X	X	X	X
Report a Problem	X	X	X		X
Save/Restore Customizable Console Data				X	
Save Upgrade Data					X
Single Step Console Internal Code		X	X		X
Tip of the Day	X	X	X	X	X
Transmit Console Service Data	X	X	X	X	X
Transmit Vital Product Data			X		X
User Management	X	X	X	X	X
User Settings	X	X	X	X	X
Users and Tasks	X	X	X	X	X
View Console Events	X	X	X	X	X
View Console Information	X	X	X	X	X
View Console Service History	X	X	X	X	X
View Console Tasks Performed	X	X	X	X	X
View Licenses	X	X	X	X	X
View PMV Records	X	X	X	X	X
View Security Logs			X	X	X
Virtual Support Element Management					X
What's New	X	X	X	X	X

Table 3. Tasks performed on objects and default user IDs

Tasks	Default user IDs				
	OPERATOR	**ADVANCED**	**SYSPROG**	**ACSADMIN**	**SERVICE**
Hardware Messages	X	X	X	X	X
Operating System Messages	X	X	X	X	X
Daily					
Activate	X	X	X		X
Deactivate	X	X	X		X
Grouping			X	X	
Reset Normal	X	X	X		X
Recovery					
Access Removable Media			X		X
Integrated 3270 Console	X	X	X		X
Integrated ASCII Console	X	X	X		X
Load	X	X	X		X
Load from Removable Media or Server			X		X
PSW Restart		X	X		X
Reset Clear	X	X	X		X
Reset Normal	X	X	X		X
Single Object Operations	X	X	X	X	X
Start All Processors		X	X		X
Stop All Processors		X	X		X
Service					
Archive Security Logs			X		X
Backup Critical Data			X		X
Manage Power Service State			X		X
Network Traffic Analyzer Authorization				X	
Perform Problem Analysis	X	X	X		X
Perform Transfer Rate Test					X
Redundant I/O Interconnect Status and Control			X		X
Report a Problem	X	X	X	X	X
Reset Error Thresholds					X
Restore Critical Data					X
Retrieve Backup and Upgrade Data		X	X	X	X
Save Upgrade Data					X

Table 3. Tasks performed on objects and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	**ADVANCED**	**SYSPROG**	**ACSADMIN**	**SERVICE**
Service Required State Query					X
Service Status	X	X	X	X	X
Transmit Service Data	X	X	X	X	X
View PMV Records	X	X	X	X	X
View Service History	X	X	X		X
Change Management					
Alternate Support Element			X		X
Alternate Support Element Engineering Change (ECs)					X
Change Internal Code		X	X		X
Concurrent Upgrade Engineering Changes (EC)			X		X
Engineering Changes (ECs)					X
Manage PCI System Services	X	X	X		X
Product Support Directed Changes					X
Query Channel Crypto/Configure Off/On Pending	X	X	X	X	X
Query Coupling Facility Reactivations	X	X	X		X
Retrieve Internal Code		X	X		X
Save Legacy Upgrade Data					X
Single Step Internal Code Changes		X	X		X
Special Code Load					X
System Information	X	X	X	X	X
Update PCI Adapter Internal Code	X	X	X		X
View Internal Code Changes Summary			X		X
Remote Customization					
Customer Information			X		X
Remote Service			X		X
Operational Customization					
Automatic Activation			X		
Change LPAR Controls			X		X
Change LPAR Cryptographic Controls			X		X
Change LPAR Group Controls			X		X
Change LPAR I/O Priority Queuing			X		X

Table 3. Tasks performed on objects and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	**ADVANCED**	**SYSPROG**	**ACSADMIN**	**SERVICE**
Change LPAR Security			X		X
Configure Channel Path On/Off		X	X		
Customize/Delete Activation Profiles			X		
Customize Scheduled Operations			X	X	X
Customize Support Element Date/Time	X	X	X	X	X
Enable I/O Priority Queuing			X		X
Enable/Disable Dynamic Channel Subsystem			X		X
Logical Processor Add			X		X
OSA Advanced Facilities			X		X
Reassign I/O Path		X	X		X
Storage Information	X	X	X		X
View Activation Profiles	X	X			X
View LPAR Cryptographic Controls			X		X
Object Definition					
Add Object Definition				X	X
Change Object Definition				X	X
Reboot Support Element				X	X
Remove Object Definition				X	
Configuration					
Advanced Facilities			X		X
Channel PCHID Assignment	X	X	X		X
Channel Problem Determination	X	X	X		X
Configure On/Off	X	X	X		X
Cryptographic Configuration			X		X
Cryptographic Management	X	X	X	X	X
Display Adapter ID			X		X
Edit Frame Layout					X
FCP Configuration	X	X	X		X
FCP NPIV Mode On/Off	X	X	X		X
Input/Output (I/O) Configuration			X		X
Input/Output (I/O) Configuration Save and Restore					X
Manage Flash Allocation			X		X

Table 3. Tasks performed on objects and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	**ADVANCED**	**SYSPROG**	**ACSADMIN**	**SERVICE**
Manage Key Manager Connections			X	X	
Manage System Time			X		X
Perform Model Conversion			X		
Release I/O Path		X	X		X
Service On/Off	X	X	X		X
Show LED			X		X
System Input/Output Configuration Analyzer			X		X
Transmit Vital Product Data			X		X
View Frame Layout			X		
View Partition Resource Assignments					X
Energy Management					
Energy Optimization Advisor			X		X
Set Power Cap			X		X
Set Power Saving			X		X
Monitor					
Environmental Efficiency Statistics	X	X	X		X
Monitors Dashboard	X	X	X	X	X
Monitor System Events			X		

Logging on to the Support Element with a Hardware Management Console user name

When you log on to the Support Element with a Hardware Management Console user name, the following scenarios are considered.

- When the Support Element does not have a user name that matches the Hardware Management Console user name, the Support Element attempts to match to the Hardware Management Console user name based on the user name and password that is provided on the Support Element log on prompt. The Support Element user name is created dynamically with permissions based on the Hardware Management Console user name.
  - If a single Hardware Management Console user name matches both the user name and password on the Support Element, then this user name is logged on to the Support Element.
  - If multiple Hardware Management Console user names match both the user name and password on the Support Element, then the matching user names are compared based on properties such as permissions or settings.
    - If all matching user names have the same properties, then the user name from the Hardware Management Console that most recently targeted the Support Element is used.
    - If at least one user name has different properties, then a user name cannot be chosen and that user name cannot log on to the Support Element.
- As you attempt to log on to the Support Element with a Hardware Management Console user name and password, the appropriate audit logs are displayed.

Introduction to Dynamic Partition Manager (DPM)

A new administrative mode, Dynamic Partition Manager (DPM), is introduced with Hardware Management Console (HMC) Version 2.13.1. A system can be configured to run in either standard Processor Resource/ Systems Manager (PR/SM) mode or DPM mode, which uses PR/SM functions but presents a simplified user interface for creating partitions and managing system resources. The mode is enabled prior to system power-on reset (POR).

Partitions on a DPM-enabled system can host a single operating system or hypervisor. DPM supports the Linux operating system and hypervisors that can host multiple Linux images. DPM also supports Secure Service Container partitions.

DPM provides dynamic I/O management capabilities through which you can accomplish the following tasks.

- Create and provision an environment - Creation of new partitions, assignment of processors and memory, and configuration of I/O adapters. HMC tasks to accomplish these functions include:
  - **New Partition**
  - **Partition Details**
  - **Manage Processor Sharing**
  - **Manage Adapters**
  - **Configure Storage**
- Manage the environment - Modification of system resources without disrupting running workloads.
- Monitor and troubleshoot the environment - Source identification of system failures, conditions, states, events that may lead to workload degradation.

  To view current statistics for a DPM-enabled system, you can select the system from the navigation pane, then select the **Monitor** tab from the work pane area, as shown in Figure 7 on page 30. (The **Monitors Dashboard** task is not applicable for DPM-enabled systems.)

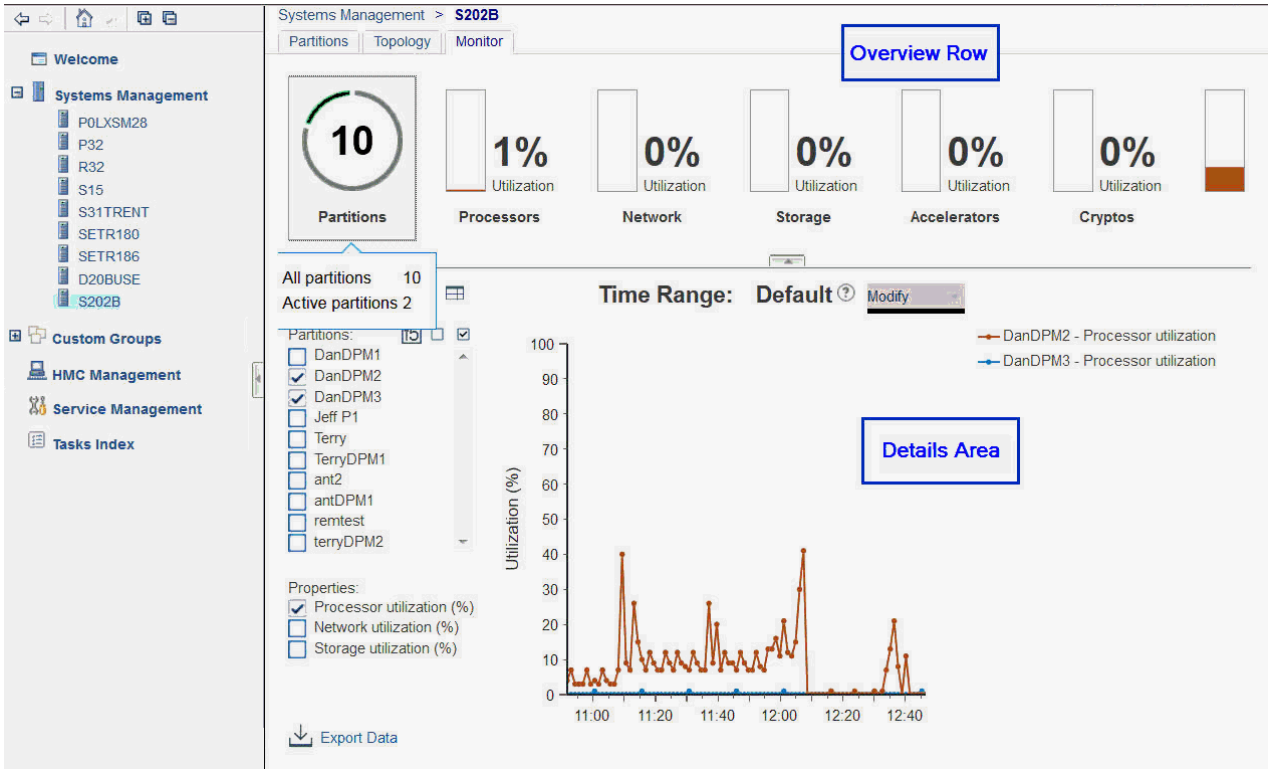


Figure 7. DPM System Monitoring

DPM task and resource roles

Tasks and resources need to be made available or excluded based on the roles to which they are assigned. You may create your own specific task and resource roles which include specific tasks and resources; however, HMC user management provides default roles for your convenience. Table 5 on page 31 identifies the DPM tasks along with default task roles. The table identifies the task roles in which a particular task is included. It also documents the resource roles that are required to complete a task.

The Details task has unique behavior with respect to roles. The Details task (view only) is always available for all resources accessible to a user ID. If a user ID has permission for the Details task, through an assigned task role, modifications may be made in the details task. Specific Details task permissions are assigned to default task roles as shown in Table 5 on page 31.

For example consider user ID SIGMUND. SIGMUND has been given the Defined System Managed Objects resource role but not the System Programmer (SP) task role, which contains the Partition Details task. SIGMUND will still be able to launch details task for a Partition, but the content of the task will be displayed read-only such that SIGMUND cannot modify to the resource.

All tasks that can be launched from the HMC workspace are marked in **bold**. Where there are both administrative and operator roles, such as SP and OP, any permissions given to the operator are also available for the administrator role. See Table 4 on page 31 for the tasks mapping legend.

Table 4. DPM task roles mapping legend

Legend	Description
AA	Access Administrator Tasks
SP	System Programmer Tasks
OP	Operator Tasks
AOP	Advanced Operator Tasks
SER	Service Representative Tasks
SA	Storage Administrator Tasks
X	Required role to perform a task.
O	At least one of the roles is required to perform a task.
*	Denotes a task that is available through the Support Element (SE) only.

Table 5. DPM task roles mapping

DPM Tasks	Task Roles					
	AA	SP	OP	AOP	SER	SA
Configure Storage		O			O	O"1" on page 33
- Create, modify, or delete a storage group or tape link		X				
- Attach a storage group or tape link to a partition		X				
- Detach a storage group or tape link from a partition		X				
- Change an HBA device number for an FCP storage group or an FCP tape link		X				
Delete Partition		O			O	

Table 5. DPM task roles mapping (continued)

DPM Tasks	Task Roles					
	AA	**SP**	**OP**	**AOP**	**SER**	**SA**
Disable Dynamic Partition Manager*					X	
Dump (Partition)		O	O	O	O	
Enable Dynamic Partition Manager*					X	
Getting Started with Dynamic Partition Manager	O	O	O	O	O	
Manage Processor Sharing		O			O	
Manage Adapters		O	O	O	O	
- Adapter Details		O			O	
- Create HiperSockets Adapter		O			O	
- Delete HiperSockets Adapter		O			O	
- Reassign Channel Path IDs		O			O	
- Reassign Devices		O			O	
- Export WWPNs		O	O	O	O	
New Partition (basic mode)		O			O	
New Partition (advanced mode)		O			O	
- Controls		O			O	
Partition Details		O			O	
- Controls		O			O	
Start (start a single DPM system)		O			O	
Start (start one or more DPM partitions)		O	O	O	O	
Stop (stop a single DPM system)		O			O	
Stop (stop one or more DPM partitions)		O	O	O	O	
System Details		O			O	
- Configure System Management (OSM) Adapters*					X	
- Manage Secure Execution Keys or Import Secure Execution Keys*					X	

Table footnote:

1. During the initial storage setup for a DPM-enabled system, the storage administrator does not have access to the **Configure Storage** task until the system administrator configures storage cards for the system.

Introduction to the HMC Mobile app

The IBM HMC Mobile for Z and LinuxONE (HMC Mobile) app provides an easy-to-use interface for securely monitoring and managing IBM Z and LinuxONE systems from anywhere.

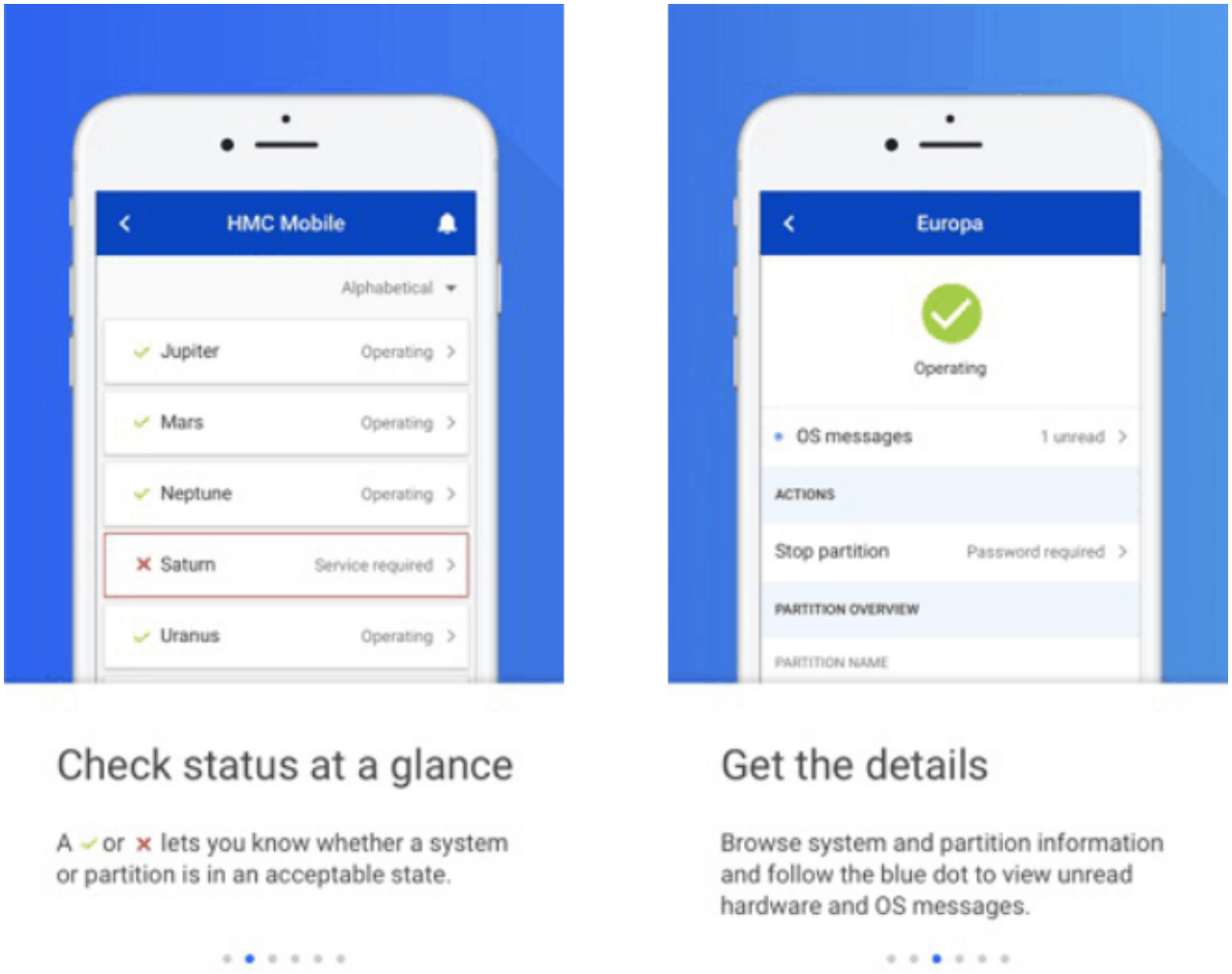


Figure 8. Select pages from the tour of the HMC Mobile app

The HMC Mobile app provides system and partition views, status monitoring, hardware messages, operating system messages, and the ability to receive push notifications from the HMC, using the existing support server connection. Management tasks include the ability to change activation profiles, as well as to start (or activate) and to stop (or deactivate) partitions. Through the app, users can monitor or manage systems that either run in standard mode (that is, with Processor Resource/System Manager or PR/SM), or run with Dynamic Partition Manager (DPM) enabled.

Through the **HMC Mobile Settings** task on the HMC, administrators can enable the app for use, restrict usage to specific HMC users and IP addresses, restrict the app to read-only access, and more. This task includes links to the iOS App Store or Google Play store, where you can download the HMC Mobile app to your mobile device. For these links to be displayed, you must be connected to the HMC through a remote

browser and have access to the internet. You must have one of the following versions installed on the mobile device that you plan to use.

- iOS 11 or later
- Android 4.4 (KitKat) or later

For more information, see the online help for the **HMC Mobile Settings** task, and the FAQs on the HMC Mobile app website at http://ibm.biz/hmc-mobile.

To download the HMC Mobile app to your mobile device, go to the iOS App Store or Google Play store.

- http://ibm.biz/hmc-mobile-ios
- http://ibm.biz/hmc-mobile-android

Introduction to the installation survey

If your company has recently installed or upgraded a new system, a survey is available that enables you to provide feedback about your installation experience. Thirty days after the installation, the survey will become available; it will be launched the first time a user with the sysprog role logs into an HMC with a remote web browser.

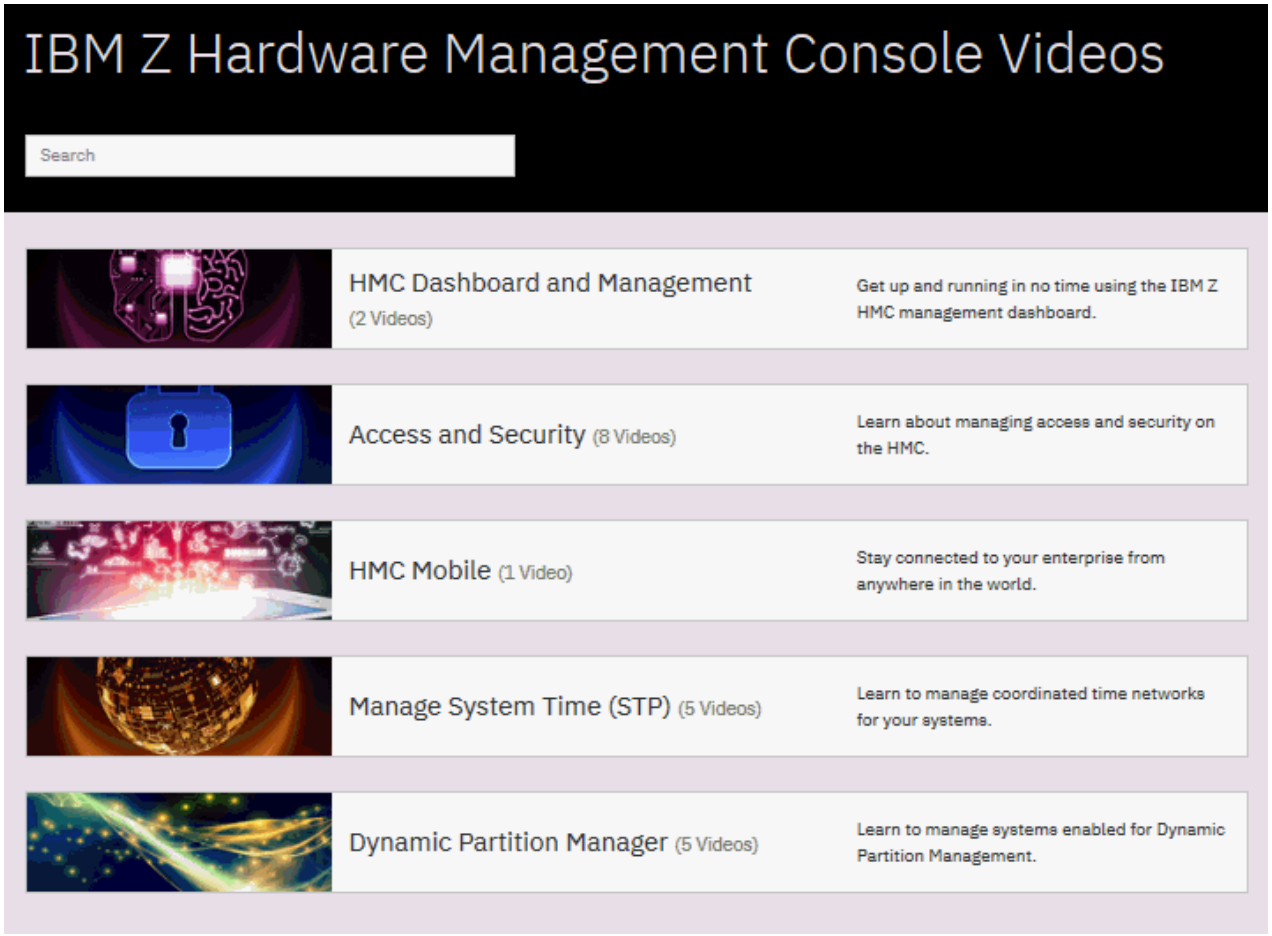
The survey is brief and easy to step through. It focuses on how you feel about the installation that you just performed and gives you the option to provide an email address so that IBM can follow-up with you regarding your installation experience.

If you are presented with the installation survey on the HMC, we encourage you to take the survey and to share it with your colleagues. We appreciate your feedback on the system that you recently installed and are using. It will be used as valuable input as we strive to continually improve the IBM Z platform.

YouTube videos for HMC content

You can now see additional Hardware Management Console information by viewing YouTube videos at https://ibm.biz/IBM-Z-HMC. The videos that are currently available include the following topics:

- HMC Dashboard and Management
- Access and Security
- HMC Mobile
- Management System Time (STP)
- Dynamic Partition Manager



Supported character sets

The console only supports Single-Byte Character Sets (SBCS) for data entry.

Changing your time-of-day clock

This section includes some additional information pertaining to “Setting the Support Element time” on page 36 and “Setting the Support Element time zone” on page 35.

Setting the Support Element time zone

When the time zone is changed at the time source, each CPC is notified of the change and the operating system adjusts its time zone to that of the time source. Because there was no change to the Coordinated Universal Time (UTC), the Support Element(s) is not notified of a change.

To set or update the Support Element(s) clock's time zone, use the following steps:

1. Open the group that contains the object with the Support Element that you want to connect to.
2. Select one CPC.
3. Open the **Single Object Operations** task. The Single Object Operations Task Confirmation window is displayed.
4. If you want to continue establishing a session with a single CPC console, click **Yes**. The Primary Support Element window is displayed.
5. Open the **Customize Support Element Date/Time** task.
6. The Customize Support Element Date and Time window displays the current Support Element date, time, and time zone. Enter the new information, then click **OK**.
7. The Customize Support Element Date and Time Confirmation window is displayed, then click **Yes**.

8. The Customize Support Element Date/Time Progress window is displayed.

   Then the message "System (Sysplex) time is in use. Your input will not be used to set the battery operated clock." displays in the status field.

   This message means that the Support Element detected an active time source and updated its date, time, and time zone to match that of the time. Click **OK**.

Setting the Support Element time

The following describes the actions to take when setting the time depending on whether or not a time source (such as ETR or STP) is enabled.

Time source enabled

Attention: Issuing a set time on a Sysplex Timer (9037) may cause any running operating systems to enter a disabled wait state. Consult your operating system documentation for details.

If the ETR, which uses the Sysplex Timer (9037), is installed in the processor complex, the time, date, and offset from the Sysplex Timer will be used to set the time-of-day in all attached CPCs. If you need to correct the time, change the time at the ETR.

If Server Time Protocol (STP) is enabled in the CPC, the time, date, and offsets from the Current Time Server will be used to set the time-of-day. If you need to correct the time-of-day, adjust the time at the current server.

Time source not enabled

The Support Element(s) contain a battery operated TOD clock. The CPC TOD clock will be set using the Support Element TOD when the system is activated.

Use the following steps to correct the date or time in the Support Element(s):

1. Select a group of defined CPCs or an individual CPC.
2. Open the **Customize Support Element Date/Time** task.
3. The Customize Support Element Date and Time window displays the current Hardware Management Console date, time, and time zone. Enter the new information, then click **Use New Time...**.

   Note: Depending on your machine type and model the Support Element **Clock** and **Time zone** fields cannot be modified by the Hardware Management Console. In that case, you must use the **Single Object Operations** task to set the Support Element time zone.
4. The Customize Support Element Date and Time Confirmation window is displayed, then click **Yes**.
5. The Customize Support Element Date/Time Progress window is displayed. Click **OK** to continue with the task.

Attention: The following steps will disrupt the operating system if it is running, and should only be performed if the CPC TOD needs to be updated now.

Note: These steps assume that the activation profiles have been set up for each CPC.

Use the following steps to correct the CPC TOD:

1. Select a group of defined CPCs or an individual CPC.
2. Open the **Activate** task.
3. Click **Yes** on the Activate Task Confirmation window.
4. The Activate Progress window is displayed. Once Activate is complete, click **OK**.

Remote operations

Remote operations are designed for human interaction and use the Graphical User Interface (GUI) used by a local Hardware Management Console operator. There are two ways to perform operations remotely:

- Use a remote Hardware Management Console, or

- Use a web browser to connect to a local Hardware Management Console.

The *remote Hardware Management Console* is a Hardware Management Console that is on a different subnet from the Support Element, therefore the Support Element cannot be autodiscovered with IP multicast.

The choice between a remote Hardware Management Console and a web browser connected to a local Hardware Management Console is governed principally by the scope of control that is needed. A remote Hardware Management Console defines a specific set of managed objects that is directly controlled by the remote Hardware Management Console, while a web browser to a local Hardware Management Console has control over the same set of managed objects as the local Hardware Management Console. The communications connectivity and communication speed is an additional consideration; LAN connectivity provides acceptable communications for either a remote Hardware Management Console or web browser control.

Using a remote Hardware Management Console

A remote Hardware Management Console gives the most complete set of functions because it is a complete Hardware Management Console; only the process of configuring the managed objects is different from a local Hardware Management Console (see the **Add Object Definition** task). As a complete Hardware Management Console, a remote Hardware Management Console has the same setup and maintenance requirements as a local Hardware Management Console. A remote Hardware Management Console needs LAN TCP/IP connectivity to each managed object (Support Element) that is to be managed; therefore, any customer firewall that may exist between the remote Hardware Management Console and its managed objects must permit Hardware Management Console to Support Element communications to occur. A remote Hardware Management Console may also need communication with another Hardware Management Console for service and support. Table 6 on page 37 and Table 7 on page 38 shows the ports a remote Hardware Management Console uses for communications.

Table 8 on page 39 and Table 9 on page 39 shows the ports a remote Support Element uses for communications.

Table 6. Hardware Management Console inbound traffic from customer networks

TCP/IP Source Port	Usage
ICMP Type 8	Establish communications with resources being managed by the Hardware Management Console.
tcp 58787 - 58788 udp 58788	Automatic discovery of servers.
udp 9900	Hardware Management Console to Hardware Management Console automatic discovery.
tcp 55555	SSL encrypted communications from servers. The internal firewall only allows inbound traffic from the servers that are defined to the Hardware Management Console.
tcp 9920	SSL encrypted communications from Hardware Management Consoles and servers.
tcp 443	Remote user access to the Hardware Management Console. Inbound traffic for this port is only allowed by the internal firewall if **Remote operation** has been **Enabled** for the Hardware Management Console by using the **Customize Console Services** task.
tcp 9950 - 9959	Proxy **Single Object Operations** sessions to a server.
udp 161 tcp 161 tcp 3161	SNMP automation of the Hardware Management Console. Inbound traffic for these ports is only allowed by the internal firewall when SNMP automation is enabled by using the **Customize API Settings** task.

Table 6. Hardware Management Console inbound traffic from customer networks (continued)	
TCP/IP Source Port	**Usage**
tcp 6794	Web services SSL encrypted automation traffic. Inbound traffic for this port is only allowed by the internal firewall when Web Services automation is enabled by using the **Customize API Settings** task. Also, supports the HMC Mobile app, when enabled using the **HMC Mobile Settings** task.
tcp 61612	Connecting to the Web Services API message broker and flowing Streaming Text Oriented Messaging Protocol (STOMP) over the connection when the Web Services API is enabled by using the **Customize API Settings** task.
tcp 61617	Connecting to the Web Services API message broker and flowing OpenWire over the connection when the Web Services API is enabled by using the **Customize API Settings** task.
udp 123	Set the time of the servers.
udp 520	Interactions with routers and only used on the Hardware Management Console if **'routed'** is enabled in the **Customize Network Settings** task.
tcp 22	Remote access by Product Engineering and only allowed by the internal firewall if remote product engineering access is configured using the **Customize Product Engineering Access** task.
tcp 21	Inbound FTP requests. This is ***only*** enabled when the **Enable FTP Access to Hardware Management Console Mass Storage Media** task is being used. FTP is an unencrypted protocol, for maximum security these tasks should not be used on the Hardware Management Console.
tcp 67, 69, 4011 udp 67, 68, 69, 4011	These ports are utilized for allowing the HMC to become a boot server for a selected recovery image when the boot server is successfully started on the **Manage Console Recovery** task.

Table 7. Hardware Management Console outbound traffic to customer networks	
TCP/IP Source Port	**Usage**
ICMP Type 8	Establish communications with system resources being managed by the Hardware Management Console.
udp 9900	Hardware Management Console to Hardware Management Console automatic discovery.
tcp 58787 udp 58787	Automatic discovery of and establishing communications with servers.
tcp 55555	SSL encrypted communications to servers.
tcp 9920	SSL encrypted communications to Hardware Management Consoles and servers.
tcp 443	**Single Object Operations** to a server console.
tcp x	User authentication using an LDAP server where ***x*** is the port that the LDAP server is running on.
tcp 443	Call home requests as part of the Remote Support Facility (RSF). Also, supports the HMC Mobile app, when enabled using the **HMC Mobile Settings** task.
tcp 21	Load system software or utility programs.
tcp 22	Retrieve the SSH public key of hosts, using the **Manage SSH Keys** task, for securing SFTP connections to FTP servers. Also, used for the SFTP connections.

Table 7. Hardware Management Console outbound traffic to customer networks (continued)	
TCP/IP Source Port	**Usage**
udp 123	Connecting to a Network Time Protocol (NTP) server.
tcp 25	Send email events to a Simple Mail Transfer Protocol (SMTP) server for delivery, by using the **Monitor System Events** task, when the HMC is configured. (Might be a port other than 25, but 25 is the default SMTP port that most SMTP servers use.)
tcp 67, 69, 4011 udp 67, 68, 69, 4011	These ports are utilized for allowing the HMC to become a boot server for a selected recovery image when the boot server is successfully started on the **Manage Console Recovery** task.

Table 8. Support Element inbound traffic from customer networks	
TCP/IP Source Port	**Usage**
ICMP Type 8	Establish communications with Hardware Management Consoles (HMCs) managing the server.
tcp/udp 58787	Automatic discovery of system resources by HMCs.
tcp 55555	SSL encrypted communications from Hardware Management Consoles.
tcp 9920	SSL encrypted communications from Hardware Management Consoles.
tcp 443	Remote user access to the Support Element. Inbound traffic for this port is only allowed by the internal firewall if the **Single Object Operations** task is performed to the Support Element from the HMC.
udp 161 tcp 161 tcp 3161	SNMP automation. Inbound traffic for these ports is only allowed by the internal firewall when SNMP automation is enabled by using the **Customize API Settings** task.
udp 520	Interactions with routers and only used on the Support Element if **'routed'** is enabled in the **Customize Network Settings** task.
tcp 22	Remote access by Product Engineering and only allowed by the internal firewall if remote product engineering access is configured using the **Customize Product Engineering Access** task.

Table 9. Support Element outbound traffic to customer networks	
TCP/IP Source Port	**Usage**
ICMP Type 8	Establish communications with Hardware Management Consoles (HMCs) managing the Support Element.
udp 9900	Hardware Management Console to Hardware Management Console automatic discovery.
tcp 58787 udp 58787	Automatic discovery of system resources by HMCs.
tcp 55555	SSL encrypted communications to Hardware Management Consoles.
tcp 9920	SSL encrypted communications to Hardware Management Consoles.
tcp x	User authentication using an LDAP server where ***x*** is the port that the LDAP server is running on.
tcp 21	Load system software or utility programs.

Table 9. Support Element outbound traffic to customer networks (continued)	
TCP/IP Source Port	**Usage**
tcp 22	Retrieve the SSH public key of hosts, using the **Manage SSH Keys** task, for securing SFTP connections to FTP servers. Also, used for the SFTP connections.
udp 520	Interactions with routers and only used on the Support Element if **'routed'** is enabled in the **Customize Network Settings** task.
udp 123	Connecting to a Network Time Protocol (NTP) server.

A remote Hardware Management Console needs connectivity to another Hardware Management Console that has connectivity for service and support.

Performance (that is, time to perform an operation) and the availability of the status information and access to the control functions of the Support Element is very dependent on the reliability, availability, and responsiveness of the customer network that interconnects the remote Hardware Management Console with the managed object. A remote Hardware Management Console monitors the connection to each Support Element and attempts to recover any lost connections and can report those connections that cannot be recovered.

Security for a remote Hardware Management Console is provided by the Hardware Management Console user logon procedures in the same way as a local Hardware Management Console. As with a local Hardware Management Console, all communication between a remote Hardware Management Console and each Support Element is encrypted. Certificates for secure communications are provided, and can be changed by the user if wanted (see the **Certificate Management** task).

Note: When you use a browser (see "Web browser requirements" on page 41) to access the Hardware Management Console or Support Element, the Windows operating systems change the way certificates are presented and authenticated to the operating system. If the domain name that you specify on the address bar is not listed in the certificate that is being presented to the client, then the browser informs you that the certificate cannot be authenticated to a trusted source. You can contact your support system for detailed instructions on resolving this issue.

TCP/IP access to the remote Hardware Management Console is controlled through its internally managed firewall and is limited to Hardware Management Console-related functions. Hardware Management Console domain security (see the **Domain Security** task) might be used to isolate systems on a common LAN or to provide additional security. Individual remote users can be configured to have restricted access in the same way as they could be configured on a local Hardware Management Console.

Using a web browser

If you need occasional monitoring and control of managed objects connected to a single local Hardware Management Console, then the web browser is a good choice. An example of using the web browser might be an off-hours monitor from home by an operator or system programmer.

Each Hardware Management Console contains a web server that can be configured to allow remote access for a specified set of users. If a customer firewall exists between the web browser and the local Hardware Management Console, Table 10 on page 40 shows the ports a web browser needs for communication to a Hardware Management Console.

Table 10. Ports used by a web browser for communications to the Hardware Management Console	
Port	**Use**
tcp 443	Secure browser to web server communication
tcp 9950-9959	Proxy support for Single Object Operation

After a Hardware Management Console has been configured to allow web browser access (see the **Customize Console Services** task and the **User Management** task), a web browser gives an enabled user access to all the configured functions of a local Hardware Management Console, except those functions

that require physical access to the Hardware Management Console such as those that access local media. The user interface presented to the remote web browser user is the same as that of the local Hardware Management Console and is subject to the same constraints as the local Hardware Management Console.

The web browser can be connected to the local Hardware Management Console using an encrypted LAN TCP/IP connection (HTTP protocols). Logon security for a web browser is provided by the Hardware Management Console user logon procedures. Certificates for secure communications are provided, and can be changed by the user if wanted (see the **Certificate Management** task).

Performance (that is, time to perform an operation) and the availability of the status information and access to the control functions of the managed objects is very dependent on the reliability, availability, and responsiveness of the network that interconnects the web browser with the local Hardware Management Console. Since there is no direct connection between the web browser and the individual managed objects, the web browser does not monitor the connection to each Support Element, does not do any recovery, and does not report any lost connections; these functions are handled by the local Hardware Management Console.

The web browser system does not require connectivity to support system for service or support and maintenance of the browser and system level is the responsibility of the customer.

If the web address of the Hardware Management Console is specified using the format https://*xxx.xxx.xxx.xxx* (where *xxx.xxx.xxx.xxx* is the IPv4 address) or https://[*xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx*] (where *xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx* is the IPv6 address) and Microsoft Internet Explorer is used as the browser, a host name mismatch message is displayed. To avoid this message, you can choose to do one of the following:

- Using the **Certificate Management** task on the Hardware Management Console, modify the **Subject Alternative Names** property from the Certificate Management window. In the **Modify DNS and IP Address** window, within the list of DNS entries, provide the IP address of the Hardware Management Console that you need in the web address of the Internet Explorer browser.

  Note: The IP address of the Hardware Management Console is usually included in the list of IP Address entries for the Subject Alternative Names property and should not change.
- A browser should be used or a host name should be configured for the Hardware Management Console, using the **Customize Network Settings** task, and this host name should be specified in the web address instead of an IP address. Namely, using the format https://*hostname.domain_name* or https://*hostname* (for example, using https://hmc1.ibm.com or https://hmc1).

Web browser requirements

The Hardware Management Console web browser requires a supported web browser and cookie support in browsers that connects to it. It is required that the web browser uses the HTTP 1.1 protocol and if you are using a proxy server, the HTTP 1.1 protocol is enabled for the proxy connections.

Additionally, pop-ups must be enabled for all Hardware Management Consoles addressed in the browser if running with pop-ups disabled.

The following browsers have been tested and include the recommended minimum Java SE Runtime Environment (JRE) update:

- Microsoft Internet Explorer 11

  Note: The **Compatibility View** option must be disabled. (Select **Tools** from the menu bar, then select **Compatibility View settings**.)
- Microsoft Edge 44
- Firefox ESR 60
- Google Chrome Version 75
- Safari Version 12

Getting ready to use the web browser

Before you can use a web browser to access a Hardware Management Console, you must:

- Configure the Hardware Management Console to allow remote control for specified users.
- For LAN-based connections, know the TCP/IP address of the Hardware Management Console to be controlled, and have properly setup any firewall access between the Hardware Management Console and the web browser.
- Have a valid user ID and password assigned by the Access Administrator for Hardware Management Console web access.

Configuring the Hardware Management Console for web browser access from LAN

1. Log on to the Hardware Management Console with the ACSADMIN default user ID.
2. Open the **User Management** task. The User Management window is displayed.
3. For each user that you want to allow web browser access, select the user ID, then select the Details icon to modify. The User Details window is displayed for that user ID.
4. Select **Allow remote access to the console**, then click **OK**.
5. Open the **Customize Console Services** task. The Customize Console Services window is displayed.
6. Select **Enabled** on the **Remote operation** selection, then click **OK**.

Logging on the Hardware Management Console from a LAN connected web browser

Use the following steps to log in to the Hardware Management Console from a LAN connected web browser:

1. Ensure that your web browser PC has LAN connectivity to the wanted Hardware Management Console.
2. From your web browser, enter the web address of the wanted Hardware Management Console, using the format https://*hostname.domain_name* (for example: https://hmc1.ibm.com), IPv4 address https://*xxx.xxx.xxx.xxx*, or IPv6 address https://[*xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx*].

   If this is the first access of the Hardware Management Console for the current web browser session you can receive a certificate error. This certificate error is displayed if:

   - The web server contained in the Hardware Management Console is configured to use a self-signed certificate and the browser has not been configured to trust the Hardware Management Console as an issuer of certificates, or
   - The Hardware Management Console is configured to use a certificate signed by a Certificate Authority (CA) and the browser has not been configured to trust this CA.

   In either case, if you know that the certificate being displayed to the browser is the one used by the Hardware Management Console, you can continue and all communications to the Hardware Management Console are encrypted.

   If you do not want to receive notification of the certificate error for the first access of any browser session, you can configure the browser to trust the Hardware Management Console or the CA. In general, to configure the browser:

   - You must indicate that the browser will permanently trust the issuer of the certificate, or
   - By viewing the certificate and installing, to the database of trusted CAs, the certificate of the CA that issued the certificate used by the Hardware Management Console.

   If the certificate is self-signed, the Hardware Management Console itself is considered the CA that issued the certificate.
3. When prompted, enter the user name and password assigned by your Access Administrator.

Remote support facility

The Hardware Management Console (HMC) Remote Support Facility (RSF) provides communication to a centralized support system network for hardware problem reporting and service. The types of communication provided include:

- Problem reporting and repair data
- Fix delivery to the service processor and Hardware Management Console
- Hardware inventory data
- On Demand enablement (optional).

These actions are also referred to as *call-home events*.

Some requests use HTTPS protocol and others use encrypted TCP sockets and in either case use a high-grade Transport Later Security (TLS) to encrypt the data that is transmitted. The destination TCP/IP addresses and the host names are published to enable you to update your firewalls to accept the required outgoing connections.

The Remote Support Facility is designed to ensure that the security of your system is not compromised. The following security characteristics are in effect:

- Remote Support Facility requests are always initiated from the Hardware Management Console to support system. An inbound connection is never initiated from the support system.
- All data transferred between the Hardware Management Console and the support system are encrypted in a high-grade TLS encryption.
- When initializing the TLS encrypted connection the Hardware Management Console validates the trusted host by its digital signature issued for the support system.
- Data sent to the support system consists solely of hardware problems and configuration data. No application or customer data is transmitted to the support system.
- The Hardware Management Console can be configured to use a second network card to physically separate a private LAN connection from the Internet-enabled network.
- The Hardware Management Console audit log is updated each time a connection is made with the support system.

A Support Element can call-home service events using any Hardware Management Console (at its release level or higher) that has been configured for outbound connectivity and has been configured as a call-home server when the CPC object was defined to the Hardware Management Console. A Hardware Management Console can call-home its own service events if it is configured for call-home. It is also eligible to use another Hardware Management Console that has been automatically discovered or has been manually configured using the **Customize Outbound Connectivity** task.

To avoid a single point of failure, it is recommended that each Support Element and Hardware Management Console be configured to use multiple call-home servers. The first available call-home server attempts to handle each service event. If the connection or transmission fails with this call-home server the service request is tried again using the other available call-home servers until one is successful or all have been tried.

See the **Customize Outbound Connectivity** task for a detailed description of the options available to configure the Remote Support Facility on the Hardware Management Console.

Prior to configuring the remote support facility

The ability to call-home from the Hardware Management Console (HMC) to the support system requires Hardware Management Console access to an external network. If you are doing this for the first time, you must plan to enable firewalls and evaluate your security policy. Details of the implementation of the Remote Support Facility are available in the *Integrating the Hardware Management Console's Broadband Remote Support Facility into your Enterprise*, SC28-6986. You can find this publication in the **Library** section of Resource Link (www.ibm.com/servers/resourcelink).

The Hardware Management Console can be enabled to connect directly to the Internet (see Figure 9 on page 44) or to connect indirectly from a customer-provided proxy server (see Figure 10 on page 44). The decision about which of these approaches works best for your installation depends on the security and networking requirements of your enterprise.

If a secure connection is used between the customer-provided proxy server and the HMC and the customer-provided proxy server is protected by a X.509 certificate or a chain of X.509 certificates, additional certificate-related configuration might be required on the HMC. By default, the HMC is configured to trust known Certificate Authorities (CAs) such as Verisign, Thawte, and Entrust. If the proxy server is protected by a single self-signed certificate, the HMC must be configured to trust this certificate. If the proxy server is protected by a chain of X.509 certificates, the HMC must be configured to trust at least one of the certificates in the chain. This trust is established within the **Certificate Management** task by selecting **Manage Trusted Signing Certificates**, from the **Advanced** drop-down menu.

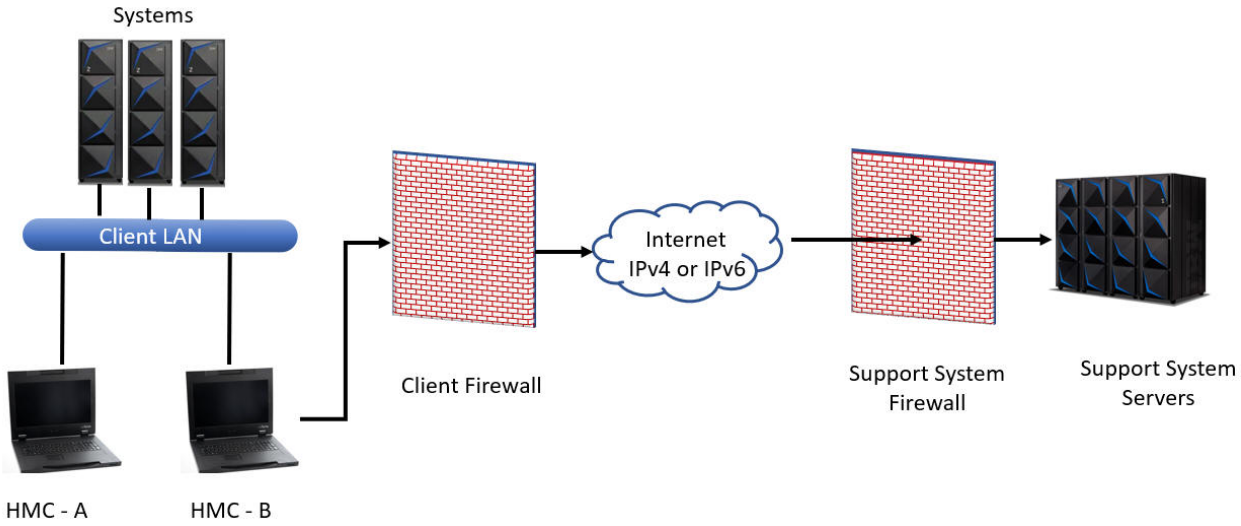


Figure 9. TLS connectivity

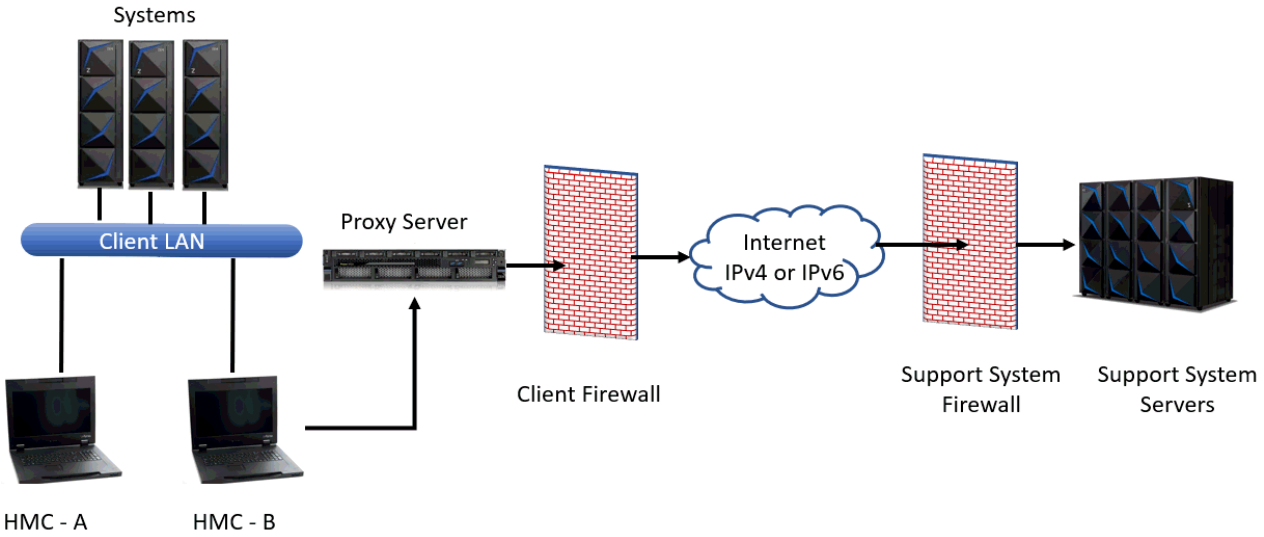


Figure 10. TLS with proxy server connectivity

Refer to the **Outbound Connectivity Settings** from the **Customize Outbound Connectivity** task for information to ensure that your installation has the required firewall rules to enable access.

Audit support for remote syslog

The HMC 2.15.0 release provides a new option for audit support. Previously, Hardware Management Console (HMC) users might use the **Audit and Log Management** task or **Customize Scheduled Operations** task to offload xml and html formatted audit logs, security logs, and console events.

Now, you are able to consolidate a wider variety of logs, such as: security logs, audit logs, console events, hardware messages, BCPii logs, and Web Services API logs. In addition, it offloads directly to centralized servers that use established and industry-common syslog protocols, which can include any syslog enabled log consolidation tool. This eliminates the need for your own automation and goes directly to the consolidation point. The intent of the central logging instance is to collect all relevant messages across the enterprise immediately when they are created by each system to avoid a later removal of these messages and deleted traces of security incidents. (For more information about allowing a syslog enabled endpoint to forward syslog messages to your server, see the documentation that is provided for your syslog enabled log consolidation tool.)

A new HMC task, **Manage Syslog Servers**, is available to configure to forward selected consolidated syslog entries from the HMC or managed Support Elements (SE) to customer-controlled syslog servers. Currently, for the HMCs own remote syslogging configuration, you must configure each additional HMC uniquely or use the **Configure Data Replication** task. For each SEs remote syslogging configuration, any previous SE configurations are shown with the previous customization settings and can be altered if required.

This task allows you to add a syslog server, specifying a host name or IP address and a port where the server is listening for syslog messages. For each server, you can also specify which consoles should send syslog messages to it, and what types of messages each console should send.

Forwarding connectivity from the HMC and SE work differently although they are configured similarly. For each configured remote syslog server on the HMC, the HMC must have connectivity directly to the server. For each configured remote syslog server on the SE, there must be a managing HMC that has connectivity to that server. In this case, if there is such an HMC, the SE discovers it automatically and proxies the forwarding connectivity through it. If an SE cannot locate an HMC with connectivity or if an HMC does not have connectivity for its own logs, then a rolling buffer of logs is kept for forwarding when connectivity is restored. This exploits buffering capability that is built into remote syslog.

LDAP support for user authentication

Lightweight Directory Access Protocol (LDAP) support for Hardware Management Console user authentication allows a Hardware Management Console to be configured to use an LDAP server to perform user ID and password authentication at logon time. The user ID is defined on the Hardware Management Console along with the roles to be given to the user ID (see the **User Management** task for more information). Hardware Management Console settings related to the user ID will continue to reside on the Hardware Management Console, and the LDAP directory will be used to authenticate the user, therefore eliminating the need to store the user ID's password locally. Both SSL and non-SSL connections to the LDAP server are supported.

This function is designed to more easily assist system administrators in the creation of Hardware Management Console user IDs matching existing company user names and to eliminate the need to create and distribute passwords when this is already being managed by an LDAP accessible corporate control mechanism. This can also help meet corporate security guidelines.

IPv6 support

The Hardware Management Console supports the IPv6 protocol. It can communicate by using IPv4 (TCP/IP Version 4), IPv6 (TCP/IP Version 6), or both. The IPv6 protocol was developed by the Internet Engineering Task Force to address the limitations in the existing IPv4 protocol, particularly, the limited number of IPv4 addresses. For more information, see IPv6 (www.ipv6.org).

Whenever you need to specify a TCP/IP address, you have the option of specifying an IPv4 or IPv6 TCP/IP address.

The IPv4 address is written as four decimal numbers, representing four bytes of the IP address, which is separated by periods (for example, `9.60.12.123`).

The IPv6 address can be written as eight groups of four hexadecimal digits, which are separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

Note: For IPv6 simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or you can use a double colon in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

In most cases, you will specify a domain name to avoid having to remember and specify the complicated IPv6 addresses.

Note: The domain name is converted to an IP address if a DNS server has been defined. Use the **Customize Network Settings** task to enable DNS.

Context sensitive help

Context sensitive help allows you to view abbreviated help information for input fields or selectable fields that appear on the task window. To enable this function:

1. Click on the blue **i** that is displayed in the upper right corner of the task window (see Figure 11 on page 46). Every time a new task window opens you need to click **i** to enable context sensitive help.

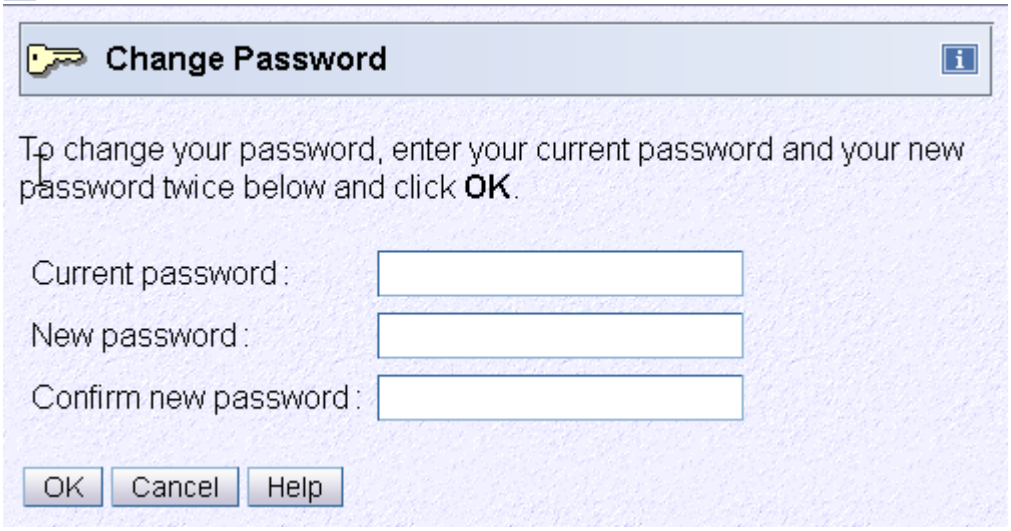


Figure 11. Context sensitive help not enabled

2. Once context sensitive help is enabled the **i** in the upper right corner of the task window changes to an orange **?**. As you place your cursor over the input fields or selectable fields the abbreviated help text is displayed in a small box within the task window (see Figure 12 on page 47). Using the Tab key also allows you to view the help for each field. As you tab to each field, context sensitive help is displayed.

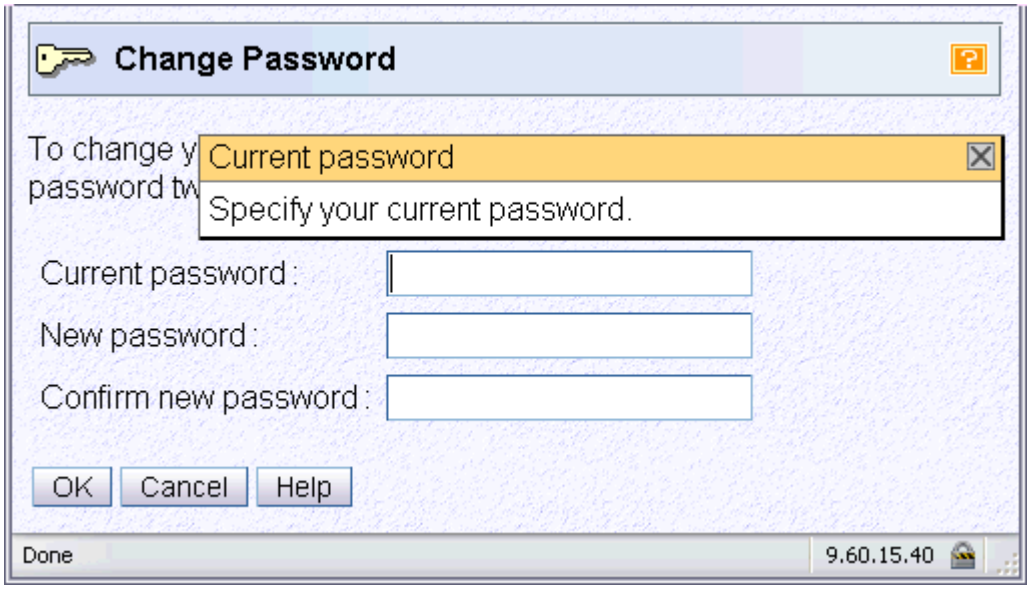


Figure 12. Context sensitive help enabled

- You have the capability to move the help box if it hides some of the information on the task window. As you move your cursor into the help box area the cursor will change from an arrow to a yellow cross arrow. Holding the left mouse button down within the box allows you to drag the box to a more convenient area in the task window.
- You can close the help box by clicking on the **X** in the upper right corner. This will not disable the context sensitive help for the task window, it just removes the help box for the item you were getting help on.
- Scroll bars can be used on the bottom and side of the task window for expanding the task window and allowing more area to view the help box.
- You can continue to perform task options while the context sensitive help is enabled.

3. When you are ready to disable context sensitive help for the task window, click on the **?**.

Disruptive tasks

Some of the Hardware Management Console tasks can be considered *disruptive*. Some of these tasks include:

- **Daily Tasks:** Activate, Deactivate, Reset Normal
- **Recovery Tasks:** Load, Load from Removable Media or Server, PSW Restart, Reset Clear, Reset Normal, Start All, Stop All
- **Change Management Tasks:** Change Internal Code, Engineering Changes (ECs), Product Engineering Directed Changes, Single Step Internal Code Changes, Special Code Load
- **Operational Customization Tasks:** Configure Channel Path On/Off
- **Configuration Tasks:** Manage System Time

Note: Launching the **Stop** task can be considered disruptive under the following circumstances:

- Targeting a system or partitions on which IBM Dynamic Partition Manager (DPM) is enabled.
- Confirming changes from the **Adapter Details** window.

Performing a task on a CPC or CPC image might disrupt its operation. The Disruptive Task Confirmation window that is shown in Figure 13 on page 48 is an example of a disruptive task about to be performed on an object. In this particular case the user profile option to require password verification for disruptive tasks is enabled.

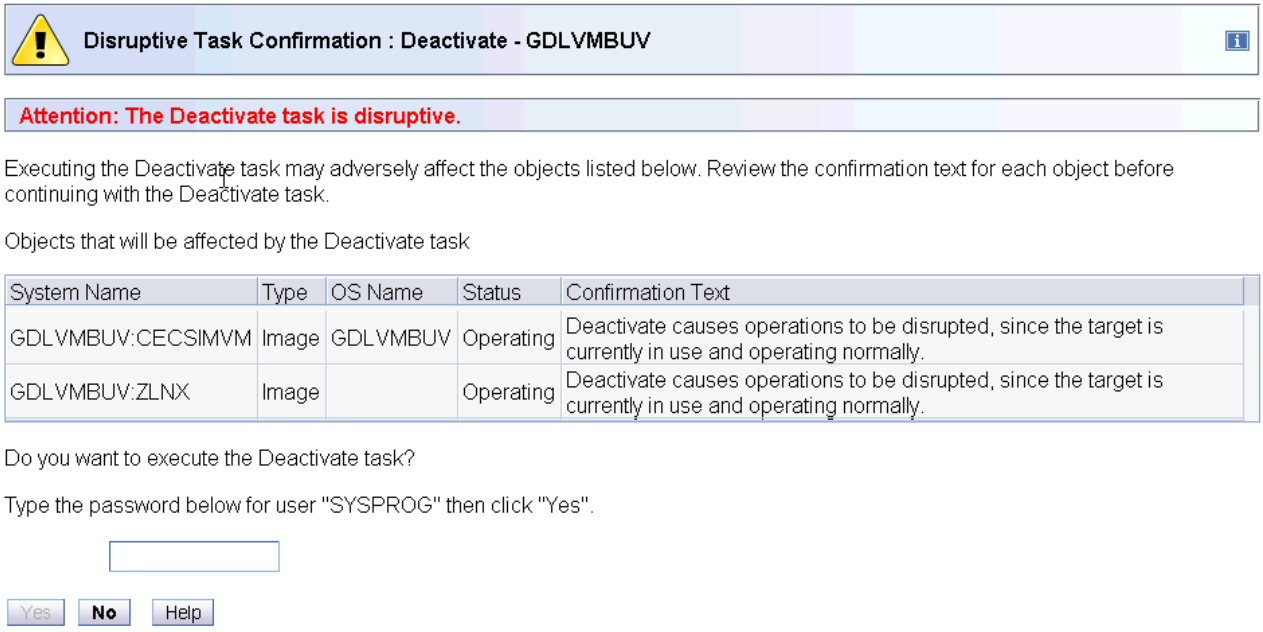


Figure 13. Disruptive task confirmation window

Depending on your user ID, you might not be able to perform the task on the selected object unless you provide required confirmation text or a required password. See the **Disruptive Task Confirmation** task help if you need additional information for this task confirmation window.

Notes:

- For tasks that are performed by using the **Single Object Operation** task, the password that is used for the Disruptive Task Confirmation window depends on if the user ID that was used to log on to the Hardware Management Console is also defined on the Support Element when the **Single Object Operation** task is used. If the user ID also exists on the Support Element, then the password must match the one for the user on the Support Element. If the user ID does not exist on the Support Element, then the password must match the one for the user ID on the Hardware Management Console.
- It is possible that the access administrator did not assign a password requirement for a particular user ID (set by the access administrator in the **User Management** task). In this case, the password input field does not display for that user ID.
- The default SERVICE user ID must always provide a password to proceed with a disruptive task.

Locking an object

You may want to lock an object preventing you from accidentally performing a disruptive task on the object. Unlock the object only when you want to perform a disruptive task on the object.

Note: The **Lockout disruptive task** setting only affects operations from the Hardware Management Console workplace that you are currently working at and its web browser. It does not affect any operations at the Support Element or operations initiated from other Hardware Management Consoles.

About activation profiles

Activation Profiles are required for CPC and CPC image activation. They are used to tailor the operation of a CPC and are stored in the Support Element that is associated with the CPC. There are four types of activation profiles:

Reset:

Every CPC in the processor cluster needs a reset profile to determine the mode in which the CPC licensed internal code will be loaded and how much central storage and expanded storage will be used. The maximum number of reset profiles that are allowed for each CPC is 26.

Image:
If logically partitioned (LPAR) mode has been selected in the reset profile, each partition has an image profile. The image profile determines the number of CPs that the image use and whether these CPs will be dedicated to the partition or shared. It also allows you to assign the amounts of central storage and expanded storage to be used by each partition. Depending on the Support Element model and machine type, the maximum number of image profiles that are allowed for each CPC can be in the range 64 - 255.

Load:
A load profile is needed to define the channel address of the device from which the operating system will be loaded. Depending on the Support Element model and machine type, the maximum number of load profiles that are allowed for each CPC can be in the range 64 - 255.

Group:
A group profile defines the group capacity value that can be customized in determining the allocation and management of processor resources that are assigned to the logical partition in a group. This profile will not contain the name(s) of the LPAR images that make up the group.

Default profiles of each of these types are provided. The default profiles can be viewed (see Figure 14 on page 49), copied to create new profiles, and modified by using the **Customize/Delete Activation Profiles** task.

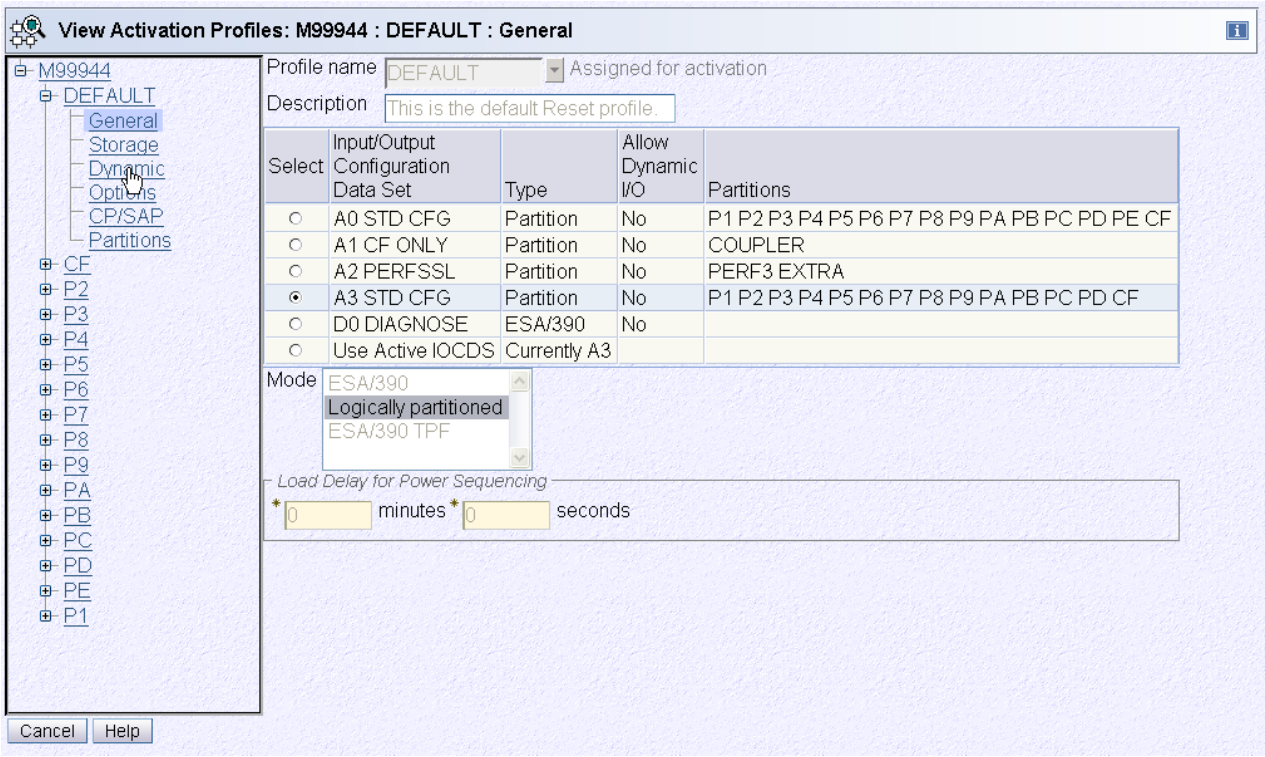


Figure 14. View activation profile default window

The **Activate** task activates the CPC or CPC image. Initially, the Default profile is selected. You might specify an activation profile other than the Default by selecting the desired CPC or CPC image icon in the list.

You can also specify a different activation profile by using the **Change Options...** window as shown in Figure 15 on page 50. You can click **Change Options...** to display a window allowing you to select a different profile name as shown in Figure 16 on page 50. (See **System Details** or **Image Details** for more information.)

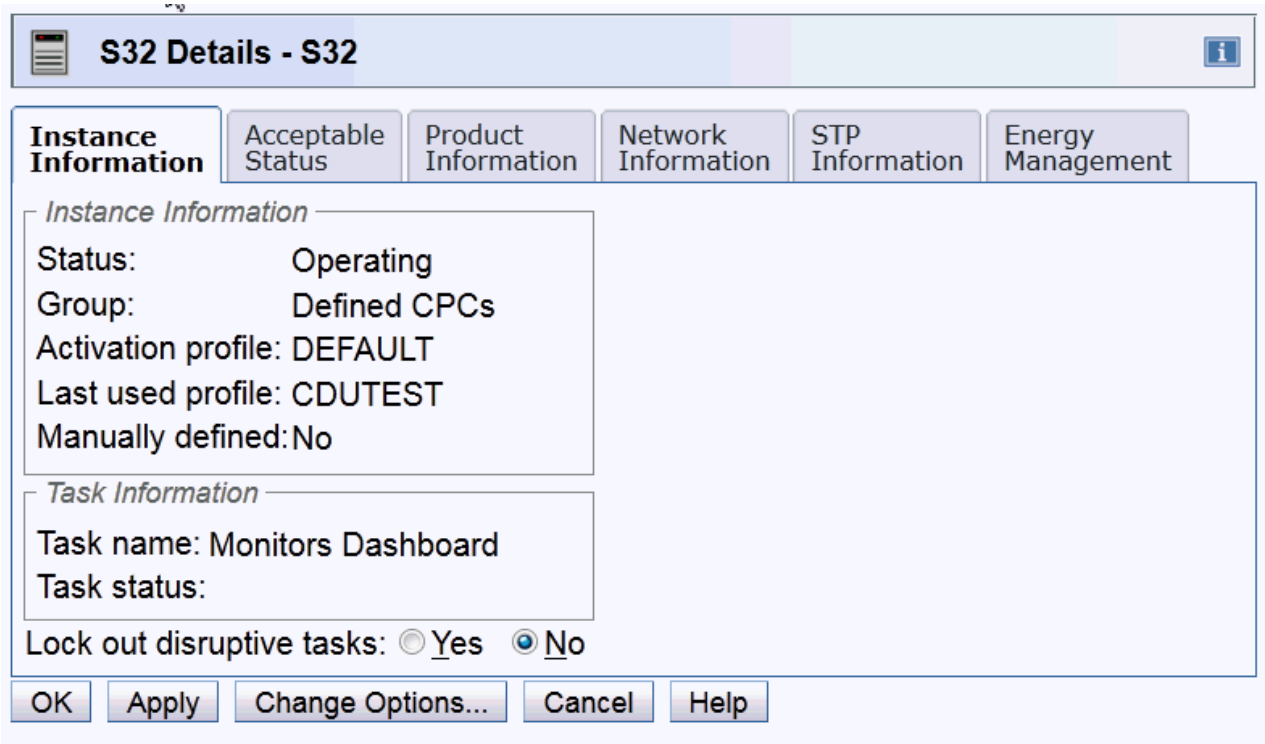


Figure 15. System details window

The activation profile corresponding to the system or image of the Details window is effective when the **Activate** task is performed on the object.

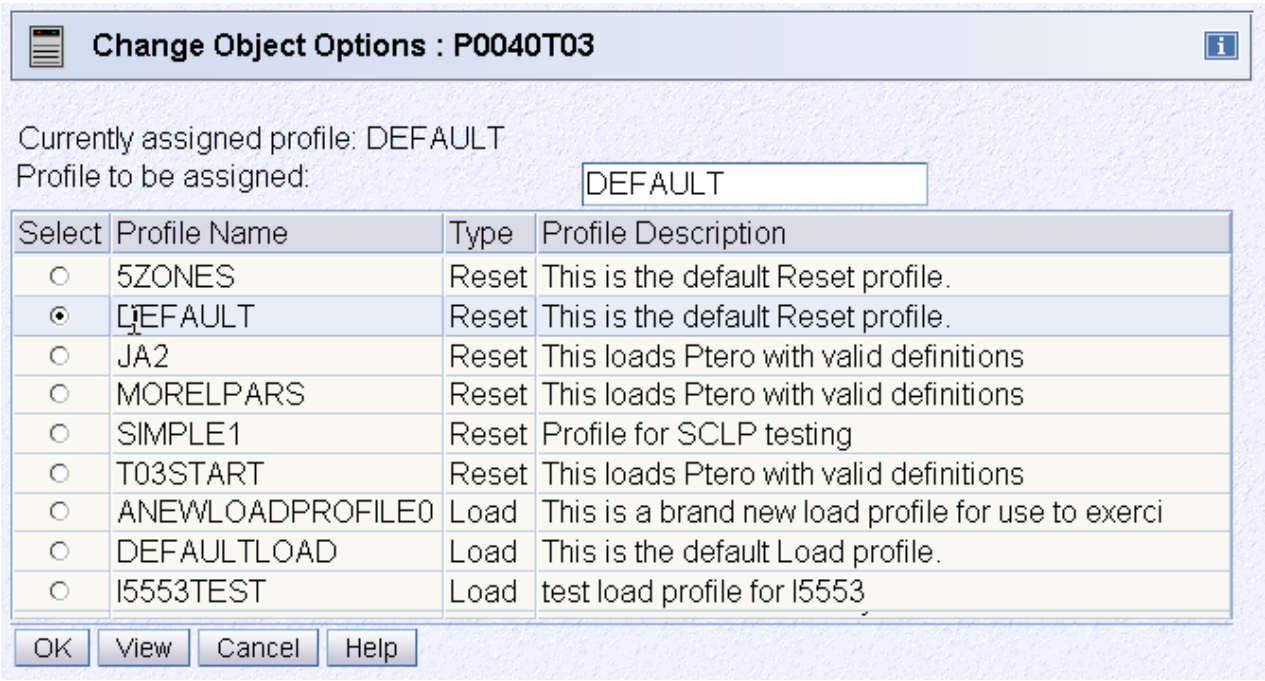


Figure 16. Change object options window

For more detailed information on activation profiles, see the **Customize/Delete Activation Profiles** task.

USB flash memory drive

The USB flash memory drive is a removable writable media available on the Hardware Management Console. There can be more than one USB flash memory drive inserted into the console at one time.

Note: If you are running a task that accesses a USB flash memory drive make sure that you are accessing the correct USB flash memory drive for your task.

Also, running backup from the Hardware Management Console requires a USB flash memory drive inserted in the console. You should install the USB flash memory drive in the Hardware Management Console and do not remove it. This method is essential when you are running a backup scheduled operation.

When you are using a task that requires reading from or writing to removable media, "USB flash memory drive" on page 50 displays a possible Select Media Device task window.

Note: If you are using systems prior to IBM z15™ (z15™), a CD/DVD-ROM can still be an acceptable media device.

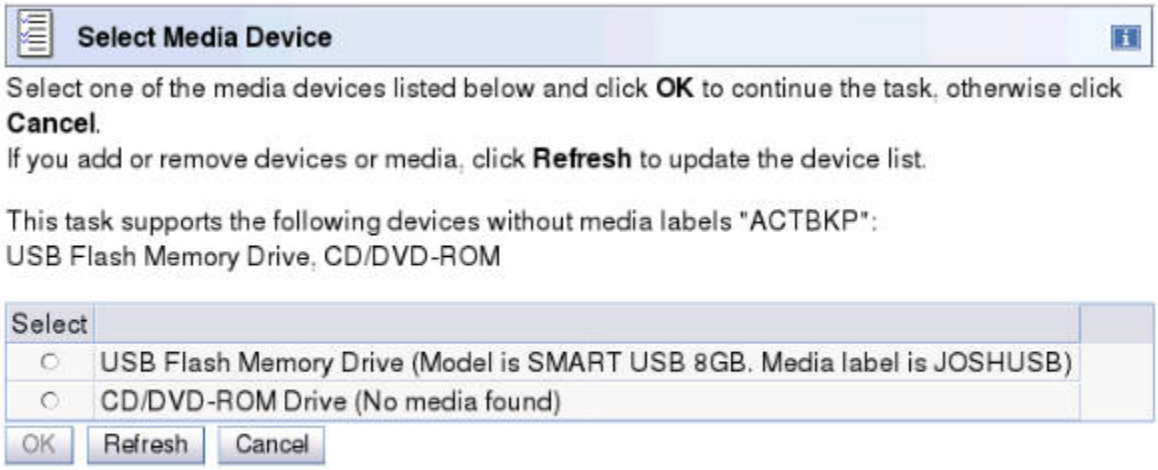


Figure 17. Select media device window

The Hardware Management Console Version 2.12.0 no longer supports a diskette or DVD-RAM media. The available media is USB flash memory drive and CD/DVD-ROM (if one exists).

Notes:

- If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. If the media is not inserted properly, the console does not beep three times and a message is displayed indicating the drive was not added. You need to remove the device and try again.
- Tested virtual file allocation table (VFAT) and second extended file system (EXT2) USB flash memory drives, include IBM packaged SMART drives.
- Only the media that has been supplied by IBM or was formatted on the Hardware Management Console or Support Element should be used in the console.

USB flash memory drive alternatives

There are times when you may not want to use a USB flash memory drive or you cannot use read/write media. The following table lists the tasks that use the USB flash memory drive and identifies a USB flash memory drive alternative the task supports.

Table 11. USB flash memory drive alternatives

Task Name	USB Flash Memory Drive Alternative
Access Removable Media	FTP server, CD/DVD-ROM (if available)
Advanced Facilities	FTP server

Table 11. USB flash memory drive alternatives (continued)

Task Name	USB Flash Memory Drive Alternative
Alternate Support Element Engineering Changes (ECs)	Access to the support system, CD/DVD-ROM (if available)
Archive Security Logs	FTP server
Audit and Log Management	FTP server
Backup Critical Console Data	FTP server
Certificate Management	Use remote browser from workstation, CD/DVD-ROM (if available)
Change Console Internal Code	Read only media option (feature code 0845), FTP server
Change Internal Code	Read only media option (feature code 0845), FTP server
Concurrent Upgrade Engineering Changes (ECs)	Read only media option (feature code 0845)
Copy Console Logs to Media	Transmit service data
Enable FTP Access to Mass Storage Media	CD/DVD-ROM (if available)
Engineering Changes (ECs)	CD/DVD-ROM (if available)
Format Media	Not applicable
Load from Removable Media or Server	FTP server, CD/DVD-ROM (if available)
Manage Print Screen Files	Transmit service data, remotely download image files
Manage Storage Resources > Export World Wide Port Name List	Use remote browser from workstation
Manage Storage Resources > Import Storage Access List	use remote browser from workstation, CD/DVD-ROM (if available)
Mount Virtual Media	Use remote browser from workstation, CD/DVD-ROM (if available)
Offload Problem Analysis Data to Removable Media	Transmit service data
OSA Advanced Facilities	FTP server
Product Support Directed Changes	Product support provides an image for the service representative to burn onto media
Reassign Hardware Management Console	CD/DVD-ROM (if available)
Retrieve Internal Code	Read only media option (feature code 0845), FTP server
Save/Restore Customizable Console Data	Use HMC data replication
Save Upgrade Data	FTP server
Single Step Console Internal Code	FTP server
System Input/Output Configuration Analyzer	FTP server
Transmit Console Service Data	FTP server, Transmit to Remote Support Facility (RSF)
Transmit Service Data	FTP server, Transmit to Remote Support Facility (RSF)

Table 11. USB flash memory drive alternatives (continued)	
Task Name	**USB Flash Memory Drive Alternative**
Transmit Vital Product Data	Send to your service representative
Tree Style User Interface > Table Export Data	See the *HMC Web Services API*, SC27-2638, publication for a programming alternative, use remote browser from workstation
View Security Logs	CD/DVD-ROM (if available)

Server requirements for supporting FTP, SFTP, or FTPS

Use the following guidelines for a Linux operating system server supporting FTP, SFTP, or FTPS.

FTP (File Transfer Protocol)

- Recommend vsftpd 2.0 or higher
- Server must support passive FTP data transfers
- Client firewalls may need to be configured to allow the passive data connection to occur

SFTP (SSH File Transfer Protocol)

- Recommend openssh 4.4 or higher
- Only user name and password client authentication is currently supported
- Client key authentication is not supported

FTPS (FTP Secure)

- Recommend vsftpd 2.0 or higher
- Server must support passive FTP data transfers
- Server must support explicit FTPS connections
- Client firewalls may need to be configured to allow the passive data connection to occur

Coupling Facility Control Code (CFCC) commands

The coupling facility control code (CFCC) commands are described below.

CFDUMP

Purpose:
Forces a non-disruptive dump of the coupling facility.

Syntax:

Access Level:
You can use this command from all access levels.

Required Parameters:
None.

Optional Parameters:
None.

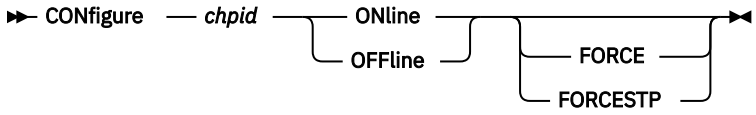
Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the CFDUMP command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

CONFIGURE

Purpose:
Configures channel paths online or offline in the coupling facility (CF) configuration. Trying to configure offline the last CF CHPID will result in a message saying it is the last CHPID. This can be overridden by using the optional FORCE or FORCESTP options.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

chpid
A two-digit hexadecimal address that identifies a channel path to configure online or configure offline.

ONline
Configure online a specified channel path.

OFFline
Configure offline a specified channel path.

Optional Parameters:

FORCE
Used to force the removal of the last coupling link that goes to a particular CF, but will not force the removal of the last coupling link providing STP connectivity.

FORCESTP
Used to force either the removal of the last coupling link that goes to a particular CF, or the removal of the last coupling link providing STP connectivity.

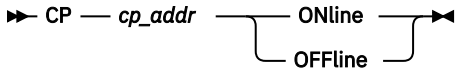
Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the CONFIGURE command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

CP

Purpose:
Configures central processors (CPs) online or offline in the coupling facility configuration.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

cp_addr
A one or two-digit hexadecimal address that identifies a central processor (CP) to configure online or configure offline.

ONline
Configure online a specified central processor.

OFFline
Configure offline a specified central processor.

Optional Parameters:
None.

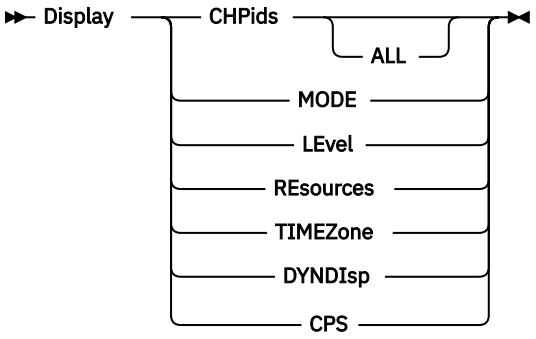
Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the CP command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

DISPLAY

Purpose:
Displays coupling facility resource information.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

CHPids
Displays the channel paths currently configured online to the coupling facility.

MODE
Displays the current coupling facility volatility mode (NONVOLATILE or VOLATILE).

LEvel
Displays the coupling facility release, service level, build date, build time, and facility operational level.

REsources
Displays coupling facility resource information-number of central processors, coupling facility receiver channels, and storage available to the coupling facility.

TIMEZone
Displays the hours east or west of Greenwich Mean Time (GMT) used to adjust timestamps in messages.

DYNDIsp
Displays the dynamic Coupling Facility (CF) dispatching setting. It can be ON, OFF, or THIN.

CPS
Displays the online and standby central processors that are assigned to the Coupling Facility partition.

Optional Parameters:

ALL
Displays the status of all channel paths when entered with the CHPids parameter.

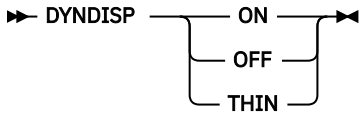
Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the DISPLAY command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

DYNDISP

Purpose:
Turns Dynamic Coupling Facility (CF) Dispatching on or off for a coupling facility logical partition.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

ON
Enables dynamic CF dispatching. This option enables dynamic CF dispatching for a coupling facility logical partition to use it as a backup coupling facility if a primary coupling facility fails. While dynamic CF dispatching is enabled for a coupling facility logical partition:

- It uses minimal processor resources (despite its processing weight) and its unused processor resources are shared with other active logical partitions until it is needed as a backup coupling facility.
- It automatically becomes a backup coupling facility if a primary coupling facility fails.
- It uses its full share of processor resources (determined by its processing weight) only while it is used as a backup coupling facility.

OFF
Disables dynamic CF dispatching. This option disables dynamic CF dispatching for a coupling facility logical partition to use it as a primary coupling facility.

THIN
Enables the use of thin interrupts by the Coupling Facility (CF). This option allows the CF to take advantage of thin interrupt processing to initiate more timely dispatching of the shared CPs or shared ICFs.

Note: This parameter is available beginning with CFCC Release 19.

Optional Parameters:
None.

Restrictions:

- The command is available only with Coupling Facility Control Code Release 4, Service Level 1.03, and subsequent service levels or releases.
- The command is valid only in a coupling facility logical partition.

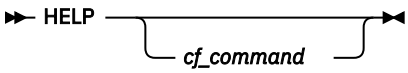
Usage Notes:

- Use the DYNDISP command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

HELP

Purpose:
Displays coupling facility command syntax for the command you enter.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:
None.

Optional Parameters:

cf_command
A coupling facility control code command (other than HELP) whose syntax you want to display. If you enter HELP without an optional parameter, a list of coupling facility control code commands will display.

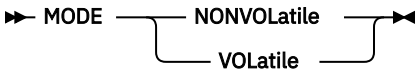
Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the HELP command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

MODE

Purpose:
Defines the volatility mode to be used for coupling facility operation.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

NONVOLatile
Specifies that the coupling facility run in nonvolatile mode and should be used if an uninterruptible power supply (UPS) is available for the processor complex that the coupling facility is running on. The coupling facility does ***not*** monitor the installation or availability of a UPS but maintains a nonvolatile status for the coupling facility.

VOLatile
Specifies that the coupling facility run in volatile mode regardless of the actual volatility state of the coupling facility. Coupling facility storage contents are lost if a power failure occurs or if coupling facility power is turned off. This is the preferred mode for coupling facility operation without an uninterruptible power supply (UPS) backup.

Optional Parameters:
None.

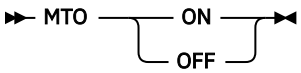
Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the MODE command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

MTO

Purpose:
Turns coupling facility message timeout tracking on or off.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

ON
Turns on message timeout tracking.

OFF
Turns off message timeout tracking.

Optional Parameters:
None.

Restrictions:
Valid only in a coupling facility logical partition.

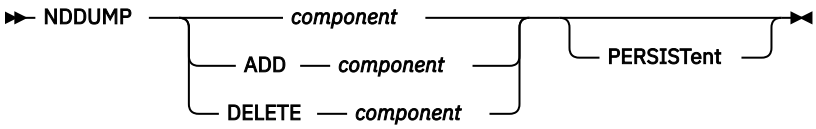
Usage Notes:
Use the MTO command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

NDDUMP

Purpose:
Turns coupling facility nondisruptive dumping on or off for each of the components. The components are listed as required parameters.

Note: Since persistence is not automatic, it must be requested explicitly using the optional PERSISTent keyword.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

component
Use one or more of the following:

ALL
DEFault
TIMETST
TIMEOUT
DUPLEX
SECTEST
SHOOTIOP
XIDETECT
XISECMRB
XISMEC1

XISMEC2

Optional Parameters:

PERSISTent
Used to persist settings across CF activations.

Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the NDDUMP command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task. If you issue an NDDUMP command to modify a setting, the change will persist across CF activations.

If running on VICOM, VM, or when running with no dedicated processors, all NDDUMP settins are defaulted to OFF. When running on hardware with at least one dedicated processor, the currently defaulted ON settings are: DUPLEX, SHOOTIOP, SECTEST, XIDETECT, and XISECMRB.

If the optional parameter PERSISTent is used, then the setting will persist across CF activations. Issuing the NDDUMP DEFault command will restore the current default settings and remove previously persistent settings.

Setting explanations:

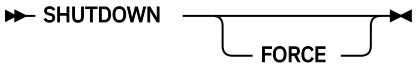
TIMETST - 200 ms timeout
SECTEST - 1 second timeout
TIMEOUT - Duplexing related 250 ms timeout
DUPLEX - Duplexing related dumping
SHOOT_IOP - Shooting IOP
XIDETECT - XI detection phase 1
XISECMRB - XI detection phase 2 overall
XISMEC2 - XI detection phase 2, SMEC = 2
XISMEC1 - XI detection phase 2, SMEC = 1

SHUTDOWN

Purpose:
Ends coupling facility operation and puts all coupling facility logical central processors (CPs) into a disabled wait state, when active structures are not present. If active structures are present, the shutdown operation is canceled and the coupling facility continues operating.

To unconditionally shut down the coupling facility, independent of whether active structures are present, use the optional FORCE parameter. SHUTDOWN FORCE unconditionally ends coupling facility operation and puts all coupling facility logical CPs into a disabled wait state.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:
There are ***no*** required parameters; however, the SHUTDOWN command requires confirmation before it shuts down the coupling facility. A message prompts you to confirm or cancel the shutdown request.

Optional Parameters:

FORCE
Unconditionally ends coupling facility operation and puts all coupling facility logical CPs into a disabled wait state.

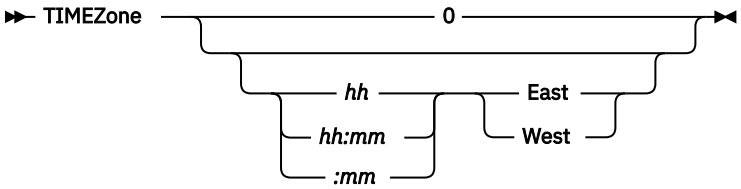
Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the SHUTDOWN command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

TIMEZONE

Purpose:
Sets timezone offset from Greenwich Mean Time (GMT) for a coupling facility.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

0
Specifies that the message timestamps reflect Greenwich Mean Time (GMT).

hh
Specifies the number of hours east or west of Greenwich Mean Time (GMT).

hh:mm
Specifies the number of hours and minutes east or west of Greenwich Mean Time (GMT).

:mm
Specifies the number of minutes east or west of Greenwich Mean Time (GMT).

East
Specifies that time is to be added to Greenwich Mean Time (GMT).

West
Specifies that time is to be subtracted from Greenwich Mean Time (GMT).

Optional Parameters:
None.

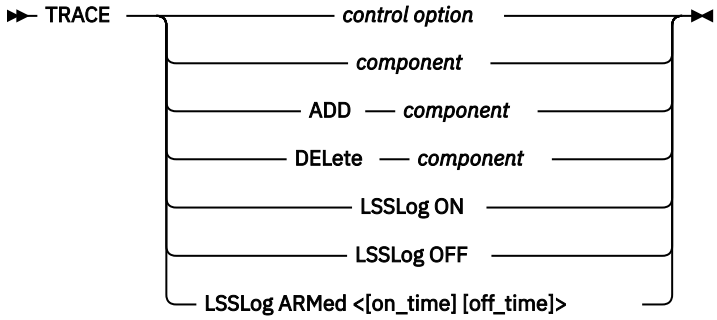
Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the TIMEZONE command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

TRACE

Purpose:
Sets the trace options in the coupling facility.

Syntax:



Access Level:
You can use this command from all access levels.

Required Parameters:

control options

ALL
FULL
WRAp
SAVe
FREeze
OFF
HALf
NOWrap
REStore
UNFreeze

components
Use one or more of the following:

DEFault
LSS
DEBug/trace
GLObal
CAChe
MESsage
CONsole
LISt
DIAgnostics
KERnel
FENce
RECovery
STOrage
DUMp
PERformance
NONvolatility
LISTSubset

Required Parameters (control options):

ALL
Turns tracing on for all components.

FULL
Allows only component traces specified by the full option.

WRap
Allows the trace table to wrap. This is the default setting.

SAVe
Saves the current trace settings so they can be restored.

FREeze
Freezes the trace table.

OFF
Turns tracing completely off.

HALf
Allows only component traces specified by the half option. This is the default setting.

NOWrap
Stops the trace table from wrapping.

REStore
Restores the trace setting to the previously saved setting.

UNFreeze
Unfreezes the trace table.

Optional Parameters:
None.

Restrictions:
Valid only in a coupling facility logical partition.

Usage Notes:
Use the TRACE command from the Hardware Management Console workplace or from a central processor complex (CPC) console session while in the **Operating System Messages** task.

Coupling Facility Control Code (CFCC) messages

The coupling facility control code (CFCC) messages are described below.

CF0001I ***xxxxxxxx* is not a valid CF command.**

Explanation:
You have entered a command (*xxxxxxxx*) that is not an acceptable coupling facility command.

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter an acceptable coupling facility command.

CF0003I **Too many parameters specified for *xxxxxxxx*.**

Explanation:
You have entered more parameters than are allowed for the coupling facility command (*xxxxxxxx*).

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter the command with the appropriate parameters.

CF0004I **Unknown *xxx* parameter - *xxxxxxxx*.**

Explanation:
You have entered an unknown parameter for a coupling facility command (*xxxxxxxx*).

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter the command with the appropriate parameters.

CF0005I A required operand is missing.

Explanation:
You have entered a coupling facility command without a required operand.

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter the command with the required operand.

CF0006I No parameters permitted for *xxxxxxxx* command.

Explanation:
You specified a parameter for command (*xxxxxxxx*) that does not allow parameters.

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter the command without parameters.

CF0009I Licensed Internal Code - Property of IBM

Explanation:
This is the copyright statement for the coupling facility control code.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0010I Coupling Facility is active with *xxxxxx*.

Explanation:
The current number of central processors (CPs), coupling facility receiver (CFR) channel paths, and amount of allocatable storage is displayed.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0011I Coupling Facility is active with *xxxxxx*.

Explanation:
The current number of central processors (CPs), coupling facility receiver (CFR) channel paths, and amount of allocatable storage is displayed. It also displays the amount of SCM storage available.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0075I Last link. Will result in lost connectivity. Use "con *xx* off FORCE" to force chpid offline.

Explanation:
You tried to configure off the last link to the coupling facility. This will result in a loss of connectivity to z/OS®. If this is what you want to do, use the FORCE option on the CONFIGURE OFF command. The command was canceled.

System action:
Coupling facility operation continues

Operator response:
None.

CF0082I If SHUTDOWN is confirmed, share data will be lost.

Explanation:
You entered the SHUTDOWN command. You must confirm or cancel the command to continue.

System action:
Coupling facility operation continues.

Operator response:
Either confirm or cancel the SHUTDOWN request.

CF0090A Do you really want to shut down the Coupling Facility? (YES/NO)

Explanation:
The coupling facility requires that you confirm or cancel your command to shut down the coupling facility.

System action:
The SHUTDOWN command is not accepted unless you confirm your decision to shut down the coupling facility; if you cancel, the SHUTDOWN command is ignored and coupling facility operation continues.

Operator response:
Enter the appropriate response. To confirm a shut down request, you must enter **Yes**.

CF0091I SHUTDOWN command canceled.

Explanation:
You have canceled shut down of the coupling facility or you have unacceptably confirmed your intention to shut down the coupling facility (for example, you entered Y instead of entering Yes).

System action:
The SHUTDOWN command has been canceled; coupling facility operation continues.

Operator response:
None, if your intention was to cancel shut down. If you still want to shut down the coupling facility, re-enter the SHUTDOWN command and appropriately confirm your intention at the prompt.

CF0093I There are structures present in the CF. SHUTDOWN canceled.

Explanation:
The command was canceled. There are structures present in the coupling facility and the FORCE option was not specified.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0099I The message buffer is full. CFCC has lost messages.

Explanation:
The coupling facility message buffer is full and will continue to lose messages until you clear space in the buffer.

System action:
Coupling facility operation continues, but all incoming coupling facility messages are lost.

Operator response:
Delete one or more messages from the Operating System Messages window of the Hardware Management Console Workplace or of a central processor complex (CPC) console session.

CF0100I MODE is VOLATILE.

Explanation:
The coupling facility mode is defined as volatile.

System action:
Coupling facility operation continues.

Operator response:

None.

CF0101I MODE is NONVOLATILE.

Explanation:
The coupling facility volatility mode is defined as nonvolatile.

System action:
Coupling facility operation continues.

Operator response:
None

CF0105I No channel paths are in use.

Explanation:
There are currently no coupling facility channel paths online.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0106I Channel path(s):

Explanation:
The coupling facility channel paths listed are currently online.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0139I CHPID *xx* NOT ONLINE. No action required.

Explanation:
The specified channel path is already offline. No further action is necessary.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0140I CHPID *xx* ONLINE, type CFR|ICFR

Explanation:
You have successfully configured the channel path online.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0141I CFR|ICFR *xx* already ONLINE.

Explanation:
The specified channel path is already online. No further action is necessary.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0142I CFR|ICFR *xx* is ONLINE but not functional.

Explanation:

The channel path was successfully configured online but is in an error state.

System action:
Coupling facility operation continues, but the channel path is not available for use.

Operator response:
Configure the channel path offline, then configure it online. If unsuccessful, determine if there is a channel subsystem problem.

CF0143I CHPID *xx* ONLINE, path is not a CFR.

Explanation:
The command was canceled. This is not a valid CHPID. The CONFIGURE command must be for the CFR CHPID.

System action:
Coupling facility operation continues.

Operator response:
Verify that the CHPID number of the channel path is correct and re-enter the command. If unsuccessful, use the channel monitor of the central processor complex (CPC) console for further error information.

CF0144I CHPID *xx* OFFLINE due to path errors.

Explanation:
An error occurred during initialization of the channel path and the channel path was configured offline.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the command. If unsuccessful, ensure that the channel path is correctly configured.

CF0145I Physical CONFIG ON of path *xx* failed.

Explanation:
The specified channel path has not been configured online. An error occurred during the physical configuration of the channel path.

System action:
Coupling facility operation continues.

Operator response:
Verify that the CHPID number of the channel path is correct and re-enter the command. If unsuccessful, use the channel monitor of the central processor complex (CPC) console for further error information.

CF0146I Physical CONFIG OFF of path *xx* failed, CFR|ICFR remains ONLINE.

Explanation:
The specified channel path has not been logically or physically configured offline and could still be active. An error occurred during the physical deconfiguration of the channel path.

System action:
Coupling facility operation continues; if active, the specified channel path can still send messages.

Operator response:
Verify that the CHPID number of the channel path is correct and re-enter the command. If unsuccessful, use the channel monitor of the central processor complex (CPC) console for further error information.

CF0147I Physical CONFIG OFF of path *xx* failed, CFR|ICFR is not functional.

Explanation:
An error occurred during the physical deconfiguration of the specified channel path and the channel path is not functional.

System action:
Coupling facility operation continues.

Operator response:
Determine if there is a problem in the channel subsystem.

CF0148I Physical CONFIG OFF of path *xx* failed, path is not a CFR.

Explanation:
The command was canceled. This is not a valid CHPID. The CONFIGURE OFF command must be for CFR CHPID.

System action:
Coupling facility operation continues.

Operator response:
Verify that the CHPID number of the channel path is correct and re-enter the command. If unsuccessful, use the channel monitor of the central processor complex (CPC) console for further error information.

CF0149I CHPID *xx* OFFLINE.

Explanation:
You have successfully configured the channel path offline.

System action:
The channel path has been configured offline; coupling facility operation continues.

Operator response:
None.

CF0150I SHUTDOWN is already in progress due to power loss.

Explanation:
You entered a SHUTDOWN command when shut down of the coupling facility is already in progress due to a power loss.

System action:
The additional SHUTDOWN command is not accepted; coupling facility shut down continues.

Operator response:
None.

CF0151I Command cancelled - shutdown in progress due to power loss.

Explanation:
You entered a coupling facility command while shut down is in progress.

System action:
The command is **not** accepted; coupling facility shut down continues.

Operator response:
None.

CF0152I WARNING: No usable CFRs located.

Explanation:
No CFR channel paths are currently configured online and available for use.

System action:
Coupling facility operation continues but no communication to or from systems attached to the coupling facility is possible.

Operator response:
Configure online CFR channel paths to all systems attached to the coupling facility or shut down the coupling facility.

CF0153I ALL is the only valid option for DISPLAY CHPIDS.

Explanation:
You specified a parameter for the Display CHPIDs command that is not allowed.

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter Display CHPIDs to display the channel paths configured online to the coupling facility.

CF0202I ONLINE/OFFLINE parameter missing.

Explanation:
You entered the CONFIGURE command without a required parameter (ONline or OFFline).

System action:
The command was not accepted; coupling facility operation continues.

Operator response:
Re-enter the command with the appropriate parameter.

CF0212I Service Processor interface error. MODE is set to VOLATILE.

Explanation:
Connection to the service processor has been disrupted and the coupling facility volatility mode has been reset to volatile.

System action:
Coupling facility operation continues in volatile mode.

Operator response:
Determine if a problem exists at the support element.

CF0221I Mode (VOL/NONVOL) must be specified with MODE command.

Explanation:
You entered the MODE command without a required parameter.

System action:
The command was not accepted; coupling facility operation continues.

Operator response:
Re-enter the command with the appropriate parameter.

CF0222I Mode is not valid; specify MODE VOL/NONVOL.

Explanation:
You entered the MODE command with an unacceptable required parameter.

System action:
The command was not accepted; coupling facility operation continues.

Operator response:
Re-enter the command with the appropriate parameter.

CF0224I Mode remains unchanged.

Explanation:
You attempted to define a volatility mode that is currently defined for the coupling facility.

System action:
The command was not accepted; coupling facility operation continues.

Operator response:
If the current volatility mode definition is acceptable, no response is required. If not, re-enter the MODE command with the appropriate parameter.

CF0225I CHPID number was not supplied or is not valid.

Explanation:
You attempted to configure a channel path online or offline without specifying either a channel path number or a valid channel path number.

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter the command with the appropriate channel path number.

CF0234I SE interface error. Unable to obtain Channel Path Info.

Explanation:
The channel path information is not available. The DISPLAY CHPIDS ALL command could not read the information from the Support Element.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the command. If unsuccessful, use the channel monitor of the central processor complex (CPC) console for further error information.

CF0250I CF is NONVOLATILE.

Explanation:
Coupling facility volatility status has changed to nonvolatile. The coupling facility will continue to run if a primary power failure occurs.

System action:
Coupling facility operation continues in power save mode.

Operator response:
None.

CF0251I CF is VOLATILE.

Explanation:
Coupling facility volatility status has changed to volatile. Coupling facility storage contents will be lost if a power failure occurs or if coupling facility power is turned off.

System action:
Coupling facility operation continues with coupling facility storage contents exposed to loss if a power outage occurs.

Operator response:
Determine the cause of the power status change.

CF0253I Limited Service Processor function.

Explanation:
Some service processor functions are not currently available to the coupling facility.

System action:
Coupling facility operation continues; however, nonvolatility status and the capability to enter coupling facility control program commands may not be available.

Operator response:
Determine the cause of the Support Element problem.

CF0254I Service Processor is not functional.

Explanation:
The Support Element has failed.

System action:
Coupling facility operation continues; however, some coupling facility functions may **not** be available.

Operator response:
Determine the cause of the Support Element failure.

CF0261I Control Unit *x* CHPID(s) *xx* miscabled.

Explanation:
The control unit *x* is miscabled.

System action:
An incident record is sent to z/OS. Coupling facility operation continues.

Operator response:
None.

CF0262I Control Unit *x* CHPID(s) *xx* not operational.

Explanation:
The control unit *x* and CHPID are not operational.

System action:
An incident record is sent to z/OS. Coupling facility operation continues.

Operator response:
None.

CF0263I Link Degraded - CHPID *xx*

Explanation:
A link error has occurred and is degrading channel performance.

System action:
Coupling facility operation continues.

Operator response:
Determine the cause of the link error.

CF0264I Link Failed - CHPID *xx*

Explanation:
A link error has occurred and prevents further use of the channel.

System action:
The channel is deconfigured.

Operator response:
Determine the cause of the link failure.

CF0265I CFR|ICFR failure detected on path *xx*.

Explanation:
An error occurred on the specified channel path and the channel path was configured offline.

System action:
Coupling facility operation continues.

Operator response:
See message "CF0266I" on page 70.

CF0266I Issue CONFIGURE *xx* ONLINE to recover CFR|ICFR.

Explanation:
An error occurred on the specified channel path and the channel path was configured offline.

System action:
Coupling facility operation continues.

Operator response:
Try configuring the channel path online. If unsuccessful, determine if there is a problem in the channel subsystem.

CF0270I Timezone is Greenwich Mean Time (GMT)

Explanation:
Greenwich Mean Time (GMT) is used to timestamp messages.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0271I **Timezone is *xx* East|West of Greenwich Mean Time (GMT)**

Explanation:
The timezone offset (East or West) of Greenwich Mean Time (GMT) used to timestamp messages is displayed.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0272I **Timezone is missing or is not valid.**

Explanation:
You have **not** specified, or have **not** specified correctly, a required parameter.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the command correctly.

CF0280I **CFCC Release *xx.xx*, service level *xx.xx***
Built on mm/dd/yy at hh:mm:ss
Code Load Features:
Facility Operational Level: *x*

Explanation:
The coupling facility control code level is displayed.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0282I **Not a valid sid.**

Explanation:
You have entered a command with an unacceptable parameter.

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter the coupling facility command with an acceptable parameter.

CF0284I **CP address was not supplied or is not valid.**

Explanation:
You entered the CP command without a central processor (CP) address or you entered an address that was not a hexadecimal value in the range 0-FF.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the command with a valid CP address.

CF0285I **CP *xx* ONLINE.**

Explanation:
The specified central processor is configured online to the coupling facility.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0286I CP *xx* OFFLINE.

Explanation:
The specified central processor is configured offline to the coupling facility.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0287I CP *xx* already ONLINE.

Explanation:
The specified central processor is already configured online to the coupling facility.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0288I CP *xx* already OFFLINE.

Explanation:
The specified central processor does not belong to the coupling facility's configuration.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0289I CP *xx* logically OFFLINE; Physical deconfig failed.

Explanation:
Coupling facility activity has ended on the specified central processor (CP). An error occurred during the deconfiguration of the CP from the coupling facility.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the CP *xx* OFFLINE command. If unsuccessful, use the processor monitor of the central processor complex (CPC) console to determine if a CP problem exists.

CF0290I CP *xx* remains OFFLINE; Physical config failed.

Explanation:
The specified central processor (CP) has *not* been configured online. An error occurred during the configuration of the CP to the coupling facility.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the CP xx ONLINE command. If unsuccessful, use the processor monitor of the central processor complex (CPC) console to determine if a CP problem exists.

CF0291I CP *xx* is not recognized.

Explanation:
The specified central processor (CP) address is not recognized.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the command using a recognized CP address.

CF0292I Unresponsive CP *xx*; Starting CP recovery action.

Explanation:
The specified central processor (CP) has not ended operation. CP recovery has started and should remove the CP from the coupling facility configuration.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0293I CP *xx* is the only CP ONLINE; No action is taken.

Explanation:
The CP *xx* OFFLINE command was not accepted because the specified central processor (CP) is the last CP available to the coupling facility.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0294I Unresponsive CP *xx*; CP remains OFFLINE.

Explanation:
An error occurred during initialization of the specified central processor (CP) and the CP was configured offline from the coupling facility.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the command. If unsuccessful, use the processor monitor of the central processor complex (CPC) console to determine if a CP problem exists.

CF0295I SCLP deconfig failed, path xx is a CPC-critical STP timing link.
"Use 'con *xx* off FORCESTP' to force chpid offline"

Explanation:
You have entered a command with an unacceptable parameter.

System action:
The command is not accepted; coupling facility operation continues.

Operator response:
Re-enter the coupling facility command with the force option.

CF0300I Storage Error - Resource offline.

Explanation:
The coupling facility detected a storage error and stopped using the affected storage.

System action:
Coupling facility operation continues using the remaining storage.

Operator response:
If extensive storage has been taken offline, you may need to repair it to maintain adequate coupling facility operation.

CF0301I Processor Error - Resource offline.

Explanation:
A central processor (CP) error was detected and the coupling facility configured the CP offline.

System action:
Coupling facility operation continues on the remaining CPs.

Operator response:
Determine the cause of the CP failure.

CF0302I Service Processor Error - Critical resource offline.

Explanation:
A service processor failure was detected.

System action:
Coupling facility operation continues; however, service processor functions are not available.

Operator response:
Determine the cause of the Support Element failure.

CF0303I A machine error affected *xxxxxxxx* command processing; re-enter the command if necessary.

Explanation:
A machine error occurred when the last command (*xxxxxxxx*) was processing.

System action:
Coupling facility operation continues; however, processing of the command may **not** have completed.

Operator response:
Re-enter the command.

CF0304I Processor Error - CP *xx* offline.

Explanation:
An error was detected on the specified central processor (CP) and the coupling facility configured the CP offline.

System action:
Coupling facility operation continues on the remaining CPs.

Operator response:
Determine the cause of the CP failure.

CF0400I CF commands: (see Commands)

Explanation:
None.

System action:
Coupling facility operation continues.

Operator response:
None.

Commands
CFDUMP - force non-disruptive dump.
CONFIGURE - take CHPID online or offline.
CP - take CP online or offline.
DISPLAY - show resources.
DYNDISP - set dynamic CF dispatch.
HELP - <command> specific help
MODE - set volatility mode.
MTO - set message timeout tracking.
NDDUMP - set nondisruptive dumping options.
SHUTDOWN - terminate CF operation.
TIMEZONE - set timezone offset.
TRACE - set trace options.

CF0401I Shutdown command format: (see Format)

Explanation:
None.

System action:

Coupling facility operation continues.

Operator response:
None.

Format
SHUTDOWN
Note: When prompted, enter **YES** to confirm or **NO** to cancel.

CF0402I CP command formats: (see Formats)

Explanation:
None.

System action:
Coupling facility operation continues.

Operator response:
None.

Formats
CP *xx* ONline
CP *xx* OFFline
Where *xx* is a hex CP address
Example: `cp 1 offline`

CF0403I Configure command formats: (see Formats)

Explanation:
None.

System action:
Coupling facility operation continues.

Operator response:
None.

Formats
CONfigure *xx* ONline
CONfigure *xx* OFFline
Where *xx* is a hex CHPID number
Example: `configure 11 offline`

CF0405I Timezone command formats: (see Formats)

Explanation:
None.

System action:
Coupling facility operation continues.

Operator response:
None.

Formats
TIMEZone 0
TIMEZone hh East
TIMEZone hh:mm West
TIMEZone :mm West
Where hh (hours) must be in the range 0-23 and mm (minutes) must be in the range 0-59.
Example: `timezone 11:49 east`

CF0406I Display command formats: (see Formats)

Explanation:
None.

System action:

Coupling facility operation continues.

Operator response:
None.

Formats
Display CHPids < ALL >
Required operands: LEvel, MODE, REsources, TIMEZone, DYNDIsp, CPS
Example: `display timezone`

CF0407I Mode command formats: (see Formats)

Explanation:
None.

System action:
Coupling facility operation continues.

Operator response:
None.

Formats
MODE *required operand*
Required operands: NONVOLatile, VOLatile
Example: `mode volatile`

CF0408I DYNDISP command formats: (see Formats)

Explanation:
Used to turn dynamic dispatching on or off.

System action:
Coupling facility operation continues.

Operator response:
None.

Formats
DYNDISP *required operand*
Required operands: ON, OFF, THIN
Example: `dyndisp on`

CF0409I MTO command format: (see Formats)

Explanation:
Used to turn message timeout tracking on or off.

System action:
Coupling facility operation continues.

Operator response:
None.

Formats
MTO *required operand*
Required operands: On, Off
Example: `Mto on`

CF0410I Trace command formats: (see Formats)

Explanation:
None.

System action:
Coupling facility operation continues.

Operator response:
None.

Formats
TRace [control option] [component] [ADD component] [DELete component] [LSSLog ON] [LSSLog OFF] [LSSLog ARMed <[on_time]< off_time >>]
Control options:
ALL, FULL, WRAp, SAVe, FREeze, OFF, HALf, NOWrap, REStore, UNFreeze
Components (one or more of the following):
DEFault, LSS, DEBug/trace, GLObal, CAChe, MESsage, CONsole, LISt, DIAgnostics, KERnel, FENce, RECovery, STOrage, DUMp, PERformance, NONvolatility, LISTSubset
Examples:
```
trace add cache kernel fence
trace lsslog armed 10 31
```

CF0411I Nddump command formats: (see Formats)

Explanation:
None.

System action:
Coupling facility operation continues.

Operator response:
None.

Formats
NDdump [control option] [component] [ADD component] [DELete component]
Control options: OFF
Components (one or more of the following):
ALL, DEFault, TIMETST, TIMEOUT, DUPLEX, SECTEST, SHOOTIOP, XIDETECT, XISECMRB, XISMEC1, XISMEC2
Example: `nddump add timeout`

CF0412I CFdump command format: (see Format)

Explanation:
None.

System action:
Coupling facility operation continues.

Operator response:
None.

Format
CFDUMP
Example: `cfdump`

CF0500I (ON/OFF) must be specified with DYNDISP command.

Explanation:
You must specify either **ON** or OFF with the **DYNDISP** command.

System action:
Command not executed. Coupling facility operation continues.

Operator response:
None.

CF0501I Parameter is not valid; specify DYNDISP ON/OFF.

Explanation:
An incorrect parameter was specified for the DYNDISP command.

System action:
Command not executed. Coupling facility operation continues.

Operator response:
None.

CF0502I Dynamic CF Dispatching Enablement remains unchanged.

Explanation:
You specified a setting that the dynamic dispatching is already set to. The enablement setting is not changed.

System action:
Command not executed. Coupling facility operation continues.

Operator response:
None.

CF0504I DYNDISP command canceled. Command not valid in ICMF mode.

Explanation:
The command was canceled. The command is not allowed when the CF is running in ICMF mode.

System action:
Command not executed. Coupling facility operation continues.

Operator response:
None.

CF0505I DYNDISP command canceled. Command has no effect with dedicated CPs.

Explanation:
The DYNDISP command was canceled. The command has no effect when the CF partition contains only dedicated processors.

System action:
Command not executed. Coupling facility operation continues.

Operator response:
None.

CF0506I Dynamic CF Dispatching is Disabled.

Explanation:
Dynamic CF dispatching has been disabled.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0507I Dynamic CF Dispatching is Enabled and currently active.

Explanation:
Dynamic CF dispatching has been disabled.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0508I Dynamic CF Dispatching is Enabled, but not active.

Explanation:
Dynamic CF dispatching has been enabled, but is not currently active.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0509I DYNDISP command canceled - Dynamic CF Dispatching cannot be disabled when CF contains both dedicated and shared processors.

Explanation:
Dynamic CF dispatching cannot be disabled when the CF partition is configured with both dedicated and shared processors.

System action:
Command canceled. Coupling facility operation continues.

Operator response:
None.

CF0510I DYNDISP command canceled - The 'hardware' does not support THINinterrupts.

Explanation:
The DYNDISP command was canceled. The command has no effect when the hardware does not support thin interrupts.

System action:
Command not executed. Coupling facility operation continues.

Operator response:
None.

CF0511I Dynamic CF Dispatching is THINinterrupts and currently active.

Explanation:
Dynamic CF dispatching is enabled for thin interrupts.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0512I Dynamic CF Dispatching is THINinterrupts.

Explanation:
The current setting for Dynamic CF dispatching is thin interrupts.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0550I Nddump option accepted.

Explanation:
The non-disruptive dumping controls have been changed.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0551I Invalid dump format or command.

Explanation:
The non-disruptive dumping controls are not changed.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the coupling facility command with a valid format or command.

CF0552I Invalid dump parameter - *xxxx*.

Explanation:
The non-disruptive dumping controls are not changed.

System action:
Coupling facility operation continues.

Operator response:
Re-enter the coupling facility command with a valid parameter.

CF0553I Active Non-disruptive dumping controls.

Explanation:
The non-disruptive dumping controls are displayed.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0600I Display CPS command did not work. Please reissue the command.

Explanation:
The service element did not execute the command. Try reissuing the command.

System action:
Command canceled. Coupling facility operation continues.

Operator response:
None.

CF0601I CPU Information:

Explanation:
Information for all of the processors assigned to the CF partition is displayed.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0602I CPS command canceled - Command is not valid in a z/VM® environment.

Explanation:
The display CPU information command is not valid when the CF is running as a z/VM guest.

System action:
Command is canceled. Coupling facility operation continues.

Operator response:
None.

CF0603I CPU Other Information:

Explanation:
Displays all configured CPs and whether they are shared or dedicated.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0700I MTO (ON/OFF) must be specified with MTO command.

Explanation:
You must specify either ON or OFF with the MTO command.

System action:
Command not executed. Coupling facility operation continues.

Operator response:

None.

CF0701I Parameter is not valid; specify MTO ON/OFF.

Explanation:
An incorrect parameter was specified for the MTO command.

System action:
Command not executed. Coupling facility operation continues.

Operator response:
None.

CF0702I The MTO table is Enabled.

Explanation:
Message timeout tracking was enabled.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0703I The MTO table is Disabled.

Explanation:
Message timeout tracking was disabled.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0800I A non-disruptive dump was taken by the CF.

Explanation:
A non-disruptive dump was taken by the CF.

System action:
Coupling facility operation continues.

Operator response:
None.

CF0801I A non-disruptive structure dump was taken by the CF.

Explanation:
A non-disruptive structure dump was taken by the CF.

System action:
Coupling facility operation continues.

Operator response:
None.

Audit, Event, and Security Log Messages

Log messages

The log messages included in this section can be applicable to the following consoles:

- IBM Z (Z) Hardware Management Console (HMC) and Support Element (SE)
- IBM LinuxONE (LinuxONE) Hardware Management Console (HMC) and Support Element (SE)
- Trusted Key Entry (TKE) workstation

The following log messages are new for Version 2.15.0:

- “2097” on page 252
- “2098” on page 252
- “2099” on page 252
- “6072” on page 320
- “6073” on page 320
- “6111” on page 320
- “6112” on page 320
- “6120” on page 320
- “6121” on page 321
- “6122” on page 321
- “6123” on page 321
- “6124” on page 321
- “6125” on page 321
- “6132” on page 321
- “6133” on page 321
- “6140” on page 322
- “6141” on page 322
- “6142” on page 322
- “6143” on page 322
- “6144” on page 322
- “6145” on page 323

Messages 1-100

1	**Start was requested.**
2	**Stop was requested.**
3	**Multisystem channel communication unit 0 power-on reset has occurred.**
4	**Multisystem channel communication unit 1 power-on reset has occurred.**
5	**Multisystem channel communication unit 2 power-on reset has occurred.**
6	**Multisystem channel communication unit 3 power-on reset has occurred.**
7	**Multisystem channel communication unit (MCCU) 0 diagnostic power-on reset occurred.**
8	**Multisystem channel communication unit (MCCU) 1 diagnostic power-on reset occurred.**
9	**Multisystem channel communication unit (MCCU) 2 diagnostic power-on reset occurred.**
10	**Multisystem channel communication unit (MCCU) 3 diagnostic power-on reset occurred.**
11	**Processing unit is powered on.**
12	**Processing unit is powered off.**
13	**Load was successful for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

14	**Load failure occurred for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

15	**Load was cancelled for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

16	**System check.**
17	**A scheduled operation started.**
18	**Input/output (I/O) processor power-on reset has ended.**
19	**Activation has started.**
20	**Deactivation has started.**
21	**Power-on reset was started.**
22	**Channel power-on reset was started.**
23	**Input/output (I/O) processor power-on reset was started.**
24	**Battery operated clock old time.**
25	**Battery operated clock new time.**
26	**Manual problem analysis was started.**
27	**Automatic problem analysis was started.**
28	**The following internal code fixes were activated: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

29	**The following internal code fixes were deactivated: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

30	**The following internal code changes were installed: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

31	**The following internal code changes were activated: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

32	**The following internal code changes were removed: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

33	**The following internal code changes were accepted: *{0}*.**

Explanation

Substitution variables are:

*{0}*EC number and MCL level of the change

34	**An internal code change failure occurred.**
35	**System exerciser was started.**
36	**System exerciser has ended.**
37	**A logon occurred in service representative mode.**
38	**A logon occurred in product engineering mode.**
39	**A load will be attempted for system *{0}* with the following options: type *{1}*, store status *{4}*, address *{2}*, parameter *{3}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load type
*{2}*Load address
*{3}*Load parameter
*{4}*Load store status value

40	**A logoff occurred.**
41	**Manual problem analysis has ended.**
42	**Automatic problem analysis has ended.**
43	**Problem analysis results were displayed to the customer.**
44	**Problem analysis service information was transmitted to the Service Support System.**
45	**Machine check recovery was started.**
46	**Machine check recovery has ended.**
47	**Multisystem channel communication unit 0 diagnostics ran successfully.**
48	**Multisystem channel communication unit 1 diagnostics ran successfully.**
49	**Multisystem channel communication unit 2 diagnostics ran successfully.**
50	**Multisystem channel communication unit 3 diagnostics ran successfully.**
51	**The console application was initialized.**
52	**The Hardware Management Console Application (HWMCA) console was disabled.**
53	**Storage device or tape adapter customization change request.**
54	**Storage device or tape adapter customization change request.**
55	**Workstation adapter customization change request.**

56	**Workstation adapter customization change request.**
57	**S/370 channel customization change request.**
58	**Input/output (I/O) communication adapter customization change request.**
59	**Input/output (I/O) communication adapter customization change request.**
60	**Input/output (I/O) communication adapter customization change request.**
61	**ASCII adapter customization change request.**
62	**IEEE 802.3 adapter customization change request.**
64	**Transmission Control Protocol/Internet Protocol (TCP/IP) customization change request.**
65	**Request for price quotation adapter customization change request.**
66	**Request for price quotation adapter customization change request.**
67	**Request for price quotation adapter customization change request.**
68	**Request for price quotation adapter customization change request.**
69	**Request for price quotation adapter customization change request.**
70	**Input/output (I/O) adapter customization change request.**
71	**Input/output (I/O) adapter customization change request.**
72	**Input/output (I/O) adapter customization change request.**
73	**Input/output (I/O) adapter customization change request.**
74	**Input/output (I/O) adapter customization change request.**
75	**Input/output (I/O) adapter customization change request.**
76	**Redundant bit was set.**
77	**Backup battery power is active.**
78	**Power is restored.**
79	**Remote console was invoked.**
80	**Operations management is active.**
81	**User profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*User profile name

82	**User profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*User profile name

83	**The vital product data was rebuilt.**
84	**A request to send configuration data to the Service Support System was put on the remote support queue.**
85	**Configuration data and vital product data were restored from diskette.**
86	**An upgrade installation operation was started.**

87	**Configuration data was changed to an edit operation.**
88	**An input/output (I/O) controller was power-on reset.**
89	**An input/output (I/O) controller was power-on reset.**
90	**An input/output (I/O) controller was power-on reset.**
91	**An input/output (I/O) controller was power-on reset.**
92	**An input/output (I/O) controller was power-on reset.**
93	**An input/output (I/O) controller was power-on reset.**
94	**An input/output (I/O) controller was power-on reset.**
95	**An input/output (I/O) controller was power-on reset.**
96	**An input/output (I/O) controller was power-on reset.**
97	**An input/output (I/O) controller was power-on reset.**
98	**An input/output (I/O) controller was power-on reset.**
99	**An input/output (I/O) controller was power-on reset.**
100	**An input/output (I/O) controller was power-on reset.**

Messages 101-200

101	**An input/output (I/O) controller was power-on reset.**
102	**An input/output (I/O) controller was power-on reset.**
103	**An input/output (I/O) controller was power-on reset.**
104	**An input/output (I/O) controller was power-on reset.**
105	**An input/output (I/O) controller was power-on reset.**
106	**An input/output (I/O) controller was power-on reset.**
107	**An input/output (I/O) controller was power-on reset.**
108	**An input/output (I/O) controller was power-on reset.**
109	**An input/output (I/O) controller was power-on reset.**
110	**An input/output (I/O) controller was power-on reset.**
111	**Activation was successful.**
112	**Activation has failed.**
113	**Deactivation was successful.**
114	**Deactivation has failed.**
115	**The *{1}* profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Profile type

116	**The *{1}* profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Profile type

117	**The *{1}* profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Profile type

118	**The *{1}* profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Profile type

119	**A scheduled operation completed successfully.**
120	**A scheduled operation failed.**
121	**A scheduled operation was added.**
122	**A scheduled operation was attempted but did not start.**
123	**A logon occurred in operator mode.**
124	**A logon occurred in advanced operator mode.**
125	**A logon occurred in access administrator mode.**
126	**A logon occurred in system programmer mode.**
127	**Setup installation options operation started.**
128	**Setup installation options operation ended.**
129	**The keylock position is secure.**
130	**The keylock position is manual.**
131	**The keylock position is normal.**
132	**The keylock position is auto.**
133	**Internal code change was retrieved.**
134	**Uninterruptible power supply (UPS) battery is active.**
135	**Processor battery is active.**
136	**Local unsuccessful logon detected.**
137	**Operations management unsuccessful logon detected.**
138	**Remote operations unsuccessful logon detected.**
139	**An automatic dial attempt was made.**
140	**A manual dial attempt was made.**
141	**A call attempt was successful.**
142	**A call attempt was not successful.**
143	**A failure alert was generated.**
144	**Failure alert information was transmitted to the central site.**

145	**Events in the event log were deleted.**
146	**Due to event log space limitations, obsolete events were deleted.**
147	**A remote console session terminated successfully from system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

148	**A remote console session terminated with an error condition from system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

149	**Line disconnect key was requested.**
150	**A remote connection was attempted.**
151	**A remote connection failed.**
152	**A remote connection was successful.**
153	**Automatic activation was enabled.**
154	**Automatic activation was disabled.**
155	**Multisystem channel communication unit 0 successfully installed.**
156	**Multisystem channel communication unit 1 successfully installed.**
157	**Multisystem channel communication unit 2 successfully installed.**
158	**Multisystem channel communication unit 3 successfully installed.**
159	**Multisystem channel communication unit 0 successfully removed.**
160	**Multisystem channel communication unit 1 successfully removed.**
161	**Multisystem channel communication unit 2 successfully removed.**
162	**Multisystem channel communication unit 3 successfully removed.**
163	**Multisystem channel communication unit 0 configuration changed.**
164	**Multisystem channel communication unit 1 configuration changed.**
165	**Multisystem channel communication unit 2 configuration changed.**
166	**Multisystem channel communication unit 3 configuration changed.**
167	**Write of input/output configuration data set (IOCDS) *{0}* in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS identifier

168	**Stand alone build of input/output configuration data set (IOCDS) *{0}* in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS identifier

169 **Diskette import of configuration source *{0}* started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

170 **Tape import of configuration source *{0}* started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

171 **Edit of configuration source *{0}* is in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS name

172 **Disassemble of input/output configuration data set (IOCDS) *{0}* to configuration source.**

Explanation

Substitution variables are:

*{0}*IOCDS name

173 **Export of configuration source *{0}* to system tape started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

174 **S/370 check stop occurred.**

175 **A scheduled operation failed to start within the specified time window.**

176 **The system clock has changed.**

177 **Cable reconnected.**

178 **Power-on reset has ended.**

179 **An automatic dial to *{0}* was attempted. The dial operation failed.**

Explanation

Substitution variables are:

*{0}*Phone number

190 **Problem analysis found, but did not report, a problem identical to an open problem.**

191 **Local unsuccessful logon threshold exceeded.**

192 **Operations management unsuccessful logon threshold exceeded.**

193 **Remote operations unsuccessful logon threshold exceeded.**

194 **The following internal code changes were deleted: *{0}*.**

Explanation

Substitution variables are:

*{0}*Engineering change numbers

195 **Problem analysis found nothing to report.**

196 **Write of input/output configuration data set (IOCDS) *{0}* in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS name

197 **Stand-alone build of input/output configuration data set (IOCDS) *{0}* in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS identifier

198 **Diskette import of configuration source *{0}* started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

199 **Tape import of configuration source *{0}* started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

200 **Edit of configuration source *{0}* is in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS name

Messages 201-300

201 **Disassemble of input/output configuration data set (IOCDS) *{0}* to configuration source.**

Explanation

Substitution variables are:

*{0}*IOCDS name

202 **Export of configuration source *{0}* to system tape started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

203 **An automatic dial to *{0}* was attempted. The dial operation was successful.**

Explanation

Substitution variables are:

*{0}*Telephone number

204 **S/390 check stop occurred.**

205 **A scheduled operation failed to start within the specified time window.**

206 **The system clock has changed.**

207 **Cable reconnected.**

208 **Power-on reset has ended.**

209 **Input/output (I/O) processor power-on reset for *{0}* was started on channel path identifier *{1}*.**

Explanation

Substitution variables are:

*{0}*CPC name
*{1}*CHPID type

210 **Input-output (I/O) processor power-on reset for *{0}* was completed on channel path identifier *{1}*.**

Explanation

Substitution variables are:

*{0}*CPC name
*{1}*CHPID type

211 **Customization change request for Input-output (I/O) processor *{0}* on channel path identifier *{1}*.**

Explanation

Substitution variables are:

*{0}*IOP name
*{1}*CHPID type

213 **Activation has started using the *{1}* profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile type
*{1}*Profile name

214 **Deactivation has started for *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

215 **An automatic dial to *{0}* was attempted. The dial operation failed.**

Explanation

Substitution variables are:

*{0}*Telephone number

216 **User *{0}* has logged on in *{1}* mode.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*User role

217 **Channel path swap completed for channels *{0}* and *{1}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

218 **Reset of swapped channel paths completed for channels *{0}* and *{1}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

219 **Channel path swap for channels *{0}* and *{1}* will be active after power-on reset.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

220 **Reset of swapped channel paths for channels *{0}* and *{1}* will be active after power-on reset.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

221 ***{0}* was made the active input/output configuration data set (IOCDS).**

Explanation

Substitution variables are:

*{0}*IOCDS identifier

222 **Input/output configuration data set (IOCDS) *{0}* written to *{1}* by *{2}*.**

Explanation

Substitution variables are:

*{0}*IOCDS name
*{1}*IOCDS identifier
*{2}*Function, such as IOCP

223 **Hardware configuration definition (HCD) data set written.**

224 **Channel path identifier *{0}* entered the reserved state.**

Explanation

Substitution variables are:

*{0}*CHPID type

225 **Channel path identifier *{0}* entered the standby state.**

Explanation

Substitution variables are:

*{0}*CHPID type

226 **Channel path identifier *{0}* entered the online state.**

Explanation

Substitution variables are:

*{0}*CHPID type

227 **Dynamic input/output (I/O) reconfiguration started.**

228 **Dynamic input/output (I/O) reconfiguration ended.**

229 **Activation started for system *{0}* using profile *{1}*.**

Explanation

Substitution variables are:

*{0}*Target name
*{1}*Profile name

230 **Activation completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

231 **Activation failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

232 **Deactivation started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

233 **Deactivation completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

234 **Deactivation failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

235 **System reset started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

236 **System reset completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

237 **System reset failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

238 **Activate request was initiated for system *{0}* using profile *{1}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name
*{1}*Profile name

239 **Activate request has ended successfully for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

240 **Activate request has ended with failure for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

241 **Deactivate request was initiated for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

242 **Deactivate request has ended successfully for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

243 **Deactivate request has ended with failure for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

244 **System reset started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

245 **System reset completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

246 **System reset failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

247 **A start operation completed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

248 **A start operation failed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

249 **A stop operation completed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

250 **A stop operation failed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

251 **A restart operation completed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

252 **A restart operation failed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

253 **Engineering change (EC) upgrade started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

254 **Engineering change (EC) upgrade completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

255 **Engineering change (EC) upgrade failed.**

256 **System check stop.**

257 **Logon by *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

258	**Logoff.**
259	**Load successful *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

260	**Power-on successful.**
261	**Power-off started.**
262	**System reset successful.**
263	**Battery operated clock was set.**
264	**Activate successful *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

265	**Deactivate successful *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

266	**Midnight at processor controller.**
267	**Expanded storage in check stopped state.**
268	**Partition *{0}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*Image name

269	**Channel subsystem failure.**
270	**Central storage failure.**
271	**Expanded storage failure.**
272	**System complex (Sysplex) timer failure.**
273	**Link failure on channel path identifier (CHPID) *{0}*.**

Explanation

Substitution variables are:

*{0}*CHPID type

274	**Processor *{0}* has entered disabled wait state (PSW *{1}*).**

Explanation

Substitution variables are:

*{0}*Processor number
*{1}*PSW number

275 **Partition *{0}* processor *{1}* has entered disabled wait (PSW *{2}*).**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Processor number
*{2}*PSW number

276 **Program status word (PSW) loop not valid on processor *{0}* (*{1}*).**

Explanation

Substitution variables are:

*{0}*Processor number
*{1}*Target number

277 **Logically partitioned mode failure.**

278 **Logically partitioned mode initialization complete.**

279 **Logically partitioned mode initialization failure.**

280 **Vary Processor *{0}* command received.**

Explanation

Substitution variables are:

*{0}*Processor number

281 **Vary vector element *{0}* command received.**

Explanation

Substitution variables are:

*{0}*Vector number

282 **Processor *{0}* failed to initialize.**

Explanation

Substitution variables are:

*{0}*Processor number

283 **Processor *{0}* in check stopped state *{1}*.**

Explanation

Substitution variables are:

*{0}*Processor number
*{1}*Check stopped state

284 **CHPIDs *{0}*-*{1}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

285 **CHPID *{0}* deconfigured during reset *{1}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Reset state

286 **Vector element *{0}* failed.**

Explanation

Substitution variables are:

*{0}*Vector number

287 **Physical processor *{0}* logically check stopped.**

Explanation

Substitution variables are:

*{0}*Processor name

288 **Time of day (TOD) clock failure.**

289 **Cryptographic feature failure *{0}*.**

Explanation

Substitution variables are:

*{0}*Failure reason

290 **Dynamic storage access link failure.**

291 **Processor controller error occurred.**

292 **Service processor damage machine check occurred.**

293 **Cryptographic feature sensor activated.**

294 **Operator console not operational *{0}*.**

Explanation

Substitution variables are:

*{0}*Console name

295 **Call authorization requested.**

296 **Outbound remote support call started.**

297 **Outbound remote support call delayed for *{0}* hours.**

Explanation

Substitution variables are:

*{0}*Number of hours

298	**Service call accepted, support group notified.**
299	**Remote support call completed.**
300	**Remote support call failed.**

Messages 301-400

301	**Remote support call cancelled.**
302	**Power-off started.**
303	**Power-on reset completed.**
304	**System reset completed.**
305	**System power-on reset completed.**
306	**Transition into physically partitioned (PP) mode.**
307	**Transition into single image (SI) mode.**
308	**Vary storage range *{0}*-*{1}* megabyte command received.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

309	**Vary storage element *{0}* command received *{1}*.**

Explanation

Substitution variables are:

*{0}*Storage element
*{1}*Command result

310	**Vary expanded storage element command received *{0}*.**

Explanation

Substitution variables are:

*{0}*Command result

311	**Vary channel path command received *{0}*.**

Explanation

Substitution variables are:

*{0}*Command result

312	**Vary channel set *{0}* channel number *{1}* command received *{2}*.**

Explanation

Substitution variables are:

*{0}*Channel set
*{1}*Channel number
*{2}*Command result

313 **Command completed. Response code: *{0}*.**

Explanation

Substitution variables are:

*{0}*Response code number

314 **Hardware element configured on: *{0}*.**

Explanation

Substitution variables are:

*{0}*Hardware element

315 **Hardware element configured off: *{0}*.**

Explanation

Substitution variables are:

*{0}*Hardware element

316 **Central storage configured on: *{0}*-*{1}*.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

317 **Central storage configured off: *{0}*-*{1}*.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

318 **Expanded storage configured on: *{0}*-*{1}*.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

319 **Expanded storage configured off: *{0}*-*{1}*.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

320 **Power or thermal system failure.**

321 **Critical power or thermal fault.**

322 **Logout analysis disabled.**

323 **Load failed *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor number

324 **Load cancelled *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor number

325 **Load rejected *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor number

326 **Power on failed.**

327 **Power on cancelled.**

328 **Power on rejected.**

329 **System reset failed.**

330 **System reset cancelled.**

331 **System reset rejected.**

332 **Activate failed *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

333 **Activate cancelled *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

334 **Activate rejected *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

335 **Deactivate failed *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

336 **Deactivate cancelled *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

337 **Deactivate rejected *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

338 **CHPID *{0}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*338

339 **Vector element failed *{0}*.**

Explanation

Substitution variables are:

*{0}*Vector name

340 **Invalid PSW loop on processor *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor number

341 **Processor *{0}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*Processor number

342 **CHPID *{0}* deconfigured during reset.**

Explanation

Substitution variables are:

*{0}*CHPID type

343 **Vector element failed.**

344 **Crypto failure.**

345 **Operator console not operational.**

346 **Vary storage element *{0}* command received.**

Explanation

Substitution variables are:

*{0}*Storage element

347 **Vary expanded storage element command received.**

348 **Vary channel path command received.**

349 **Vary channel set *{0}* channel number *{1}* command received.**

Explanation

Substitution variables are:

*{0}*Channel set
*{1}*Channel number

350 **CHPIDs *{0}*-*{1}* deconfigured during reset *{2}*.**

Explanation

Substitution variables are:

*{0}*Start CHPID range
*{1}*End CHPID range
*{2}*Target name

351 **CHPIDs *{0}*-*{1}* deconfigured during reset.**

Explanation

Substitution variables are:

*{0}*Start CHPID range
*{1}*End CHPID range

352 **Partition *{2}*: CHPIDs *{0}* and *{1}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*CHPID type
*{2}*CHPID type

353 **Processor *{0}* has entered disabled wait state.**

Explanation

Substitution variables are:

*{0}*Processor number

354 **Automatic activation has started using the *{1}* profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile type
*{1}*Profile name

355	**System activity analysis started.**
356	**System activity analysis ended.**
358	**DCAF attempt rejected: DCAF target program is already active with another DCAF session.**
359	**DCAF session ended.**
360	**User DCAF attempt rejected: ROF disabled or user is logged on.**
361	**PE DCAF attempt rejected: user is logged on.**
362	**DCAF attempt rejected: ROF is currently active.**
363	**DCAF attempt rejected: Bad password used.**

Messages 401-500

479	**S370 channel RPQ was successful.**
480	**S370 channel RPQ failed.**
481	**Undo S370 channel RPQ was successful.**
482	**Undo S370 channel RPQ failed.**
483	**The following operation was cancelled: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU
*{3}*Creation date

497	**The following operation was scheduled by *{1}* from *{2}*: *{0}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU

498	**The following operation started: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU
*{3}*Creation date

499	**The following operation failed to start within the specified time window: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU
*{3}*Creation date

500 **The following operation was attempted but did not start: *{0}*. It was scheduled by *{1}* from *{2}*.*{3}* on *{4}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NetId
*{3}*NAU
*{4}*Creation date

Messages 501-600

501 **The following operation was attempted but failed: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU
*{3}*Creation date

502 **The following disruptive operation started: *{0}*. It was requested from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Disruptive operation
*{1}*Network ID
*{4}*NAU

503 **The following disruptive operation started: *{0}*. It was requested by *{1}* from *{2}*.*{3}*.**

Explanation

Substitution variables are:

*{0}*Disruptive operation
*{1}*User name
*{2}*Network ID
*{3}*NAU

504 **Engineering change (EC) information query for concurrency status started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

505	**Engineering change (EC) information query for concurrency status completed.**
512	**A scheduled operation started.**
513	**A scheduled operation completed successfully.**
514	**A scheduled operation failed.**
515	**A scheduled operation failed to start within the specified time window.**
516	**A scheduled activate failed to start within the specified time window.**
517	**A scheduled deactivate failed to start within the specified time window.**
518	**A scheduled retrieve of internal code changes failed to start within the specified time window.**
519	**A scheduled install of internal code changes failed to start within the specified time window.**
520	**A scheduled hard disk backup failed to start within the specified time window.**
521	**A scheduled remove of internal code changes failed to start within the specified time window.**
522	**User *{0}* attempted to log on with a user identification or password that was not valid.**

Explanation

Substitution variables are:

*{0}*User name

523	**A remote console session was initiated with system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

524	**Concurrent internal code changes for I390/PU started.**
525	**Concurrent internal code changes for I390/PU completed.**
526	**Concurrent internal code changes for I390/PU failed.**
527	**Concurrent internal code changes for I390/PU completed with no changes required for current operating mode.**
528	**A scheduled accept of internal code changes failed to start within the specified time window.**
529	**A scheduled install and activate of internal code changes failed to start within the specified time window.**
530	**A scheduled retrieve and install of internal code changes failed to start within the specified time window.**
531	**A scheduled set clock operation failed to start within the specified time window.**
532	**A scheduled power on failed to start within the specified time window.**
533	**A scheduled power off failed to start within the specified time window.**
534	**A scheduled load failed to start within the specified time window.**
535	**A scheduled system reset failed to start within the specified time window.**
536	**A scheduled clock synchronization failed to start within the specified time window.**

537	**A scheduled operation was attempted but did not start.**
538	**Concurrent internal code changes for PR/SM started.**
539	**Concurrent internal code changes for PR/SM completed.**
540	**Concurrent internal code changes for PR/SM failed.**
541	**Concurrent internal code changes for CFCC started.**
542	**Concurrent internal code changes for CFCC completed.**
543	**Concurrent internal code changes for CFCC failed.**
544	**A scheduled activate was attempted but did not start.**
545	**A scheduled deactivate was attempted but did not start.**
546	**A scheduled retrieve of internal code changes was attempted but did not start.**
547	**A scheduled install of internal code changes was attempted but did not start.**
548	**A scheduled hard disk backup was attempted but did not start.**
549	**A scheduled remove of internal code changes was attempted but did not start.**
550	**A scheduled accept of internal code changes was attempted but did not start.**
551	**A scheduled install and activate of internal code changes was attempted but did not start.**
552	**A scheduled retrieve and install of internal code changes was attempted but did not start.**
553	**A scheduled set clock operation was attempted but did not start.**
560	**A scheduled power on was attempted but did not start.**
561	**A scheduled power off was attempted but did not start.**
562	**A scheduled load was attempted but did not start.**
563	**A scheduled system reset was attempted but did not start.**
564	**A scheduled clock synchronization was attempted but did not start.**
565	**The following internal code changes were retrieved from diskette: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

566	**The following internal code changes were retrieved from mass storage media: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

567	**The following internal code changes were requested to be retrieved from the support system: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

568 **The following internal code changes were retrieved from the server: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

569 **A failure occurred activating the following internal code fixes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

575 **A failure occurred activating internal code changes.**

576 **A failure occurred deactivating the following internal code fixes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

577 **A failure occurred retrieving the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*Message describing the failure.

578 **A failure occurred installing the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

579 **A failure occurred activating the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

581 **A failure occurred removing the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

582 **A failure occurred deleting the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

583 **A failure occurred accepting the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

586 **Retrieve internal code changes started by an automatic operations command from a central control host.**

587 **Retrieve internal code changes, started by an automatic operations command from a central control host, completed.**

590 **Communications are not active between this console and the console named *{0}*.**

Explanation

Substitution variables are:

*{0}*HMC console name

591 **Communications are not active between the Hardware Management Console and the Support Element for system *{0}*.**

Explanation

Substitution variables are:

*{0}*SE console name

Messages 601-700

614 **Activation of any existing internal code changes has started.**

615 **Coupling facility control code load started.**

616 **Coupling facility control code load completed successfully.**

617 **Coupling facility control code load failed.**

618 **Deactivate and delete of all temporary internal code fixes started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

619 **Deactivate and delete of all temporary internal code fixes completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

620 **Deactivate and delete of all temporary internal code fixes failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

621 **Retrieve internal code changes initiated by a central control host has started.**

622	**Retrieve internal code changes initiated by a central control host has completed.**
623	**Settings saved automatically to not allow installation and activation of internal code changes.**
624	**Settings saved on Hardware Management Console *{0}* to allow installation and activation of internal code changes.**

Explanation

Substitution variables are:

*{0}*Origin HMC

625	**Settings saved manually on Hardware Management Console *{0}* to not allow installation and activation of internal code changes.**

Explanation

Substitution variables are:

*{0}*Origin HMC

626	**A scheduled transmit system availability data failed to start within the specified time window.**
627	**A scheduled transmit system availability data was attempted, but did not start.**
628	**Concurrent internal code changes for channels started.**
629	**Concurrent internal code changes for channels completed.**
630	**Concurrent internal code changes for channels failed.**
631	**Concurrent internal code changes for a supported storage subsystem's device drives started.**
632	**Concurrent internal code changes for a supported storage subsystem's device drives completed.**
633	**Concurrent internal code changes for a supported storage subsystem's device drives failed.**
634	**Concurrent internal code changes for cage controller started.**
635	**Concurrent internal code changes for cage controller completed.**
636	**Concurrent internal code changes for cage controller failed.**
637	**Concurrent internal code changes for power started.**
638	**Concurrent internal code changes for power completed.**
639	**Concurrent internal code changes for power failed.**
640	**Concurrent internal code changes for Support Element started.**
641	**Concurrent internal code changes for Support Element completed.**
642	**Concurrent internal code changes for Support Element failed.**
658	**Concurrent internal code changes started.**
659	**Concurrent internal code changes completed.**
660	**Concurrent internal code changes failed.**
661	***{0}*.**

Explanation

Service require state message.

Substitution variables are:

*{0}*A message describing the reason service required state was turned on or a message saying service required state was turned off.

662	**Backup critical data started.**
663	**Backup critical data ended.**
664	**Configuration data was copied to a diskette.**
665	**Configuration data was copied to the Hardware Management Console hard disk.**
666	**The system console was initialized.**
667	**The central processor complex (CPC) console was disabled.**
668	**Concurrent internal code changes initiated by MCL process.**
669	**Concurrent internal code changes initiated by pedebug panel.**
670	**Concurrent internal code changes initiated by systemTst testcase.**
671	**Activation starting load delay for power sequencing of *{0}* seconds.**

Explanation

Substitution variables are:

*{0}*Load delay seconds

672	**Activation ending load delay for power sequencing of *{0}* seconds.**

Explanation

Substitution variables are:

*{0}*Load delay seconds

673	**Starting remote support call *{1}* for console *{0}*. Type: *{2}*.**

Explanation

Substitution variables are:

*{0}*Console name and IP address
*{1}*Date and time
*{2}*Description

674	**Remote support call generated on *{1}* completed successfully by server *{0}*.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

675	**Remote support call generated on *{1}* cancelled at server *{0}*.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

676 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Internal code error.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

677 **Remote support call generated on *{1}* failed at server *{0}*. Reason: No phone number available.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

678 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Connectivity failed.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

679 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Remote support returned an error.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

680 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Machine is not registered.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

681 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Probable connectivity failure.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

682 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Device type not supported.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

683 **A zeroize was performed against crypto element *{0}*. The Crypto Module Identifier (CMID) of the processor is: *{1}*.**

Explanation

Substitution variables are:

*{0}*Crypto number
*{1}*Crypto module identifier

684 **An import was performed against crypto element *{0}*. The Crypto Module Identifier (CMID) of the processor is: *{1}*.**

Explanation

Substitution variables are:

*{0}*Crypto number
*{1}*Crypto module identifier

685 **Installing internal code changes was attempted, but there were no changes to install.**

686 **Removing internal code changes was attempted, but there were no changes to remove.**

687 **User *{0}* was logged on automatically at the console.**

Explanation

Substitution variables are:

*{0}*User name

688 **Model conversion started**

689 **Model conversion completed successfully.**

690 **Model conversion failed.**

691 **The following operation was scheduled by *{1}* from *{2}.{3}* at IP address *{4}*: *{0}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address

692 **The following operation started: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name

*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address
*{5}*Network ID

693 **The following operation failed to start within the specified time window: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address
*{5}*Network ID

694 **The following operation was attempted but did not start: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address
*{5}*Network ID

695 **The following operation was attempted but failed: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address
*{5}*Network ID

696 **The following operation was cancelled: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU

*{4}*IP address
*{5}*Network ID

697 **The following disruptive operation started: *{0}*. It was requested by *{1}* from *{2}*.*{3}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address

Messages 701-800

701 **Battery operated clock set to new time obtained from *{0}*.**

Explanation

Substitution variables are:

*{0}*Network ID.NAU

702 **Activation profiles were imported.**

703 **System activity profiles were imported.**

704 **Activation profiles were exported.**

705 **System activity profiles were exported.**

706 **Model conversion to model *{0}* completed successfully.**

Explanation

Substitution variables are:

*{0}*Model number

707 **Changed write protect of Input/Output Configuration Data Set (IOCDS) *{0}* in *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*IOCDS name
*{1}*IOCDS identifier
*{2}*Function, such as IOCP

708 **Failed writing Input/Output Configuration Data Set (IOCDS) *{0}* to *{1}* by *{2}*.**

Explanation

Substitution variables are:

*{0}*IOCDS name
*{1}*IOCDS identifier
*{2}*Function, such as IOCP

709 **User profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*User profile name

710	**Memory upgrade completed successfully.**
711	**Memory upgrade failed.**
712	**An LPAR Dump, initiated by *{0}*, has been taken.**

Explanation

Substitution variables are:

*{0}*User name

713	**CHPID *{0}* was released.**

Explanation

Substitution variables are:

*{0}*CHPID type

714	**ID *{0}* was reassigned from logical partition *{1}* to logical partition *{2}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Old image name
*{2}*New image name

715	**The power save state started.**
716	**The power save state ended.**
717	**Display/alter was used to: *{0} {1} {2}*.**

Explanation

Substitution variables are:

*{0}*Display or alter
*{1}*Image and CP names
*{2}*Display/alter function

718	**Logical partition control settings were changed.**
719	**Logical partition security settings were changed.**
720	**Logical partition cryptographic control settings were changed.**
721	**A backup of critical data was performed.**
722	**An upgrade to EC level *{0}* was performed.**

Explanation

Substitution variables are:

*{0}*EC level

723 **Remote support call generated on *{1}* failed at server *{0}*. It will be attempted at another server if available.**

Explanation

Substitution variables are:

*{0}*Handling machine name
*{1}*Origin machine name

724 **The Support Element was upgraded to *{0}* EC level by *{1}*.**

Explanation

Substitution variables are:

*{0}*EC level
*{1}*Network ID.NAU

725 **The *{1}* profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile type
*{1}*Profile name

726 **An attempt to reassign ID *{0}* failed.**

Explanation

Substitution variables are:

*{0}*CHPID type

727 **The central storage allocated to logical partition *{0}* was changed from *{1}* MB to *{2}* MB.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old storage
*{2}*New storage

728 **The expanded storage allocated to logical partition *{0}* was changed from *{1}* MB to *{2}* MB.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old storage
*{2}*New storage

729 **Logical processor *{0}* was configured off from logical partition *{1}*.**

Explanation

Substitution variables are:

*{0}*CP number
*{1}*Image name

730 **Logical processor *{0}* was configured on to logical partition *{1}*.**

Explanation

Substitution variables are:

*{0}*CP number
*{1}*Image name

731 **A DCAF connection to the Support Element was started in user mode *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

732 **A DCAF connection to the Support Element was ended.**

733 **The security log was archived.**

734 **Remote support call generated on *{1}* is being handled by call-home server *{0}*.**

Explanation

Substitution variables are:

*{0}*Destination machine name and IP address
*{1}*Origin machine name

735 **Power on was performed.**

736 **Power off was performed.**

737 **Reset normal was performed.**

738 **Reset clear was performed.**

739 **Power-on reset started.**

740 **Power-on reset was successful.**

741 **Power-on reset was partially successful.**

742 **Power-on reset failed.**

743 **The following operation failed: *{0}*. It was scheduled by *{1}* from *{2}.{3}* on *{4}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Network ID

744 **The following operation failed: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Network ID
*{5}*IP address

745 **The following operation completed successfully: *{0}*. It was scheduled by *{1}* from *{2}.{3}* on *{4}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Network ID

746 **The following operation completed successfully: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Network ID
*{5}*IP address

747 **The RSF queue has been put on hold.**

748 **The RSF queue has been released from hold.**

749 **The *{0}* object was defined.**

Explanation

Substitution variables are:

*{0}*Object name

750 **The *{0}* object was undefined.**

Explanation

Substitution variables are:

*{0}*Object name

751 **Upgrade data was saved.**

752 **The CBU file was deleted from the hard disk.**

753 **An error was detected trying to delete the CBU file.**

754	**PMI Upgrade was successful.**
755	**PMI Upgrade failed or was not required.**
756	**User *{0}* logged off from a Platform Independent Remote Console (PIRC) at IP address *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*IP address

757	**User *{0}* was logged off from a Platform Independent Remote Console (PIRC) at IP address *{1}* due to inactivity.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*IP address

776	**Mirroring data from the primary Support Element to the alternate Support Element completed successfully.**
777	**A switch request initiated the alternate Support Element (serial number *{0}*) to now be the primary Support Element.**

Explanation

Substitution variables are:

*{0}*Serial number

778	**Mirroring data from the primary Support Element to the alternate Support Element started.**
779	**Mirroring data from the primary Support Element to the alternate Support Element failed. *{0}***

Explanation

Substitution variables are:

*{0}*Reason for the failure

780	**An alternate Support Element is not installed. Mirroring data from the primary Support Element could not be completed.**
781	**The following operation completed: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of operation
*{1}*User name
*{2}*Console name
*{3}*Date

782	**The following operation completed: *{0}*. It was scheduled by *{1}* from *{2}*.*{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Description of operation
*{1}*User name
*{2}*Network ID
*{3}*NAU
*{4}*IP address
*{5}*NAU

783	**The CBU feature has been enabled successfully.**
784	**An error was detected trying to enable the CBU feature.**
785	**A concurrent CP upgrade was performed to add *{0}* CPUs.**

Explanation

Substitution variables are:

*{0}*Number of CPs

786	**A special code load was performed.**
787	**Domain security name or password was changed on consoles: *{0}*.**

Explanation

Substitution variables are:

*{0}*Console names

788	**Remote request made to change the Support Element name.**
789	**Remote request made to reboot the Support Element.**
790	**Alternate Support Element rebooted upon completing a mirroring operation.**
791	**Switched from primary to alternate Support Element.**
792	**Switched from primary to alternate Support Element after LAN recovery.**
793	**Support Element rebooted to apply patches during concurrent patch.**
794	**Support Element rebooted to apply patches during disruptive patch.**
795	**Local request made to change the Support Element name.**
797	**Due to event log space limitations, obsolete events were deleted and file *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Log file name

798	**The number of CPs for partition *{0}* has changed from *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old number of CPs
*{2}*New number of CPs

799 **The global IO priority queuing setting has been *{0}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled

800 **Settings for logical partitions IO priority queuing were changed.**

Messages 801-900

801 **The current processing capped value for partition *{0}* changed from *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old processing capped value
*{2}*New processing capped value

802 **The current processing weight value for partition *{0}* changed from *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old processing weight value
*{2}*New processing weight value

803 **A *{0}* Alternate Support Element switch is requested by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*Switch type
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU

804 **A *{0}* Alternate Support Element switch is requested by *{1}* from *{2}.{3}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Switch type
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address

805 **A *{0}* Alternate Support Element switch was initiated from *{1}*.**

Explanation

Substitution variables are:

*{0}*Switch type
*{1}*Console requesting switch

806 **An automatic alternate Support Element switch was initiated due to *{0}*.**

Explanation

Substitution variables are:

*{0}*Reason for the switch

807 **A *{0}* Alternate Support Element switch is requested for *{1}.{2}* by *{3}* from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Switch type
*{1}*Network ID
*{2}*NAU
*{3}*HMC user name
*{4}*Origin Network ID
*{5}*Origin NAU

808 **Channel upgrade completed successfully.**

809 **Channel upgrade failed.**

810 **Channel upgrade was partially successful.**

811 **The import of the PCI cryptographic coprocessor FCV file was successful.**

812 **The zeroize of the PCI cryptographic coprocessor *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

813 **The zeroize of the PCI cryptographic coprocessor configuration was successful.**

820 **System configuration file bbruchpd.dat was deleted.**

821 **CHPID mapping function completed.**

822 **Linux CP feature update completed.**

823 **Linux CP feature update failed.**

824 **UNDO Linux CP feature completed.**

825 **UNDO Linux CP feature update failed.**

826 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Machine is not under warranty or service contract.**

Explanation

Substitution variables are:

*{0}*Destination machine name and IP address
*{1}*Origin machine name

827 **A concurrent CP downgrade was performed. Current number of *{1}* are *{0}*.**

Explanation

Substitution variables are:

*{0}*Type of CP
*{1}*Number of CPs

828 **A concurrent memory upgrade was performed to add *{0}* MBytes.**

Explanation

Substitution variables are:

*{0}*Number of MBytes

829 **A concurrent memory downgrade was performed to remove *{0}* MBytes.**

Explanation

Substitution variables are:

*{0}*Number of MBytes

830 **An import of the PCI cryptographic coprocessor UDX image was successful.**

831 **The activation of the UDX image for PCI cryptographic coprocessor *{0}* was successful. Timestamp: *{1}*, Name: *{2}***

Explanation

Substitution variables are:

*{0}*Cryptographic number
*{1}*Timestamp
*{2}*Segment 3 image name

832 **The activation of the factory default image for PCI cryptographic coprocessor *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

833 **The zeroize of the PCI cryptographic coprocessor UDX image was successful.**

834 **Unable to inform the operating system about the model conversion.**

835 **PU LICCC record has been retrieved from support system.**

836 **CBU LICCC record has been retrieved from support system.**

837 **MEM LICCC record has been retrieved from support system.**

838 **CHN LICCC record has been retrieved from support system.**

839 **DRA record has been retrieved from support system.**

840 **LCP record has been retrieved from support system.**

841 **PU LICCC record has been deleted from the hard disk.**

842 **CBU LICCC record has been deleted from the hard disk.**

843 **MEM LICCC record has been deleted from the hard disk.**

844 **CHN LICCC record has been deleted from the hard disk.**

845	**DRA record has been deleted from the hard disk.**
846	**LCP record has been deleted from the hard disk.**
847	**Concurrent internal code changes for oFCP loader started.**
848	**Concurrent internal code changes for oFCP loader completed.**
849	**Concurrent internal code changes for oFCP loader failed.**
850	**Mirroring over the customer network, because the service network is down.**
851	**CIU LICCC record has been retrieved from support system.**
852	**CIU LICCC record has been deleted from the hard disk.**
853	**Input/Output Configuration Data Sets (IOCDS) restored from *{0} {1}*.**

Explanation

Substitution variables are:

*{0}*HMC Network ID
*{1}*HMC NAU

854	**Processor drawer hardware was added at *{0}*.**

Explanation

Substitution variables are:

*{0}*Location for the processor drawer

855	**Processor drawer hardware was deleted from *{0}*.**

Explanation

Substitution variables are:

*{0}*Location for the processor drawer

856	**Concurrent processor drawer hardware add completed successfully.**
857	**Concurrent processor drawer hardware add failed.**
858	**System Complex (Sysplex) Timer was used to change ETR configuration data.**
859	**There have been *{0}* consecutive failed logon attempts for user *{1}*.**

Explanation

Substitution variables are:

*{0}*Number of failed logon attempts
*{1}*User name

860	**Backup critical console data failed, *{0}*.**

Explanation

Substitution variables are:

*{0}*State of the backup

861	**Backup critical console data completed.**
862	**Permanent LICCC update completed successfully.**
863	**Permanent LICCC update failed.**

864	**Root password was updated.**
865	**An Authorize internal code changes request of *{0}* for Hardware Management Console *{1}.{2}* and all its defined objects is being issued by *{3}* from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Request type
*{1}*HMC Network ID
*{2}*HMC NAU
*{3}*User name
*{4}*HMC Network ID
*{5}*HMC NAU

866	**The CP cryptographic assist functions have been enabled successfully.**
867	**The CP cryptographic assist functions have been disabled successfully.**
868	**System power on started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

869	**System power on completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

870	**System power on failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

871	**System restricted power on started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

872	**System restricted power on completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

873	**System restricted power on failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

874 **System power off started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

875 **System power off completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

876 **System power off failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

877 **An EC upgrade has been performed on this Support Element.**

878 **A preload has been performed on this alternate Support Element.**

879 **The scheduled *{0}* did not run because the system was running and force was not specified. It was scheduled by *{1}* from *{2}.{3}* on *{4}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*User name
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Timestamp

881 **The TKE commands for PCIX cryptographic coprocessor number *{0}* have been enabled successfully.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

882 **The TKE commands for PCIX cryptographic coprocessor number *{0}* have been disabled successfully.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

883 **Refresh request for customizing console data via the LAN from *{0}*@*{1}* was ignored since this capability is disabled.**

Explanation

Substitution variables are:

*{0}*Host name
*{1}*IP address

884 **A request to customize console data via the LAN from *{0}*@*{1}* was ignored since this capability is disabled.**

Explanation

Substitution variables are:

*{0}*Host name
*{1}*IP address

885 **Customizable console data (*{2}*) has been sent via the LAN to *{0}*@*{1}*.**

Explanation

Substitution variables are:

*{0}*Host name
*{1}*IP address
*{2}*Customizable console data type

886 **Customizable console data (*{2}*) has been received via the LAN from *{0}*@*{1}*.**

Explanation

Substitution variables are:

*{0}*Host name
*{1}*IP address
*{2}*Customizable console data type

887 **The following disruptive operation started: Deactivate. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

888 **The following disruptive operation started: Deactivate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

*{3}*Origin IP address

889 **The following disruptive operation started: Disable concurrent patch. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

890 **The following disruptive operation started: Disable concurrent patch. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

891 **The following disruptive operation started: Install code changes/Activate. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

892 **The following disruptive operation started: Install code changes/Activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

893 **The following disruptive operation started: Load. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

894 **The following disruptive operation started: Load. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

895 **The following disruptive operation started: Power off. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

896 **The following disruptive operation started: Power off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

897 **The following disruptive operation started: Power-on reset. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

898 **The following disruptive operation started: Power-on reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

899 **The following disruptive operation started: PSW restart. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

900 **The following disruptive operation started: PSW restart. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

Messages 901-1000

901 **The following disruptive operation started: Remove code changes/activate. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

902 **The following disruptive operation started: Remove code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

903 **The following disruptive operation started: Reset I/O interface. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

904 **The following disruptive operation started: Reset I/O interface. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID

*{2}*Origin NAU
*{3}*Origin IP address

905 **The following disruptive operation started: Run checkout tests. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

906 **The following disruptive operation started: Run checkout tests. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

907 **The following disruptive operation started: Set clock. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

908 **The following disruptive operation started: Set clock. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

909 **The following disruptive operation started: Stop. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

910 **The following disruptive operation started: Stop. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

911 **The following disruptive operation started: Sysplex timer configuration change. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

912 **The following disruptive operation started: Sysplex timer configuration change. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

913 **The following disruptive operation started: System reset. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

914 **The following disruptive operation started: System reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

915 **The following disruptive operation started: System reset normal for object *{0}*. It was requested by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU

916 **The following disruptive operation started: System reset normal for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address

917 **The following disruptive operation started: System reset clear for object *{0}*. It was requested by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU

918 **The following disruptive operation started: System reset clear for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address

919 **The following disruptive operation started: Unknown. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

920 **The following disruptive operation started: Unknown. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

921 **A load will be attempted for system *{0}*. The load type is normal, store status yes, address *{2}*, parameter *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load address
*{2}*Load parameter

922 **A load will be attempted for system *{0}*. The load type is normal, store status no, address *{2}*, parameter *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load address
*{2}*Load parameter

923 **A load will be attempted for system *{0}*. The load type is clear, store status yes, address *{2}*, parameter *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load address
*{2}*Load parameter

924 **A load will be attempted for system *{0}*. The load type is clear, store status no, address *{2}*, parameter *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load address
*{2}*Load parameter

925 **A load will be attempted for system *{0}*. The load type is SCSI. Refer to the security log for more details.**

Explanation

Substitution variables are:

*{0}*Image name

926 **A load will be attempted for system *{0}*. The load type is SCSI dump. Refer to the security log for more details.**

Explanation

Substitution variables are:

*{0}*Image name

927 **A load will be attempted for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image Name

928 **The following disruptive operation started: Activate. It was requested by *{0}* from *{1}*. *{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

929 **The following disruptive operation started: Activate. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

930 **The following disruptive operation started: Configure channel off. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

931 **The following disruptive operation started: Configure channel off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

932 **Activation has started using the reset profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name

933 **Activation has started using the image profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Image profile name

934 **Activation has started using the load profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Load profile name

935 **Automatic activation has started using the reset profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name

936 **Automatic activation has started using the image profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Image profile name

937 **Automatic activation has started using the load profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Load profile name

938 **User *{0}* with session ID *{1}* has requested to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*Type of shutdown

939 **An LPAR dump, initiated by a B3 PCCALL, has been taken.**

940 **An LPAR dump, initiated by the LPAR Dump Task, has been taken.**

941 **An LPAR dump, initiated by a disabled wait, has been taken.**

942 **The global IO Priority Queuing setting is *{0}* (0=disabled, 1=enabled).**

Explanation

Substitution variables are:

*{0}*1 if enabled, 0 if disabled

943 **The current processing capped value for the *{1}* CPs in partition *{0}* changed from *{2}* to *{3}* (0=not capped, 1=capped).**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*Old processing capped value
*{3}*New processing capped value

944 **The *{0}* object was locked from disruptive tasks by *{1}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*User name

945 **The *{0}* object was unlocked from disruptive tasks by *{1}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*User name

947 **A concurrent resource change has resulted in a change to the processor speed.**

948 **A user password was changed.**

949 **Channel confg files swap completed for channels *{0}* and *{1}*.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*PCHID name

950 **Dynamic partition rename was used to *{0}* logical partition *{1}*. The partition number is *{2}*, CSS ID is *{3}*, image ID is *{4}*.**

Explanation

Substitution variables are:

*{0}*add or remove
*{1}*Image name
*{2}*Partition number
*{3}*CSS identifier
*{4}*Image identifier

951 **Change CP/SAP allocation has started.**

952 **Change CP/SAP allocation has completed successfully.**

953 **Change CP/SAP allocation has failed.**

954 **A concurrent CP upgrade was performed to add *{0} {1}*.**

Explanation

Substitution variables are:

*{0}*Number of CPs
*{1}*Type of CP

955 **A concurrent resource change has resulted in a change to the processor speed.**

956 **The reset profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

957 **The load profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

958 **The image profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

959 **The system activity profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

960 **The reset profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

961 **The load profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

962 **The image profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

963 **The system activity profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

964 **The reset profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

965 **The load profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

966 **The image profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

967 **The system activity profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

968 **The reset profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

969 **The load profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

970 **The image profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

971 **The system activity profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

972 **The reset profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

973 **The load profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

974 **The image profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

975 **The system activity profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

976 **Load from removable media or server for image *{0}* completed successfully.**

Explanation

Substitution variables are:

*{0}*Image name

977 **Load from removable media or server for image *{0}* failed.**

Explanation

Substitution variables are:

*{0}*Image name

978 **Load from removable media or server for image *{0}* failed. Not enough memory in the image available.**

Explanation

Substitution variables are:

*{0}*Image name

979 **Load from removable media or server for image *{0}* has failed. There was a problem trying to read all of the data files.**

Explanation

Substitution variables are:

*{0}*Image name

980 **Dumping of SCSI IPL loader data for image *{0}* completed successfully.**

Explanation

Substitution variables are:

*{0}*Image name

981 **Dumping of SCSI IPL loader data for image *{0}* failed.**

Explanation

Substitution variables are:

*{0}*Image name

982 **The following operation started: Concurrent switch. It was requested by *{0}* from *{1}*. *{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

983 **The following operation started: Concurrent switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

984 **The following operation started: Disruptive switch. It was requested by *{0}* from *{1}*. *{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID

*{2}*Origin NAU

985	**The following operation started: Disruptive switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

986	**Channel upgrade started.**
987	**Rebuild VPD started.**
988	**CBU activation started.**
989	**CIU retrieve started.**
990	**Apply retrieved data started.**
991	**OOCOD activation started.**
992	**CBU/OOCOD undo started.**
993	**A change of system performance values has started that will *{0}*.**

Explanation

Substitution variables are:

*{0}*Description of the change

994	**A change of system performance values has completed successfully.**
995	**A change of system performance values has failed.**
996	**Rebuild VPD failed.**
997	**Rebuild of VPD is only partially complete.**
998	**CIU retrieve failed.**
999	**Maximum available memory feature added OK**
1000	**Error adding the maximum available Memory feature**

Messages 1001-1100

1001	**Maximum available memory feature was removed OK**
1002	**Error removing the mMaximum available memory feature**
1003	**Start add STP feature.**
1004	**Add STP feature failed.**
1005	**Add STP feature was successful.**
1006	**Start add FSB feature.**
1007	**Add FSB feature failed**
1008	**Add FSB feature was successful.**
1009	**Start remove STP feature.**
1010	**Remove STP feature failed.**

1011	**Remove STP feature was successful.**
1012	**Start remove FSB feature.**
1013	**Remove FSB feature failed**
1014	**Remove FSB feature was successful.**
1015	**Restore critical data was started.**
1016	**Start add RPQ 8P2333 feature.**
1017	**Add RPQ 8P2333 feature failed.**
1018	**Add RPQ 8P2333 feature was successful.**
1019	**Start remove RPQ 8P2333 feature.**
1020	**Remove RPQ 8P2333 feature failed.**
1021	**Remove RPQ 8P2333 feature was successful.**
1022	**Add RPQ 8P2333 feature was partially successful.**
1023	**Transmit VPD task entering sleep.**
1024	**Transmit VPD task waking.**
1025	**Start add OSA 3215 feature.**
1026	**Add OSA 3215 feature failed.**
1027	**Add OSA 3215 feature was successful.**
1028	**Start remove OSA 3215 feature.**
1029	**Remove OSA 3215 feature failed.**
1030	**Remove OSA 3215 feature was successful.**
1031	**Add OSA 3215 feature was partially successful.**
1044	**Start add of three phase power cord feature.**
1045	**Add three phase power cord feature failed.**
1046	**Add three phase power cord feature was successful.**
1047	**Start remove of three phase power cord feature.**
1048	**Remove three phase power cord feature failed.**
1049	**Remove three phase power cord feature was successful.**
1050	**Start add of alternate CP assignment feature.**
1051	**Add alternate CP assignment feature failed.**
1052	**Add alternate CP assignment feature was successful.**
1053	**Start remove of alternate CP assignment feature.**
1054	**Remove alternate CP assignment feature failed.**
1055	**Remove alternate CP Assignment feature was successful.**
1056	**Start synchronization with HOM.**
1057	**Start add of *{0}* feature.**

Explanation

Substitution variables are:

*{0}*Feature name

1058 **Add of *{0}* feature failed.**

Explanation

Substitution variables are:

*{0}*Feature name

1059 **Add of *{0}* feature was successful.**

Explanation

Substitution variables are:

*{0}*Feature name

1060 **Start remove of *{0}* feature.**

Explanation

Substitution variables are:

*{0}*Feature name

1061 **Remove of *{0}* feature failed.**

Explanation

Substitution variables are:

*{0}*Feature name

1062 **Remove of *{0}* feature was successful.**

Explanation

Substitution variables are:

*{0}*Feature name

1063 **The *{0}* object was set to busy by *{1}*.**

Explanation

Substitution variables are:

*{0}*Target name
*{1}*User name

1064 **The *{0}* object was set to not busy by *{1}*.**

Explanation

Substitution variables are:

*{0}*Target name
*{1}*User name

1066 **Record *{0}* contains System z Application Assist Processors (zAAPs) and has been deleted.**

Explanation

Substitution variables are:

*{0}*Record number

1067	**Domain security name or password was changed by console *{0}*.**

Explanation

Substitution variables are:

*{0}*Console name

1068	**Backup critical data completed successfully.**
1069	**Backup critical data was attempted but was not successful.**
1070	**Backup critical data encountered an error when creating the backup.**
1071	**Backup critical data completed successfully, but it was not sent to the FTP server.**
1100	**The system clock has changed.**

Messages 1101-1200

1101	**The leap second offset has changed to *{0}* seconds.**

Explanation

Substitution variables are:

*{0}*Seconds

1102	**The time zone parameters have changed.**
1103	**The coordinated timing network ID for this CPC has changed to *{0}*.**

Explanation

Substitution variables are:

*{0}*Coordinated timing network identifier

1104	**The network configuration for the coordinated timing network that this CPC is a member of has changed.**
1105	**This CPC is configured as a local clock server for the coordinated timing network that it is a member of.**
1106	**This CPC is no longer configured as a local clock server for the coordinated timing network that it is a member of.**
1107	**This CPC changed the coordinated timing network ID for the coordinated timing network to *{0}* as requested.**

Explanation

Substitution variables are:

*{0}*Coordinated timing network identifier

1108	**This CPC changed the network configuration for the coordinated timing network as requested.**
1109	**This CPC changed the network configuration for the coordinated timing network because of a recovery action.**
1110	**This CPC is requesting an adjustment to the coordinated server time after contacting an external time source via *{0}*.**

Explanation

Substitution variables are:

*{0}*External time source type and the amount of time to adjust

1111	**The migration procedure from an STP-only Coordinated Timing Network (CTN) to a mixed CTN started.**
1112	**The migration procedure from an STP-only Coordinated Timing Network (CTN) to a mixed CTN completed successfully.**
1113	**The migration procedure from an STP-only Coordinated Timing Network (CTN) to a mixed CTN was cancelled.**
1114	**The migration procedure from an STP-only Coordinated Timing Network (CTN) to a mixed CTN failed.**
1115	**Automatic adjustment of the coordinated server time to an external time source failed because the threshold was exceeded.**
1116	**Automatic adjustment of the coordinated server time to an external time source failed.**
1117	**A timeout occurred contacting the external time source to automatically adjust the coordinated server time.**
1118	**Detected another STP-only Coordinated Timing Network (CTN) with the same CTN ID.**
1119	**Lost clock synchronization.**
1120	**Pulse Per Second (PPS) signals are being used to provide highly accurate adjustments to the coordinated server time for the STP-only CTN.**
1121	**Pulse Per Second (PPS) signals are no longer being used to provide highly accurate adjustments to the coordinated server time for the STP-only CTN, as requested by the user.**
1122	**Automatic adjustment of the coordinated server time to an external time source failed because no Hardware Management Console is set up to perform the dial out.**
1123	**PPS port 0 *{0}* receiving Pulse Per Second (PPS) signals.**

Explanation

Substitution variables are:

*{0}*is or is not

1124	**PPS port 1 *{0}* receiving Pulse Per Second (PPS) signals.**

Explanation

Substitution variables are:

*{0}*is or is not

1125	**PPS port *{0}* is no longer synchronized.**

Explanation

Substitution variables are:

*{0}*Port number

1126	**PPS port *{0}* offset differs by more than the amount allowed from the PPS port that is tracking to PPS signal.**

Explanation

Substitution variables are:

*{0}*Port number

1127 **A configuration error was detected on PPS port *{0}*.**

Explanation

Substitution variables are:

*{0}*Port number

1128 **PPS port *{0}* dispersion is greater than the threshold value.**

Explanation

Substitution variables are:

*{0}*Port number

1129 **A jam synch condition was detected on PPS port *{0}*.**

Explanation

Substitution variables are:

*{0}*Port number

1130 **Pulse Per Second (PPS) signals from PPS port 0 are being used.**

1131 **Pulse Per Second (PPS) signals from PPS port 1 are being used.**

1132 **Receiving Pulse Per Second (PPS) signals on port *{0}* to provide redundancy of an External Time Source.**

Explanation

Substitution variables are:

*{0}*Port number

1133 **No longer receiving Pulse Per Second (PPS) signals.**

1134 **Adjustments to coordinated server time for the STP-only CTN are being made using information from the backup system.**

1135 **Adjustments to coordinated server time for the STP-only CTN are no longer being made using information from the backup system.**

1136 **PPS port *{0}* offset on the backup system differs by more than the amount allowed from the PPS port that is tracking to PPS signal.**

Explanation

Substitution variables are:

*{0}*Port number

1137 **Pulse Per Second (PPS) signals are no longer being used to provide highly accurate adjustments to the Coordinated Server Time for the STP-only CTN due to a failure.**

1138 **Daylight saving time started.**

1139 **Daylight saving time ended.**

1140 **The STP maximum supported version number or lowest supported version number for this CPC changed to version *{0}*.**

Explanation

Substitution variables are:

*{0}*Version number

1141 **The total time offset changed.**

1142 **The network configuration for your STP-only CTN cannot be reestablished after a power-on reset or power outage.**

1143 **Pulse Per Second (PPS) port 0 *{0}* usable as a PPS source.**

Explanation

Substitution variables are:

*{0}*is or is not

1144 **Pulse Per Second (PPS) port 1 *{0}* usable as a PPS source.**

Explanation

Substitution variables are:

*{0}*is or is not

1145 **Pulse Per Second (PPS) port *{0}* entered a fenced state.**

Explanation

Substitution variables are:

*{0}*Port number

1146 **Automated coordinated timing network recovery is enabled on this CPC.**

1147 **Automated coordinated timing network recovery is disabled on this CPC: *{0}*.**

Explanation

Substitution variables are:

*{0}*The reason the automated coordinated timing network recovery is disabled.

1148 **The joining of STP CTN *{0}* into another CTN has started.**

Explanation

Substitution variables are:

*{0}*Coordinated timing network identifier

1149 **The joining of STP CTN *{0}* into another CTN has been cancelled.**

Explanation

Substitution variables are:

*{0}*Coordinated timing network identifier

1150 **The joining of two STP CTNs into one has failed: *{0}*.**

Explanation

Substitution variables are:

*{0}*The reason the join of two CTNs failed.

1200 **Customizable console data (*{0}*) was resynchronized by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Customizable data name
*{1}*User name

Messages 1201-1300

1201 **Customizable console data (*{0}*) was deconfigured from all sources by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Customizable data name
*{1}*User name

1202 **Customizable console data (*{0}*) was changed manually by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Customizable data name
*{1}*User name

1203 **The managed objects role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*User role name

1204 **The managed objects role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*User role name

1205 **The managed objects role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*User role name

1206 **Enable CBU feature started.**

1207 **CBU UNDO failure.**

1208 **CBU UNDO was partially successful.**

1209 **Start delete CBU feature.**

1210	**CBU feature activation was successful.**
1211	**CBU feature activation failed.**
1212	**CBU feature activation was partially successful.**
1213	**OOCoD UNDO was successful.**
1214	**OOCoD UNDO failed.**
1215	**OOCoD UNDO was partially successful.**
1216	**OOCoD feature activation was successful.**
1217	**OOCoD feature activation was partially successful.**
1218	**OOCoD feature activation failed.**
1219	**The zeroize of the cryptographic number *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1220	**The zeroize of the cryptographic configuration was successful.**
1221	**The cryptographic UDX image *{0}* was successfully imported from media.**

Explanation

Substitution variables are:

*{0}*UDX image name

1222	**The activation of the UDX image for cryptographic coprocessor *{0}* was successful. Timestamp: *{1}*, Name: *{2}***

Explanation

Substitution variables are:

*{0}*Cryptographic number
*{1}*Timestamp
*{2}*UDX image name

1223	**The activation of the factory default image for cryptographic coprocessor *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1224	**The erase of the cryptographic coprocessor UDX image *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*UDX image name

1225	**The TKE commands for cryptographic coprocessor number *{0}* have been enabled successfully.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1226 **The TKE commands for cryptographic coprocessor number *{0}* have been disabled successfully.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1227 **OOCoD remove failed.**

1228 **CBU remove failed.**

1229 **CIU apply failed.**

1230 **CIU apply was successful.**

1231 **Undo temporary upgrade started.**

1232 **Undo CBU was successful.**

1233 **The configuration type of cryptographic number *{0}* has been changed to cryptographic accelerator.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1234 **The configuration type of cryptographic number *{0}* has been changed to a cryptographic CCA coprocessor.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1235 **Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* started by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*System EC number
*{1}*User name
*{2}*Originating Network ID
*{3}*Originating NAU

1236 **Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* completed.**

Explanation

Substitution variables are:

*{0}*System EC number

1237 **Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* failed.**

Explanation

Substitution variables are:

*{0}*System EC number

1238	**Prepare for concurrent processor drawer replacement started.**
1239	**PU check for concurrent processor drawer replacement started.**
1240	**PUS are prepared for concurrent processor drawer replacement.**
1241	**PUS are not ready for concurrent processor drawer replacement.**
1242	**Prepare for concurrent processor drawer replacement failed during PU check.**
1243	**Memory check for concurrent processor drawer replacement started.**
1244	**Memory is prepared for concurrent processor drawer replacement.**
1245	**Memory is not ready for concurrent processor drawer replacement.**
1246	**Prepare for concurrent processor drawer replacement failed during memory check.**
1247	**I/O check for concurrent processor drawer replacement started.**
1248	**I/O is prepared for concurrent processor drawer replacement.**
1249	**I/O is not ready for concurrent processor drawer replacement.**
1250	**Prepare for concurrent processor drawer replacement failed during I/O check.**
1251	**Prepare for concurrent processor drawer replacement was successful.**
1252	**System is not ready for concurrent processor drawer replacement.**
1253	**Prepare for concurrent processor drawer replacement failed.**
1254	**Perform concurrent processor drawer replacement started.**
1255	**Perform concurrent processor drawer replacement was successful.**
1256	**Perform concurrent processor drawer replacement failed.**
1257	**Upgrade data restore was successful. Restore type is *{0}*.**

Explanation

Substitution variables are:

*{0}*Type of restore data

1258	**Upgrade data restore was unsuccessful. Restore type is *{0}*.**

Explanation

Substitution variables are:

*{0}*Type of restore data

1259	**Concurrent processor drawer hardware add started.**
1260	**Concurrent processor drawer hardware add LICCC data error.**
1261	**Book LICCC upgrade started.**
1262	**Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* for *{1}.{2}* started by *{3}* from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*System EC number
*{1}*Destination Network ID
*{2}*Destination NAU
*{3}*User name
*{4}*Originating Network ID
*{5}*Originating NAU

1263	**Concurrent internal code changes initiated by concurrent upgrade engineering changes activate request.**
1264	**Add processor drawer hardware request was cancelled.**
1265	**Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* completed, but not all functions may be available until the next system activation.**

Explanation

Substitution variables are:

*{0}*System EC number

1266	**BFYCALL request included: *{0}* CPS, *{1}* SAPS, *{2}* ICFS, *{3}* IFLS, *{4}* zIIPS, *{5}* IFPs.**

Explanation

Substitution variables are:

*{0}*Number of CPs
*{1}*Number of SAPs
*{2}*Number of ICFs
*{3}*Number of IFLs
*{4}*Number of zIIPs
*{5}*Number of IFPs

1268	**Remote support call generated on *{1}* failed at server *{0}*. Reason: No call home server is available.**

Explanation

Substitution variables are:

*{0}*IP address of the machine handling the request
*{1}*Originating machine name

1269	**An attempt was made to accept internal code changes but there were none to accept.**
1270	**The Monitor System Events task sent an email to *{0}* with a message count of *{1}* for sources *{2}*.**

Explanation

Substitution variables are:

*{0}*Destination name
*{1}*Number of messages
*{2}*Source name

1271	**Remote request made to reboot the console by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Network ID
*{2}*NAU

1272 **The task role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*Task role name

1273 **The task role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*Task role name

1274 **The task role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*Task role name

1275 **The current processing weight value for the *{0}* CPs in partition *{1}* changed from *{2}* to *{3}*.**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*Old weight value
*{3}*New weight value

1276 **A SOO session to the remote system was started for remote system user *{0}* from *{1}* for Hardware Management Console user *{2}*.**

Explanation

Substitution variables are:

*{0}*SE user name
*{1}*HMC name
*{2}*HMC user name

1277 **A SOO session to the remote system was ended for remote system user *{0}* from *{1}*.**

Explanation

Substitution variables are:

*{0}*SE user name
*{1}*HMC name

1278 **The password for user *{0}* has changed.**

Explanation

Substitution variables are:

*{0}*User name

1279 **User *{0}* has logged on.**

Explanation

Substitution variables are:

*{0}*User name

1280 **User *{0}* has logged off.**

Explanation

Substitution variables are:

*{0}*User name

1281 ***{0}***

Explanation

Substitution variables are:

*{0}*User name

1282 ***{0}***

Explanation

Substitution variables are:

*{0}*User name

1283 ***{0}* was forcibly disconnected by Hardware Management Console user *{2}* on *{1}*.**

Explanation

Substitution variables are:

*{0}*Current SE user information
*{1}*New HMC name
*{2}*New HMC user name

1284 **User *{0}* of session *{1}* has forcibly disconnected user *{2}* of session *{3}* in order to log on locally.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*Disconnected user name or '?' if unknown
*{3}*Disconnected session identifier

1285 **User *{0}* was not permitted to log on or reconnect since another user is already logged on.**

Explanation

Substitution variables are:

*{0}*User name

1286 **User *{0}* was not permitted to log on since the userid is disabled.**

Explanation

Substitution variables are:

*{0}*User name

1287 **User *{0}* was not permitted to log on since the userid is not allowed remote access.**

Explanation

Substitution variables are:

*{0}*User name

1288 **Remote request made to restart the console by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Network ID
*{2}*NAU

1289 **Remote request made to power off the console by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Network ID
*{2}*NAU

1290 **Remote request made to shutdown the console by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Network ID
*{2}*NAU

1291 **User *{0}* of session *{1}* is using user interface "*{2}*".**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*User interface style

1292 **The user profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*User profile name

1293 **The user profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*User profile name

1294 **The managed objects role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*Managed object role name

1295 **The managed objects role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*Managed object role name

1296 **The task role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*Task role name

1297 **The task role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*Task role name

1298 **Media device "*{0}*" lock held by "*{1}*" has been unlocked.**

Explanation

Substitution variables are:

*{0}*Media device name
*{1}*Lock owner

1299 **Media device "*{0}*" lock held by "*{1}*" failed to unlock.**

Explanation

Substitution variables are:

*{0}*Media device name
*{1}*Lock owner

1300 **Fanout card movement from slot *{0}* to slot *{1}* has started.**

Explanation

Substitution variables are:

*{0}*From location
*{1}*To location

Messages 1301-1400

1301 **Fanout card movement from slot *{0}* to slot *{1}* was successful.**

Explanation

Substitution variables are:

*{0}*From location
*{1}*To location

1302 **Fanout card movement from slot *{0}* to slot *{1}* failed.**

Explanation

Substitution variables are:

*{0}*From location
*{1}*To location

1303 **There were *{0}* STI paths swapped to their alternate paths for the fanout card in slot *{1}*.**

Explanation

Substitution variables are:

*{0}*Number of STI paths
*{1}*Location

1304 **There were *{0}* STI paths swapped to their default paths for the fanout card in slot *{1}*.**

Explanation

Substitution variables are:

*{0}*Number of STI paths
*{1}*Location

1305 **The group profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

1306 **The group profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

1307 **The group profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

1308 **The group profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

1309 **The group profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

1310 **The *{0}* group was created by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Group name
*{1}*User name

1311 **The *{0}* group was deleted by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Group name
*{1}*User name

1312 **The associated activation profile for *{0}* in group *{1}* has been changed to *{2}*.**

Explanation

Substitution variables are:

*{0}*Managed object
*{1}*Group name
*{2}*Activation profile name

1313 **ID *{0}* was released from logical partition *{1}* by user *{3}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name
*{2}*User name

1314 **ID *{0}* was configured off from logical partition *{1}* by user *{3}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name
*{2}*User name

1315 **An attempt to reassign ID *{0}* from logical partition *{1}* to logical partition *{2}* by user *{3}* failed.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name
*{2}*Image name
*{3}*User name

1316 **ID *{0}* was reassigned from logical partition *{1}* to logical partition *{2}* by user *{3}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name
*{2}*Image name
*{3}*User name

1317 **ID *{0}* was released from logical partition *{1}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name

1318 **A *{0}* operation was started by *{1}* from *{2}*.*{3}*.**

Explanation

Substitution variables are:

*{0}*Function name
*{1}*Origin console (User name)
*{2}*Network ID
*{3}*NAU

1319 **Channel LICCC update done on FRU location *{0}*. Original number of ports was *{1}*, new number of ports is *{2}*.**

Explanation

Substitution variables are:

*{0}*FRU location
*{1}*Old number of ports
*{2}*New number of ports

1320 **Customize Network Traffic Authorization: Allow Support Element LAN analysis = *{0}*, Allow SE OP sys analysis = *{1}*.**

Explanation

Substitution variables are:

{0}'1' if allowed, '0' if not allowed
{1}'1' if allowed, '0' if not allowed

1321 **Network traffic analysis for PCHID *{0}* set to own partition.**

Explanation

Substitution variables are:

*{0}*PCHID number

1322 **Network traffic analysis for PCHID *{0}* set to all partitions.**

Explanation

Substitution variables are:

*{0}*PCHID number

1323 **Network traffic analysis for PCHID *{0}* set to stop.**

Explanation

Substitution variables are:

*{0}*PCHID number

1324 **User *{0}* has been disabled for *{1}* minutes because of too many invalid logon attempts.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Number of minutes user logon is disabled

1325 **User *{0}* is no longer disabled from logging on.**

Explanation

Substitution variables are:

*{0}*User name

1326 **The managed objects role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*Role name

1327 **The task role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*Role name

1328 **The time zone was changed from *{0}* to *{1}*.**

Explanation

Substitution variables are:

*{0}*Old time zone
*{1}*New time zone

1329 **The time zone is currently set to *{0}*.**

Explanation

Substitution variables are:

*{0}*Time zone

1330 **The security log is within *{0}* percent of the maximum size; it should be archived to avoid loss of data.**

Explanation

Substitution variables are:

*{0}*Percentage of available space

1331 **The user *{0}* logged into the underlying console operating system platform.**

Explanation

Substitution variables are:

*{0}*User name

1332 **The user *{0}* logged out of the underlying console operating system platform.**

Explanation

Substitution variables are:

*{0}*User name

1333 **The console internal firewall blocked an incoming packet from *{0}* for port *{1}* using protocol *{2}*.**

Explanation

Substitution variables are:

*{0}*Origin machine
*{1}*Port number
*{2}*Protocol

1334 **A concurrent CP upgrade was performed. Current number of *{1}* are *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor type
*{1}*Number of processors

1335	**Logical partition group control settings were changed.**
1336	**The backup file was written to the backup destination by Hardware Management Console *{0}***

Explanation

Substitution variables are:

*{0}*HMC Network ID.NAU

1337	**There was an ERROR writing the backup file to the backup destination using Hardware Management Console *{0}***

Explanation

Substitution variables are:

*{0}*HMC Network ID.NAU

1338	**Exclusive control was enabled by user *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

1339	**Exclusive control was disabled by user *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

1340	**An attempt for user *{0}* to log on failed.**

Explanation

Substitution variables are:

*{0}*User name

1341	**The user profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*User profile name

1342	**Start system anchor record upgrade.**
1343	**System anchor record upgrade was successful.**
1344	**System anchor record upgrade was cancelled.**
1345	**System anchor record upgrade was partially successful.**
1346	**System anchor record upgrade failed.**
1347	**Start permanent entitlement record upgrade.**

1348	**Permanent entitlement record upgrade was successful.**
1349	**Permanent entitlement record upgrade was cancelled.**
1350	**Permanent entitlement record upgrade was partially successful.**
1351	**Permanent entitlement record upgrade failed.**
1352	**Start temporary entitlement record upgrade for record ID *{0}*.**

Explanation

Substitution variables are:

*{0}*Record identifier

1353	**Temporary entitlement record upgrade was successful.**
1354	**Temporary entitlement record upgrade was cancelled.**
1355	**Temporary entitlement record upgrade was partially successful.**
1356	**Temporary entitlement record upgrade failed.**
1357	**Start channel LICCCC upgrade.**
1358	**Channel LICCCC upgrade was successful.**
1359	**Channel LICCCC upgrade was cancelled.**
1360	**Channel LICCCC upgrade was partially successful.**
1361	**Channel LICCCC upgrade failed.**
1362	**Start DIMM upgrade.**
1363	**DIMM upgrade was successful.**
1364	**DIMM upgrade was cancelled.**
1365	**DIMM upgrade was partially successful.**
1366	**DIMM upgrade failed.**
1367	**Permanent entitlement record is being staged**
1368	**Permanent entitlement record was staged successfully**
1369	**Permanent entitlement record failed to stage.**
1370	**The staged permanent entitlement record is being deleted.**
1371	**The staged permanent entitlement record has been deleted.**
1372	**The staged permanent entitlement record failed to delete.**
1373	**Temporary entitlement record is being staged**
1374	**Temporary entitlement record was staged successfully**
1375	**Temporary entitlement record failed to stage.**
1376	**The staged temporary entitlement record *{0}* is being deleted.**

Explanation

Substitution variables are:

*{0}*Record identifier

1377	**The staged temporary entitlement record has been deleted.**
1378	**The staged temporary entitlement record failed to delete.**

1379 **Activation of a temporary entitlement record *{0}* has started.**

Explanation

Substitution variables are:

*{0}*Record identifier

1380 **Activation of a temporary entitlement record was successful.**

1381 **Activation of a temporary entitlement record was cancelled.**

1382 **Activation of a temporary entitlement record was partially successful.**

1383 **Activation of a temporary entitlement record failed.**

1384 **Removal of the temporary entitlement record ID *{0}* has started.**

Explanation

Substitution variables are:

*{0}*Record identifier

1385 **Removal of a temporary entitlement record was successful.**

1386 **Removal of a temporary entitlement record failed.**

1387 **Processors are pending activation when available.**

1388 **Partition *{0}* has been assigned to use media on *{1}* by user *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*NAU : User name
*{2}*User name

1389 **Partition *{0}* is no longer assigned to media on *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*NAU : User name

1390 **Partition *{0}* is no longer assigned to media on *{1}* by request of user *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*NAU : User name
*{2}*User name

1391 **Preload save upgrade data from the primary Support Element to the alternate Support Element started.**

1392 **Preload save upgrade data from the primary Support Element to the alternate Support Element completed successfully.**

1393 **Preload save upgrade data from the primary Support Element to the alternate Support Element failed. *{0}***

Explanation

Substitution variables are:

*{0}*Reason for the failure

1394 **The zeroize of usage domain *{0}* for cryptographic number *{1}* in logical partition *{2}* was successful.**

Explanation

Substitution variables are:

*{0}*Usage domain
*{1}*Cryptographic number
*{2}*Image name

1395 **The zeroize of usage domain(s) *{0}* for cryptographic number *{1}* was successful.**

Explanation

Substitution variables are:

*{0}*Usage domains
*{1}*Cryptographic number

1396 **The zeroize of usage domain *{0}* for cryptographic number *{1}* in logical partition *{2}* is deferred until configured online.**

Explanation

Substitution variables are:

*{0}*Usage domain
*{1}*Cryptographic number
*{2}*Image name

1397 **Telephone number *{0}* is no longer available for call-home connectivity. A new one should be configured.**

Explanation

Substitution variables are:

*{0}*Telephone number

1398 **Cryptographic controls were changed for active partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

1399 **Logical processor settings were changed for active partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

1400 **The code load was successful, but the Support Element could not connect back to the Hardware Management Console to send final report.**

Messages 1401-1500

1401 **Configuration data was copied to the USB memory stick.**

1402 **Retrieving a permanent entitlement record from support system.**

1403 **Retrieval of a permanent entitlement record from support system was successful.**

1404 **Retrieval of a permanent entitlement record from support system failed.**

1405 **Retrieving a temporary entitlement record from support system.**

1406 **Retrieval of a temporary entitlement record from support system was successful.**

1407 **Retrieval of a temporary entitlement record from support system failed.**

1408 **User *{0}* has *{1}* from *{2}* to session id *{4}*. The user''s maximum role is *{5}*.**

Explanation

Substitution variables are:

*{0}*User name
{1}'logged on' or 'reconnected'
{2}'the console', or the IP address of the user interface, or 'an unknown location'
*{4}*Logon session identifier
*{5}*User's maximum user role if known or 'unknown'

1409 **User *{0}* has *{1}* from session id *{2}* for the reason: *{3}***

Explanation

Substitution variables are:

*{0}*User name
{1}'logged off' or 'disconnected'
*{2}*Logon session identifier
*{3}*Reason why the session was logged off or disconnected

1410 **User *{0}* of session *{1}* has forcibly *{2}* user *{3}* of session *{4}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
{2}'logged off' or 'disconnected'
*{3}*Forced off user name
*{4}*Forced off logon session identifier

1411 **Hardware Management Console *{0}* is unable to be used as a call home server because it has no customer information configured.**

Explanation

Substitution variables are:

*{0}*HMC name

1412 **The following disruptive operation started: Activate. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}*. *{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1413 **The following disruptive operation started: Configure channel off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1414 **The following operation started: Concurrent switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}*. *{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1415 **The following operation started: Disruptive switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}*. *{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID

*{5}*Single object operation NAU

1416 **The following disruptive operation started: Deactivate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1417 **The following disruptive operation started: Disable concurrent patch. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1418 **The following disruptive operation started: Install code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1419 **The following disruptive operation started: Load. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID

*{5}*Single object operation NAU

1420 **The following disruptive operation started: Power off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1421 **The following disruptive operation started: Power-on reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1422 **The following disruptive operation started: PSW restart. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1423 **The following disruptive operation started: Remove code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1424 **The following disruptive operation started: Reset I/O Interface. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1425 **The following disruptive operation started: Run checkout tests. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1426 **The following disruptive operation started: Set clock. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1427 **The following disruptive operation started: Stop. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1428 **The following disruptive operation started: Sysplex timer configuration change. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1429 **The following disruptive operation started: System reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1430 **The following disruptive operation started: System reset normal for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*. At this time, the user was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address
*{5}*Single object operation Network ID
*{6}*Single object operation NAU

1431 **The following disruptive operation started: System reset clear for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*. At this time, the user was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type

*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address
*{5}*Single object operation Network ID
*{6}*Single object operation NAU

1432 **The following disruptive operation started: Unknown. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1433 **The following disruptive operation started: Activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1434 **The following disruptive operation started: Configure channel off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1435 **The following operation started: Concurrent switch. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1436 **The following operation started: Disruptive switch. It was requested by *{0}* from *{1}*.*{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}*.*{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1437 **The following disruptive operation started: Deactivate. It was requested by *{0}* from *{1}*.*{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}*.*{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1438 **The following disruptive operation started: Disable concurrent patch. It was requested by *{0}* from *{1}*.*{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}*.*{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

*{6}*Single object operation IP address

1439 **The following disruptive operation started: Install code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1440 **The following disruptive operation started: Load. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1441 **The following disruptive operation started: Power off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1442 **The following disruptive operation started: Power-on reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type

*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1443 **The following disruptive operation started: PSW restart. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1444 **The following disruptive operation started: Remove code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1445 **The following disruptive operation started: Reset I/O Interface. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1446 **The following disruptive operation started: Run checkout tests. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1447 **The following disruptive operation started: Set clock. It was requested by *{0}* from *{1}*.*{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}*.*{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1448 **The following disruptive operation started: Stop. It was requested by *{0}* from *{1}*.*{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}*.*{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1449 **The following disruptive operation started: Sysplex Timer configuration change. It was requested by *{0}* from *{1}*.*{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}*.*{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

*{6}*Single object operation IP address

1450 **The following disruptive operation started: System reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{7}*) was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1451 **The following disruptive operation started: System reset normal for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*. At this time, the user (at IP address *{7}*) was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Target
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address
*{5}*Single object operation Network ID
*{6}*Single object operation NAU
*{7}*Single object operation IP address

1452 **The following disruptive operation started: System reset clear for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*. At this time, the user (at IP address *{7}*) was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Target
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address
*{5}*Single object operation Network ID
*{6}*Single object operation NAU
*{7}*Single object operation IP address

1453 **The following disruptive operation started: Unknown. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1454	**Blocking of automatic microcode installation has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled
*{1}*User name
*{2}*IP address or host name [IP address] if host name differs from IP address

1455	**The operating system upgrade was successful.**
1456	**The operating system upgrade encountered a problem copying system files from /bom directory.**
1457	**User *{0}* of session *{1}* has switched from user interface "*{2}*" to "*{3}*".**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*Old user interface style
*{3}*New user interface style

1458	**Prepare system for discontinuance started**
1459	**Prepare system for discontinuance ended with errors**
1460	**Prepare system for discontinuance ended**
1461	**Cleanup discontinuance started**
1462	**Cleanup discontinuance ended with errors**
1463	**Cleanup discontinuance ended**
1464	**Send processor change notification started**
1465	**Send processor change notification ended with errors**
1466	**Send processor change notification ended**
1467	**Data Replication being enabled**
1468	**Data Replication being disabled**
1469	**The following internal code changes were retrieved from hard drive by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1470 **The following internal code changes were installed by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1471 **The following internal code changes were removed by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1472 **The following internal code changes were accepted by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1473 **The following internal code changes were deleted by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1474 **The following internal code changes were retrieved from mass storage media by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1475 **The following internal code changes were retrieved from the server by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1476 **A failure occurred retrieving the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1477 **A failure occurred installing the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1478 **A failure occurred deleting the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1479 **A failure occurred removing the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1480 **A failure occurred accepting the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1481 **The reset profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1482 **The load profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1483 **The image profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1484 **The system activity profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

1485 **The reset profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1486 **The load profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1487 **The image profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1488 **The system activity profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

1489 **The reset profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1490 **The load profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1491 **The image profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1492 **The system activity profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

1493 **The reset profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1494 **The load profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1495 **The image profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1496 **The system activity profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

1497 **The reset profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1498 **The load profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1499 **The image profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1500 **The system activity profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

Messages 1501-1600

1501 **The reset profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1502 **The load profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1503 **The image profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1504 **The system activity profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1505 **The reset profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1506 **The load profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID

*{2}*NAU
*{3}*Interface requesting the change

1507 **The image profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1508 **The system activity profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1509 **The reset profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1510 **The load profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1511 **The image profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1512 **The system activity profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1513 The reset profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1514 The load profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1515 The image profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1516 The system activity profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1517 The reset profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID

*{2}*NAU
*{3}*Interface requesting the change

1518 **The load profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1519 **The image profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1520 **The system activity profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1521 **The reset profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1522 **The load profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

*{4}*Origin IP address

1523 **The image profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1524 **The system activity profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1525 **The reset profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1526 **The load profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1527 **The image profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1528 **The system activity profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1529 **The reset profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1530 **The load profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1531 **The image profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1532 **The system activity profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1533 **The reset profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1534 **The load profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1535 **The image profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1536 **The system activity profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name

*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1537 **The reset profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1538 **The load profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1539 **The image profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1540 **The system activity profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1542 **The group profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1543 **The group profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1544 **The group profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1545 **The group profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1546 **The group profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1547 **The group profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1548 **The group profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1549 **The group profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1550 **The group profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1551 **The group profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1552 **The group profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1553 **The group profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1554 **The group profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1555 **The group profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1556 **The group profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1557 **The reset profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1558 **The load profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1559 **The image profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1560 **The system activity profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1561 **The group profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1562 **The reset profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1563 **The load profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1564 **The image profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1565 **The system activity profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1566 **The group profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1567 **The reset profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1568 **The load profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1569 **The image profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1570 **The system activity profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1571 **The group profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1572 **The reset profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1573 **The load profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1574 **The image profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1575 **The system activity profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1576 **The group profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1577 **The reset profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1578 **The load profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1579 **The image profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1580 **The system activity profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1581 **The group profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1582 **The reset profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*. *{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1583 **The load profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1584 **The image profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1585 **The system activity profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1586 **The group profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1587 **The reset profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1588 **The load profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1589 **The image profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1590 **The system activity profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1591 **The group profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1592 **The reset profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1593 **The load profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1594 **The image profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1595 **The system activity profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1596 **The group profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1597 **The reset profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1598 **The load profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1599 **The image profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1600 **The system activity profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

Messages 1601-1700

1601 **The group profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1602 **The reset profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1603 **The load profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1604 **The image profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1605 **The system activity profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1606 **The group profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1607 **The reset profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1608 **The load profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1609 **The image profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1610 **The system activity profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1611 **The group profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1612 **The reset profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1613 **The load profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1614 **The image profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1615 **The system activity profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1616 **The group profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1617 **The reset profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1618 **The load profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1619 **The image profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1620 **The system activity profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1621 **The group profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1622 **The reset profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1623 **The load profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1624 **The image profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1625 **The system activity profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1626 **The group profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1627 **The reset profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1628 **The load profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1629 **The image profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1630 **The system activity profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1631 **The group profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1632 **The reset profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name
*{4}*Origin IP address

1633 **The load profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1634 **The image profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1635 **The system activity profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1636 **The group profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1637 **The reset profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1638 **The load profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1639 **The image profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1640 **The system activity profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1641 **The group profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

*{4}*Origin IP address

1642 **The reset profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1643 **The load profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1644 **The image profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1645 **The system activity profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1646 **The group profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1647 **The reset profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*. *{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1648 **The load profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*. *{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1649 **The image profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1650 **The system activity profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1651 **The group profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1652 **The reset profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1653 **The load profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1654 **The image profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1655 **The system activity profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name

*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1656 **The group profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1657 **The reset profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1658 **The load profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1659 **The image profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1660 **The system activity profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1661 **The group profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1662 **The reset profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1663 **The load profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1664 **The image profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

*{4}*Origin IP address

1665 **The system activity profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1666 **The group profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1667 **The reset profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1668 **The load profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1669 **The image profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1670 **The system activity profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1671 **The group profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1672 **The reset profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1673 **The load profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1674 **The image profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1675 **The system activity profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1676 **The group profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1677 **The reset profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1678 **The load profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name

*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1679 **The image profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1680 **The system activity profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1681 **The group profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1682 **The server *{0}* with key type *{1}* was added to the Network Time Protocol (NTP) configuration file.**

Explanation

Substitution variables are:

*{0}*NTP server name
*{1}*Key type of the NTP server

1683 **The server *{0}* with key type *{1}* and symmetric key value *{2}* was added to the Network Time Protocol (NTP) configuration file.**

Explanation

Substitution variables are:

*{0}*NTP server name
*{1}*Key type of the NTP server
*{2}*Symmetric key value of the NTP server

1684 **The server *{0}* was removed from the Network Time Protocol (NTP) configuration file.**

Explanation

Substitution variables are:

*{0}*NTP server name

1685 **The server *{0}* version *{1}* was removed from the Network Time Protocol (NTP) configuration file.**

Explanation

Substitution variables are:

*{0}*NTP server name
*{1}*Key type of the NTP server

1686 **The console has been enabled as a Network Time Protocol (NTP) client.**

1687 **The console is no longer enabled as a Network Time Protocol (NTP) client.**

1688 **The console has been enabled as a Network Time Protocol (NTP) server.**

1689 **The console is no longer enabled as a Network Time Protocol (NTP) server.**

1690 **The Network Time Protocol (NTP) service has detected an error and disabled itself.**

1691 **User *{0}* has attempted to log on from location *{1}* with a user identification or password that was not valid. The user''s maximum role is *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*IP address
*{2}*User's maximum user role

1692 **An attempt for user *{0}* to log on from location *{1}* failed.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*IP address

1693 **Logical partition weight settings were changed by a scheduled operation.**

1694 **The Support Element's service call logical processor event manager attempted, but could not send configuration management data (event type 04) to the following system(s): *{0}*.**

Explanation

Substitution variables are:

*{0}*Image names

1695 **Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* completed, but not all functions may be available until the next system activation. Additionally, one or more active partitions did not respond to new function notification.**

Explanation

Substitution variables are:

*{0}*System EC number

1696 **Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* completed, All functions are available but one or more active partitions did not respond to new function notification.**

Explanation

Substitution variables are:

*{0}*System EC number

1697 **Temporary On/Off CoD resources were converted to permanent resources during power-on reset**

1698 **Start add I/O drawer phase 1.**

1699 **Add I/O drawer phase 1 was successful.**

1700 **Add I/O drawer phase 1 failed.**

Messages 1701-1800

1701 **Start add I/O drawer phase 2.**

1702 **Add I/O drawer phase 2 was successful.**

1703 **Add I/O drawer phase 2 failed.**

1704 **Start remove I/O drawer phase 1.**

1705 **Remove I/O drawer phase 1 was successful.**

1706 **Remove I/O drawer phase 1 failed.**

1707 **Start remove I/O drawer phase 2.**

1708 **Remove I/O drawer phase 2 was successful.**

1709 **Remove I/O drawer phase 2 failed.**

1710 **Battery operated clock old time (prior to turning on network time protocol).**

1711 **A Change LPAR controls scheduled operation was started from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*NAU
*{1}*Network ID

1712 **Network traffic analysis for PCHID *{0}* port *{1}* set to own partition.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*Port number

1713 **Network traffic analysis for PCHID *{0}* port *{1}* set to all partitions.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*Port number

1714 **Network traffic analysis for PCHID *{0}* port *{1}* set to all data on port.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*Port number

1715 **Network traffic analysis for PCHID *{0}* port *{1}* set to stop.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*Port number

1716 **Start permanent entitlement record pre-check.**

1717 **Permanent entitlement record pre-check was successful.**

1718 **Permanent entitlement record pre-check was cancelled.**

1719 **Permanent entitlement record pre-check was partially successful.**

1720 **Permanent entitlement record pre-check failed.**

1731 **HiperSockets network traffic analyzer authorization has changed.**

1732 **HiperSockets network traffic analyzer authorization has been disabled.**

1733 **The LPAR control profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1734 **The LPAR control profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1735 **The LPAR control profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1736 **The LPAR control profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1737 **The LPAR control profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1738 **The LPAR control profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1739 **The LPAR control profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1740 **The LPAR control profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1741 **The LPAR control profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1742 **The LPAR control profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1743 **The LPAR control profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1744 **The LPAR control profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1745 **The LPAR control profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1746 **The LPAR control profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1747 **The LPAR control profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1748 **The LPAR control profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1749 **The LPAR control profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1750 **The LPAR control profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1751 **The LPAR control profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1752 **The LPAR control profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

*{4}*Origin IP address

1753 **The LPAR control profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1754 **The LPAR control profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1755 **The LPAR control profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1756 **The LPAR control profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1757 **The LPAR control profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1758 **The LPAR control profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1759 **The LPAR control profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1760 **The LPAR control profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1761 **The LPAR control profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1762 **The LPAR control profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1763 **The LPAR control profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1764 **The LPAR control profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1765 **The LPAR control profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1766 **The LPAR control profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1767 **The LPAR control profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1768 **The LPAR control profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1769 **The LPAR control profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID

*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1770 **The LPAR control profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1771 **The LPAR control profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1772 **The LPAR control profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1773 **The LPAR control profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1774 **The LPAR control profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1775 **The LPAR control profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1776 **The LPAR control profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1777 **The LPAR control profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1778 **A change LPAR controls scheduled operation failed. The request for the following partition(s) resulted in a WLM / capping conflict:\n *{0}***

Explanation

Substitution variables are:

*{0}*Image names

1779 **The user *{0}* opened an ssh session into the underlying console operating system platform from *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*HMC name

1780 **The user *{0}* ssh session closed.**

Explanation

Substitution variables are:

*{0}*User name

1781 **RSF diagnostic test trace output was saved as *{0}*.**

Explanation

Substitution variables are:

*{0}*File name of the TCP dump

1782 **The static power savings mode for this system has been enabled.**

1783 **The static power savings mode for this system has been disabled.**

1790 **LPAR controls profiles were exported.**

1791 **LPAR controls profiles were imported.**

1800 **RSF diagnostic query size operation detected *{0}* MCL files totalling *{1}* bytes.**

Explanation

Substitution variables are:

*{0}*Number of MCL files
*{1}*Number of bytes in all MCL files

Messages 1801-1900

1801 **The user template *{0}* was added.**

Explanation

Substitution variables are:

*{0}*Template name

1802 **The user template *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Template name

1803 **The user template *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Template name

1804 **The process to copy a backup file to backup media is about to start *{0}* .**

Explanation

Substitution variables are:

*{0}*Information about the backup file and backup media.

1805 **Concurrent internal code changes for PU core started.**

1806 **Concurrent internal code changes for PU core completed.**

1807 **Concurrent internal code changes for PU core failed.**

1808 **The console has been enabled as a Network Time Protocol (NTP) client. This message was recorded *{0}* seconds after the previous NTP message.**

Explanation

Substitution variables are:

*{0}*Number seconds

1809 **Power Cap settings have changed.**

1810 **The activation of an incompatible UDX image for cryptographic coprocessor *{0}* was successfully forced. Timestamp: *{1}*, Name: *{2}***

Explanation

Substitution variables are:

*{0}*Cryptographic number
*{1}*Timestamp
*{2}*UDX image name

1811 **The activation of the factory default image for cryptographic coprocessor *{0}* was successfully forced.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1812 **Replenishment of the temporary entitlement record ID *{0}* has started.**

Explanation

Substitution variables are:

*{0}*Temporary entitlement record identifier

1813 **Replenishment of the temporary entitlement record ID *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Temporary entitlement record identifier

1814 **Replenishment of the Temporary entitlement record ID *{0}* failed.**

Explanation

Substitution variables are:

*{0}*Temporary entitlement record identifier

1848 **The pending activation of the factory default image for cryptographic coprocessor *{0}* was successfully cancelled.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1849 **The following systems are not entitled for remote service: *{0}*.**

Explanation

Substitution variables are:

*{0}*Machine type and machine serial number of all systems not entitled.

1851 **Extracting and validating file *{0}* using key for family *{1}***

Explanation

Substitution variables are:

*{0}*PK1 file name
*{1}*Machine family

1852 **The user pattern *{0}* was added.**

Explanation

Substitution variables are:

*{0}*Pattern name

1853 **The user pattern *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Pattern name

1854 **The user pattern *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Pattern name

1883 **Power save enabled.**

1889 **Battery-operated clock has been adjusted by *{0}* milliseconds over the last *{1}* hours.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

*{1}*Time was adjusted over the last hours

1890 **Unable to obtain time from the CPC. The battery-operated clock for this console might not be accurate.**

1891 **Battery-operated clock has been adjusted by *{0}* milliseconds.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

1892 **Battery-operated clock has been adjusted by *{0}* millisecond over the last *{1}* hours.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted
*{1}*Amount of time that was adjusted over the last hours

1893 **Battery-operated clock has been adjusted by *{0}* milliseconds over the last hour.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

1894 **Battery-operated clock has been adjusted by *{0}* millisecond over the last hour.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

1895 **Battery-operated clock has been adjusted by *{0}* millisecond.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

1896 **The shared memory used by the backup has been already released.**

Messages 1901-2000

1915 **PMH *{0}* updated with transmitted service data**

Explanation

Substitution variables are:

*{0}*PMH number

1916 **CPC Firmware embedded framework control code load started.**

1917 **CPC Firmware embedded framework control code load completed successfully.**

1918 **CPC Firmware embedded framework control code load failed.**

1919 **Concurrent internal code changes for CPC firmware embedded framework control code started.**

1920	**Concurrent internal code changes for CPC firmware embedded framework control code completed.**
1921	**Concurrent internal code changes for CPC firmware embedded framework control code failed.**
1922	**Activation of this image was not performed.**
1923	**Software Maintenance Agreement (SWMA) has been validated.**
1924	**The firmware network adapter parameters were created for image *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

1925	**The firmware network adapter parameters were changed for image *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

1926	**The configuration type of cryptographic number *{0}* has been changed to a cryptographic EP11 coprocessor.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1927	**Start Feature on demand update.**
1928	**Feature on demand update was successful.**
1929	**Feature on demand update was cancelled.**
1930	**Feature on demand update was partially successful.**
1931	**Feature on demand update failed.**
1932	**Feature on demand record is being staged**
1933	**Feature on demand record was staged successfully**
1934	**Feature on demand record failed to stage.**
1935	**The staged feature on demand record is being deleted.**
1936	**The staged feature on demand record has been deleted.**
1937	**The staged feature on demand record failed to delete.**
1938	**Removal of a feature on demand has started.**
1939	**Removal of a feature on demand was successful.**
1940	**Removal of a feature on demand failed.**
1941	**User *{0}* has logged on to Web Services API session *{1}* from location *{2}***

Explanation

Substitution variables are:

*{0}*User name

*{1}*Session log identifier
*{2}*IP address and possibly host name if host name can be determined. If a client tag was specified on the login attempt it is also provided here.

1942 **User *{0}* has logged off from Web Services API session *{1}* due to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Session log identifier
*{2}*Reason for logoff.

1943 **Modem is not supported on this version of the HMC. *{0}* is disabled.**

Explanation

Substitution variables are:

*{0}*Function that is no longer supported

1944 **Call-home has been disabled on this HMC. You must configure an internet connection to enable remote support.**

1945 **Check of on hold internal code changes has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled
*{1}*User name
*{2}*IP address and optional host name

1946 **Starting install of the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*Collections to install , jcc is a collection an MCL?

1947 **Starting remove of the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*Collections to remove , jcc is a collection an MCL?

1948 **Authentication KEY created on primary Support Element.**

1949 **Authentication KEY sent to the alternate Support Element.**

1950 **Authentication KEY restored from the alternate Support Element.**

1951 **A flash memory allocation was added for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Logical partition name

1952 **A flash memory allocation was removed for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Logical partition name

1953 **A flash memory allocation was changed for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Logical partition name

1954 **Start remove I/O disruptively.**

1955 **Remove I/O disruptively was successful.**

1956 **Remove I/O disruptively failed.**

1957 **User *{0}* successfully logged on using pattern *{2}* with a template of *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*User pattern
*{2}*User template

1958 **Battery operated clock set to new time obtained directly from NTP server.**

1959 **Concurrent internal code changes for PCI support partition code started.**

1960 **Concurrent internal code changes for PCI support partition code completed.**

1961 **Concurrent internal code changes for PCI support partition code failed.**

1962 **The Monitor System Events task failed to send an email to *{0}* with a message count of *{1}* for sources *{2}* due to exception *{3}*.**

Explanation

Substitution variables are:

*{0}*Destination email address
*{1}*The index of the message in the queue
*{2}*Sources jcc, need a better description of Sources
*{3}*Description of the error

1964 **The current absolute capping value for the *{0}* CPs in partition *{1}* changed from *{2}* to *{3}*.**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*Old absolute capping value
*{3}*New absolute capping value

1965 **The current absolute capping value for the *{0}* CPs in partition *{1}* changed from None to *{2}*.**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*New absolute capping value

1966 **The current absolute capping value for the *{0}* CPs in partition *{1}* changed from *{2}* to None.**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*Old absolute capping value

1967 **TSD request was sent to the Support Element**

1968 **Smart card has been inserted into Support Element.**

1969 **The file *{0}* is to large to be sent to the support system.**

Explanation

Substitution variables are:

*{0}*File name

1986 **The backup file is going to be written to a removable media.**

1987 **The backup file is going to be written to a FTP server.**

1989 **Task *{0}* with identifier *{1}* started by user *{2}* in session *{3}*.**

Explanation

Substitution variables are:

*{0}*Task name
*{1}*Unique task identifier
*{2}*User name
*{3}*Logon session identifier

1990 **Task *{0}* with identifier *{1}* started by user *{2}* in session *{3}*; targets are: *{4}***

Explanation

Substitution variables are:

*{0}*Task name
*{1}*Unique task identifier
*{2}*User name
*{3}*Logon session identifier
*{4}*Names of the targets for the task

1991 **Task *{0}* with identifier *{1}* for user *{2}* has ended.**

Explanation

Substitution variables are:

*{0}*Task name
*{1}*Unique task identifier
*{2}*User name

1992	**Start generic feature on demand update.**
1993	**Generic feature on demand update was successful.**
1994	**Generic feature on demand update was cancelled.**
1995	**Generic feature on demand update was partially successful.**
1996	**Generic feature on demand update failed.**
1997	**The remote service configuration data was updated.**
1998	**The user role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*User role name

1999	**The user role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*User role name

2000	**The user role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*User role name

Messages 2001-2100

2001	**The user role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*User role name

2002	**The user role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*User role name

2004	**Concurrent internal code changes for self boot engine started.**
2005	**Concurrent internal code changes for self boot engine completed.**
2006	**Concurrent internal code changes for self boot engine code failed.**

2007 **User *{0}* has acknowledged viewing license information.**

Explanation

Substitution variables are:

*{0}*User name

2008 **Start request was initiated for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2009 **Start request has ended successfully for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2010 **Start request has ended with failure for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2011 **Stop request was initiated for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2012 **Stop request has ended successfully for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2013 **Stop request has ended with failure for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2016 **Start request for system *{0}* was cancelled.**

Explanation

Substitution variables are:

*{0}*CPC name

2017 **Concurrent internal code changes for master control support partition started.**

2018	**Concurrent internal code changes for master control support partition completed.**
2019	**Concurrent internal code changes for master control support partition failed.**
2020	**Start request was initiated for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2021	**Start request has ended successfully for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2022	**Start request has ended with failure for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2023	**Stop request was initiated for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2024	**Stop request has ended successfully for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2025	**Stop request has ended with failure for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2026	**Start request for partition *{0}* was cancelled.**

Explanation

Substitution variables are:

*{0}*Partition name

2027	**Stop request for system *{0}* was cancelled.**

Explanation

Substitution variables are:

*{0}*CPC name

2028 **A licensed internal code error detected by Hardware Management Console *{0}* caused the disablement of the installation and activation of internal code changes.**

Explanation

Substitution variables are:

*{0}*Origin HMC

2029 **User *{0}* of session *{1}* was switched from user interface "*{2}*" to "*{3}*" because Dynamic Partition Manager was enabled on a CPC *{4}* permitted to this user.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*Old user interface style
*{3}*New user interface style
*{4}*Names of the CPC's that forced the UI style change.

2030 **The zeroize of the cryptographic configuration was partially successful.**

2031 **User *{0}* was not permitted to log on since the userid is disabled due to inactivity.**

Explanation

Substitution variables are:

*{0}*User name

2032 **Virtual Flash Memory values for partition *{0}* are: *{1}* GB (initial), *{2}* GB (current), *{3}* GB (maximum).**

Explanation

Substitution variables are:

*{0}*Logical partition name
*{1}*initial Virtual Flash Memory amount
*{2}*current Virtual Flash Memory amount
*{3}*maximum Virtual Flash Memory amount

2033 **The shared secret key for user *{0}* has been reset.**

Explanation

Substitution variables are:

*{0}*User name

2034 **The cryptographic UDX image *{0}* was successfully imported from *{1}* using *{2}*.**

Explanation

Substitution variables are:

*{0}*UDX image name
*{1}*Host name
*{2}*FTP protocol type

2035 **The Mobile App preferences were changed by *{0}*. App enabled: *{1}* to *{2}* Require app password enabled: *{3}* to *{4}* Password caching enabled: *{5}* to *{6}* Actions enabled: *{7}* to *{8}* Notifications enabled: *{9}* to *{10}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*App enabled old value
*{2}*App enabled new value
*{3}*Require app password enabled old value
*{4}*Require app password enabled new value
*{5}*Password caching enabled old value
*{6}*Password caching enabled enabled new value
*{7}*Actions enabled old value
*{8}*Actions enabled new value
*{9}*Notifications enabled old value
*{10}*Notifications enabled new value

2036 **Notification preferences for the Mobile app were changed by *{0}* on device *{1}* for *{2}*. Notifications for this device are *{3}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Device token
*{2}*System name
{3}'disabled' or 'enabled'

2037 **All notification registrations cleaned for user *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

2038 **All notification registrations cleaned for device *{0}*.**

Explanation

Substitution variables are:

*{0}*Device token

2039 **All notification registrations cleaned for system with serial number *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC serial number

2040 **Power save disabled.**

2042 **User *{0}* has logged on to BCPii API session *{1}* from source *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*API session identifier
*{2}*Name for the source of the request

2043 **User *{0}* has logged off from BCPii API session *{1}* due to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*API session identifier
*{2}*Reason for logoff

2044 **The system BCPii Permissions have been altered.**

2046 **The corresponding BCPii permissions for image profile *{0}*.**

Explanation

Substitution variables are:

*{0}*The image profile name.

2047 **The corresponding BCPii permissions entry *{1}* for image profile *{0}*.**

Explanation

Substitution variables are:

*{0}*The image profile name.
*{1}*The log entry number.

2048 **Multi-factor authentication has changed.**

2049 **The corresponding Change LPAR Security BCPii permissions for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*The logical partition name.

2050 **The corresponding Change LPAR Security BCPii permissions entry *{1}* for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*The logical partition name.
*{1}*The log entry number.

2051 **Concurrent internal code changes for EDiF appliance started.**

2052 **Concurrent internal code changes for EDiF appliance completed.**

2053 **Concurrent internal code changes for EDiF appliance failed.**

2054 **A CA certificate was added to the EDiF trust store for *{0}***

Explanation

Substitution variables are:

*{0}*SE name

2055 **A server certificate was added to the EDiF trust store for *{0}***

Explanation

Substitution variables are:

*{0}*SE name

2056 **A new CA signed certificate is now set as the active certificate for *{0}***

Explanation

Substitution variables are:

*{0}*SE name

2057 **A new self-signed certificate was created and set as the active certificate for *{0}***

Explanation

Substitution variables are:

*{0}*SE name

2058 **The wrapping key expiration was successfully changed from *{0}* to *{1}* on *{2}***

Explanation

Substitution variables are:

*{0}*old value
*{1}*new value
*{2}*SE name

2059 **A CA certificate was removed from the EDiF trust store**

2060 **A server certificate was removed from the EDiF trust store**

2061 **The link encryption required was changed from *{0}* to *{1}***

Explanation

Substitution variables are:

*{0}*old value
*{1}*new value

2062 **The link authentication required was successfully changed from *{0}* to *{1}* on *{2}***

Explanation

Substitution variables are:

*{0}*old value
*{1}*new value
*{2}*SE name

2063 **The session key expiration was successfully changed from *{0}* to *{1}***

Explanation

Substitution variables are:

*{0}*old value
*{1}*new value

2064	**A set of activation profiles was changed.**

2065	**A set of activation profiles was changed. It was requested from *{0}.{1}*.**

Explanation

Substitution variables are:

*{1}*Network ID
*{2}*NAU

2066	**A set of activation profiles was changed. It was requested by *{2}* from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2067	**A set of activation profiles was changed. It was requested by *{2}* from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2068	**A set of activation profiles was changed. It was requested by Support Element LIC.**

2069	**A set of activation profiles was changed. It was requested by Support Element(*{2}*) from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2070	**A set of activation profiles was changed. It was requested by Hardware Management Console(*{2}*) from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2071 **A set of activation profiles was changed. It was requested by Support Element(*{2}*) from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2072 **A set of activation profiles was changed. It was requested by Hardware Management Console(*{2}*) from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2073 **A set of activation profiles was imported.**

2074 **A set of activation profiles was imported. It was requested from *{0}.{1}*.**

Explanation

Substitution variables are:

*{1}*Network ID
*{2}*NAU

2075 **A set of activation profiles was imported. It was requested by *{2}* from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2076 **A set of activation profiles was imported. It was requested by *{2}* from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2077 **A set of activation profiles was imported. It was requested by Support Element LIC.**

2078 **A set of activation profiles was imported. It was requested by Support Element(*{2}*) from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2079	**A set of activation profiles was imported. It was requested by Hardware Management Console(*{2}*) from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2080	**A set of activation profiles was imported. It was requested by Support Element(*{2}*) from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2081	**A set of activation profiles was imported. It was requested by Hardware Management Console(*{2}*) from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2082	**Concurrent internal code changes for PCIe Interconnect 2 started.**
2083	**Concurrent internal code changes for PCIe Interconnect 2 completed.**
2084	**Concurrent internal code changes for PCIe Interconnect 2 failed.**
2085	**Concurrent internal code changes for Power Distribution Units started.**
2086	**Concurrent internal code changes for Power Distribution Units completed.**
2087	**Concurrent internal code changes for Power Distribution Units failed.**
2088	**Concurrent internal code changes for Top of Rack Switch started.**
2089	**Concurrent internal code changes for Top of Rack Switch completed.**
2090	**Concurrent internal code changes for Top of Rack Switch failed.**
2091	**Concurrent internal code changes for BPA Controller started.**
2092	**Concurrent internal code changes for BPA Controller completed.**
2093	**Concurrent internal code changes for BPA Controller failed.**

2094 **Concurrent internal code changes for Cooling Unit Controller started.**

2095 **Concurrent internal code changes for Cooling Unit Controller completed.**

2096 **Concurrent internal code changes for Cooling Unit Controller failed.**

2097 **The following internal code changes were deleted because they are on hold: *{0}*.**

Explanation

Substitution variables are:

*{0}*Engineering change numbers

2098 **A load will be attempted for system *{0}*. The load type is NVMe load. Refer to the security log for more details.**

Explanation

Substitution variables are:

*{0}*Image name

2099 **A load will be attempted for system *{0}*. The load type is NVMe dump. Refer to the security log for more details.**

Explanation

Substitution variables are:

*{0}*Image name

Messages 3201-3300

3263 **The *{0}* object was defined. Its serial number is *{1}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*Serial number

3264 **The *{0}* object was undefined. Its serial number was *{1}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*Serial number

3265 **Failed to copy *{0}* file from backup DVD into hard drive.**

Explanation

Substitution variables are:

*{0}*File name

3266 **Failed to extract file *{0}* from the ASN.1 formatted backup PK1 file.**

Explanation

Substitution variables are:

*{0}*File name

3267 **Failed to validate backup tar file *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

3268 ***{0}* logs were removed.**

Explanation

Substitution variables are:

*{0}*Number of logs deleted

3269 ***{0}* logs were removed for the time period *{1}* UTC to *{2}* UTC.**

Explanation

Substitution variables are:

*{0}*Number of logs deleted
*{1}*Start time
*{2}*End time

Messages 3301-3400

3315 **The primary Support Element failed to send its backup file to the alternate Support Element.**

3316 **The primary Support Element successfully sent its backup file to the alternate Support Element.**

3317 **The backup file was created successfully. *{0}***

Explanation

Substitution variables are:

*{0}*The name and size of the backup file

3318 **SSLv3 protocol support has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled
*{1}*User name
*{2}*IP address and optional host name

3319 **RC4 cipher support has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*enabled or disabled
*{1}*User name; empty if unknown
*{2}*IP address and optional host name; empty if unknown

3320 **TLSv12 protocol support has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled
*{1}*User name
*{2}*IP address and optional host name

3321 **There is no alternate Support Element; therefore the primary Support Element backup file will remain only on the primary hard drive.**

Messages 4001-4100

4051 **A device monitor event occurred; Device Type: *{0}*, Action: *{1}*, Vendor: *{2}*, Model: *{3}*, Serial: *{4}***

Explanation

Substitution variables are:

*{0}*Device type
*{1}*Event type
*{2}*Vendor name
*{3}*Device model number
*{4}*Device serial number

4061 **The following role(s) \n *{0}* \n have changed.**

Explanation

Substitution variables are:

*{0}*User role names

4100 **The service state for PDU side *{0}* has been enabled.**

Explanation

Substitution variables are:

*{0}*PDU side for which service state has been enabled.

Messages 4101-4200

4101 **The service state for PDU side *{0}* has been disabled**

Explanation

Substitution variables are:

*{0}*PDU side for which service state has been disabled.

Messages 5001-5100

5000 ***{0}* application opened.**

Explanation

Substitution variables are:

*{0}*Application name

5001 ***{0}*** **application closed.**

Explanation

Substitution variables are:

*{0}*Application name

5002 **Crypto adapter passphrase logon with profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5003 **Crypto adapter group passphrase logon with profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5004 **Crypto adapter group member passphrase logon with member *{0}*.**

Explanation

Substitution variables are:

*{0}*Member name

5005 **Crypto adapter smart card logon with profile *{0}*. Logon key ID: *{1}*. Card ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Key identifier
*{2}*Card identifier

5006 **Crypto adapter group smart card logon with profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5007 **Crypto adapter group member smart card logon with member *{0}*. Logon key ID: *{1}***

Explanation

Substitution variables are:

*{0}*Member name
*{1}*Key identifier

5008 **Crypto adapter logoff for profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5010 ***{0}*** **application failed to open. Return code** ***{1}*****.**

Explanation

Substitution variables are:

*{0}*Application name
*{1}*Return code number

5011 ***{0}*** **application exited with return code** ***{1}*****.**

Explanation

Substitution variables are:

*{0}*Application name
*{1}*Return code number

5012 **Crypto adapter passphrase logon failure with profile** ***{0}*****.**

Explanation

Substitution variables are:

*{0}*Profile name

5013 **Crypto adapter group passphrase logon failure with profile** ***{0}*****.**

Explanation

Substitution variables are:

*{0}*Profile name

5014 **Crypto adapter group member passphrase logon failed for member** ***{0}*****.**

Explanation

Substitution variables are:

*{0}*Member name

5015 **Crypto adapter smart card logon failure with profile** ***{0}*****. Card ID:** ***{1}*****.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Card id number

5016 **Crypto Adapter Group Smart Card Logon Failure with Profile** ***{0}*****.**

Explanation

Substitution variables are:

*{0}*Profile name

5017 **Crypto Adapter Group Member Smart Card Logon Failed for Member** ***{0}*****.**

Explanation

Substitution variables are:

*{0}*Member name

5018 **Crypto Adapter Logoff failed.**

5019 **Crypto Adapter Change Passphrase Failure with Profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5100 **Deleting Key *{0}* from TKE Workstation DES Key Storage.**

Explanation

Substitution variables are:

*{0}*Key name

Messages 5101-5200

5101 **Deleting Key *{0}* from TKE workstation PKA key storage. Key ID: *{1}***

Explanation

Substitution variables are:

*{0}*Key name
*{1}*Key identifier

5102 **Deleting Key *{0}* from TKE workstation AES key storage.**

Explanation

Substitution variables are:

*{0}*Key name

5110 **Delete Key *{0}* from TKE workstation DES key storage failed.**

Explanation

Substitution variables are:

*{0}*Key name

5111 **Delete Key *{0}* from TKE workstation PKA Key storage failed.**

Explanation

Substitution variables are:

*{0}*Key name

5112 **Delete Key *{0}* from TKE workstation AES Key storage failed.**

Explanation

Substitution variables are:

*{0}*Key name

5120 **A signature key was loaded. Authority index: *{0}*, Key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index number
*{1}*Key identifier

5121 **The signature key was unloaded. Authority index: *{0}*, Key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index number
*{1}*Key identifier

5122 **A *{0}* was deleted from a smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Type of key deleted
*{1}*Card identifier
*{2}*Zone identifier

5123 **A *{0}* was copied to a smart card. Source card ID: *{1}*, Source zone ID: *{2}*, Target card ID: *{3}*, Target zone ID: *{4}***

Explanation

Substitution variables are:

*{0}*Type of key copied
*{1}*Source card identifier
*{2}*Source zone identifier
*{3}*Target card identifier
*{4}*Target zone identifier

5124 **A key part of type *{0}* was generated to print file *{2}* with description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key type description
*{2}*File name

5125 **A key part of type *{0}* was generated to binary file *{2}* with description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key type description
*{2}*File name

5126 **Generated signature key with index *{0}* to file *{1}* in *{2}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*File name
*{2}*Directory name

5127 **Generated signature key with index *{0}* to TKE workstation PKA key storage.**

Explanation

Substitution variables are:

*{0}*Authority index

5128 **Generated signature key with index *{0}* to smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Card identifier
*{2}*Zone identifier

5129 **Deleted authority signature key with index *{0}* on smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Card identifier
*{2}*Zone identifier

5130 **Generated RSA key to file *{0}*, Key ID: *{1}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Key identifier

5131 **RSA key was loaded to the host. Key ID: *{0}* Loaded to location: *{1}***

Explanation

Substitution variables are:

*{0}*Key identifier
*{1}*Dataset

5132 **Enciphered RSA key to file *{0}*, Key ID: *{1}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Key identifier

5133 **Generated an administrator signature key on a smart card. Name: *{0}*, SKI: *{1}*, Card ID: *{2}*, Zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Authority name
*{1}*Subject key identifier
*{2}*Card idendifier
*{3}*Zone identifier

5134 **Deleted an administrator signature key from a smart card. Name: *{0}*, SKI: *{1}*, Card ID: *{2}*, Zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Authority name
*{1}*Subject key identifier
*{2}*Card identifier
*{3}*Zone idenditier

5135 **A binary file key part was copied to a smart card. Source binary file: *{0}*, Target card ID: *{1}*, Target zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Target card identifier
*{2}*Target zone identifier

5150 **Failure loading a signature key. Authority index: *{0}*, Key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Key identifier

5151 **Failure during smart card delete. Card ID: *{0}*, Zone ID: *{1}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier

5152 **Failure during smart card copy. Source card ID: *{0}*, Source zone ID: *{1}*, Target card ID: *{2}*, Target zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Source card identifier
*{1}*Source zone identifier
*{2}*Target card identifier
*{3}*Target zone identifier

5153 **A key part of type *{0}* failed generation to print file *{2}* with description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key description
*{2}*File name

5154 **A key part of type *{0}* failed generation to binary file *{2}* with description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key description
*{2}*File name

5155 **Failed to generate authority signature key with index *{0}* to file.**

Explanation

Substitution variables are:

*{0}*Authority index

5156 **Failed to generate authority signature key with index *{0}* to TKE workstation PKA key storage.**

Explanation

Substitution variables are:

*{0}*Authority index

5157 **Failed to generate authority signature key with index *{0}* to smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Card identifier
*{2}*Zone identifier

5158 **Failed to delete authority signature key with index *{0}* on smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Card identifier
*{2}*Zone identifier

5159	**Failed to generate RSA key to file.**
5160	**Load of RSA key failed.**
5161	**Encipher of RSA key failed.**
5162	**Failure generating an administrator signature key on a smart card. Card ID: *{0}*, Zone ID: *{1}*, Failure details: *{2}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier
*{2}*Failure details

5163	**Failure deleting an administrator signature key from a smart card. Card ID: *{0}*, Zone ID: *{1}*, Failure details: *{2}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier
*{2}*Failure details

5164	**Failure during binary file to smart card copy. Source binary file: *{0}*, Target card ID: *{1}*, Target zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Target card identifier
*{2}*Target zone identifier

5200	**A valid PIN was entered for *{0}* in *{1}*. Card ID: *{2}*, Zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card reader description
*{2}*Card identifier
*{3}*Zone idendifier

Messages 5201-5300

5201	**A key part was generated on smart card in reader *{0}*. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Reader number
*{1}*Card identifier
*{2}*Zone identifier

5202 **Secure key entry to smart card in *{0}* completed. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Reader number
*{1}*Card identifier
*{2}*Zone identifier

5250 **Failure during PIN entry for *{0}* in *{1}*. Card ID: *{2}*, Zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card reader description
*{2}*Card identifier
*{3}*Zone identifier

5251 **Tried to access a *{0}* with a blocked PIN. Card ID: *{1}*, Zone ID: *{2}*, Operation: *{3}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Zone identifier
*{3}*Operation

5252 **Tried to access a *{0}* not in the same zone as the TKE crypto adapter. Card ID: *{1}*, Card Zone ID: *{2}*, TKE crypto adapter zone ID: *{3}*, Operation: *{4}***

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Card zone identifier
*{3}*Crypto adapter zone identifier
*{4}*Operation

5253 **Failure during key part generation using reader *{0}*. Card ID: *{1}*, Zone ID: *{2}*, Key type: *{3}*, Key description: *{4}***

Explanation

Substitution variables are:

*{0}*Reader number

*{1}*Card identifier
*{2}*Zone identifier
*{3}*Key type
*{4}*Key description

5254 **Secure key entry failed to smart card in *{0}*. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Card reader description
*{1}*Card identifier
*{2}*Zone identifier

5300 **The crypto module description has been updated to *{0}*.**

Explanation

Substitution variables are:

*{0}*New description

Messages 5301-5400

5301 **Released crypto module.**

5302 **Forced release of crypto module.**

5303 **Reserved crypto module.**

5304 **Load role issued to create a module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Role description

5305 **Load role issued to change a module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Role description

5306 **Delete module-wide role issued. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Role description

5307 **Load authority issued to create a module-wide authority. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Authority index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email address
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5308 **Load authority issued to change a module-wide authority. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Authority index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email address
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5309 **Delete module-wide authority issued. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Authority index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email address
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5310 **Host user ID *{0}* logged onto host *{1}* with mixed case password support set to *{2}*.**

Explanation

Substitution variables are:

*{0}*User identifier
*{1}*Host name

*{2}*Mixed case choice

5311 **Logoff host *{0}***

Explanation

Substitution variables are:

*{0}*Host name

5312 **Host *{0}* opened.**

Explanation

Substitution variables are:

*{0}*Host name

5313 **Host user ID *{0}* logged onto group *{1}* with mixed case password support set to *{2}*.**

Explanation

Substitution variables are:

*{0}*User identifier
*{1}*Group name
*{2}*Mixed case choice

5314 **Group *{0}* opened.**

Explanation

Substitution variables are:

*{0}*Group name

5315 **Host Query for environment settings, Time = *{0}*, ICSF FMID = *{1}*, Date = *{2}*, Access control = *{3}*.**

Explanation

Substitution variables are:

*{0}*Time
*{1}*Function modification identifier
*{2}*Date
*{3}*Host access control

5316 **A key part of type *{0}* was loaded to key part register labeled *{1}* in domain *{2}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key label
*{2}*Domain index

5317 **A key part of type *{0}* with description *{1}* and label *{2}* was loaded to TKE workstation key storage.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key description
*{2}*Key label

5318 **Key part register labeled *{0}* completed for domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*Domain index

5319 **Operational key part register *{0}* was cleared for for domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*Domain index

5320 ***{0}* Register in domain *{1}* was cleared.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index

5321 **Crypto module in index *{0}* was disabled by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Key identifier

5322 **Command enable crypto module for crypto module in index *{0}* was issued.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5323 **Command enable crypto module for crypto module in index *{0}* was cosigned by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Key identifier

5324 **Zeroize issued for domain index *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5325 **Zeroize cosigned for domain index *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5326 **Changed signature key index from *{0}* to *{1}*.**

Explanation

Substitution variables are:

*{0}*Old index
*{1}*New index

5327 **Load role issued to update domain controls for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5328 **Pending command *{2}* deleted by authority index *{1}* on host crypto module index *{0}*, TSN: *{3}*, Signature key ID: *{4}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Command
*{3}*Tower serial number
*{4}*Key identifier

5329 **Pending command *{2}* cosigned by authority index *{1}* on host crypto module index *{0}*, TSN: *{3}*, Signature key ID: *{4}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Command
*{3}*Tower serial number
*{4}*Key identifier

5330 **Crypto module with ID *{0}* was authenticated and *{1}* by the user.**

Explanation

Substitution variables are:

*{0}*Crypto module identifier
*{1}*Authentication result

5331 **The *{0}* Register in domain *{1}* was loaded. *{2}* Key part hash: *{3}***

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index
*{2}*Key part loaded
*{3}*Key part hash

5332 **The *{0}* Register for domain *{1}* was set.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index

5333 **Not authorized to verb *{0}* on TKE workstation crypto adapter.**

Explanation

Substitution variables are:

*{0}*Verb name

5334 **Configuration information from file *{0}* was applied to the crypto module at index *{1}* on host *{2}*. *{3}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Crypto module index
*{2}*Host identifier
*{3}*Audit text

5335 **Configuration information was collected from the crypto module at index *{0}* on host *{1}* and saved in the file *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Host identifier
*{2}*File name

5336 **The crypto module at index *{0}* on host *{1}* was enrolled in migration zone *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Host identifier
*{2}*Zone identifier

5337 **An IA smart card has approved applying configuration data to a target crypto module or domain group. Card ID: *{0}*, Zone ID: *{1}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier

5338 **A KPH smart card has approved rewrapping the transport key during configuration migration. Card ID: *{0}*, Zone ID: *{1}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier

5339 **The default key wrapping method for *{0}* was changed to *{1}* for domain *{2}*.**

Explanation

Substitution variables are:

*{0}*Token type
*{1}*Wrapping method
*{2}*Domain index

5340 **Decimalization tables were activated in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. Tables activated:**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5341 **Decimalization tables were deleted in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. Tables deleted: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Deleted table list

5342 **Decimalization tables were loaded in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. Tables loaded: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Loaded table list

5343 **Restricted PINs were activated in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. PINs activated: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Activated pins list

5344 **Restricted PINs were deleted in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. PINs deleted: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Deleted pins list

5345 **Restricted PIN loaded in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. PIN loaded: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Loaded pins list

5346 **Data set *{0}* on host *{1}* was allocated successfully.**

Explanation

Substitution variables are:

*{0}*Data set name
*{1}*Host name

5347 **Coordinated change master key for data set type *{0}* domain *{1}* crypto module *{2}* host *{3}* was successful.**

Explanation

Substitution variables are:

*{0}*Data set type
*{1}*Domain index
*{2}*Crypto module index
*{3}*Host name

5348 **Access control tracking *{0}* request was issued for domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Request type
*{1}*Domain index

5349 **The clock on the crypto module on host *{0}* at index *{1}* was set to *{2}*.**

Explanation

Substitution variables are:

*{0}*Host
*{1}*Crypto module index
*{2}*New time

5350 **Certificate with label *{0}* was activated in domain *{1}* using authority index *{2}*, signature key ID: *{3}*.**

Explanation

Substitution variables are:

*{0}*Label name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5351 **Certificate label changed from *{0}* to *{1}* in domain *{2}* using authority index *{3}*, signature key ID: *{4}*.**

Explanation

Substitution variables are:

*{0}*Old label name
*{1}*New label name
*{2}*Domain index
*{3}*Authority index
*{4}*Signature key identifier

5352 **Deleted certificate *{0}* from domain *{1}* using authority index *{2}*, signature key ID: *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name

*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5353 **Certificate with label *{0}* was loaded in domain *{1}* using authority index *{2}*, signature key ID: *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5354 **Certificate with label *{0}* was replaced in domain *{1}* using authority index *{2}*, signature key ID: *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5355 **Load role issued to create a domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain inde

5356 **Load role issued to change a domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5357 **Delete domain-specific role issued for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5358 **Load authority issued to create a domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5359 **Load authority issued to change a domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5360 **Delete domain-specific authority issued for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telphone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5361 **Enter imprint mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5362 **Enter imprint mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5363 **Enter PCI-compliant mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5364 **Enter PCI-compliant mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5365 **Exit PCI-compliant mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5366 **Exit PCI-compliant mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5367 **Enter migration mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5368 **Enter migration mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5369 **Exit migration mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5370 **Exit migration mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5371 **Migration mode was extended 24 hours for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5372 **Clear secure audit log issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5373 **Clear secure audit log cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5374 **Load role cosigned to create a module-wide role by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5375 **Load role cosigned to change a module-wide role by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5376 **Delete module-wide role cosigned by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5377 **Load authority cosigned to create a module-wide authority by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5378 **Load authority cosigned to change a module-wide authority by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5379 **Delete module-wide authority cosigned by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5380 **Load role cosigned to create a domain-specific role for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index

*{1}*Authority index
*{2}*Signature key identifier

5381 **Load role cosigned to change a domain-specific role for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5382 **Delete domain-specific role cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5383 **Load authority cosigned to create a domain-specific authority for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5384 **Load authority cosigned to change a domain-specific authority for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5385 **Delete domain-specific authority cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5386 **Load role cosigned to update domain controls for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5387 **Exit imprint mode completed for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5400 **A Crypto module description update failed for description: *{0}*.**

Explanation

Substitution variables are:

*{0}*Description

Messages 5401-5500

5401 **Failed to release crypto module.**

5402 **Failed to force release of crypto module reserved by *{0}*.**

Explanation

Substitution variables are:

*{0}*Reserver

5403 **Failed to reserve crypto module.**

5404 **Failure issuing Load role to create a module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description

5405 **Failure issuing Load role to change a module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description

5406 **Failure issuing Delete module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description

5407 **Failure issuing Load authority to create a module-wide authority. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5408 **Failure issuing Load authority to change a module-wide authority. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telphone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5409 **Failure issuing Delete module-wide authority. Index: *{1}*, name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5410 **User *{0}* logon failed for host *{1}* with mixed case password support set to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Host name
*{2}*Mixed case setting

5411 **Host *{0}* failed to open.**

Explanation

Substitution variables are:

*{0}*Host name

5412 **User *{0}* logon failed for group *{1}* with mixed case password support set to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Group name
*{2}*Mixed case setting

5413 **Group *{0}* failed to open.**

Explanation

Substitution variables are:

*{0}*Group name

5414 **Host Query for environment settings failed, Time = *{0}*, ICSF FMID = *{1}*, Date = *{2}*, Access control = *{3}*.**

Explanation

Substitution variables are:

*{0}*Time
*{1}*Function modification identifier
*{2}*Date
*{3}*Access control

5415 **A key part of type *{0}* with description *{1}* failed to load to key part register labeled *{2}*.**

Explanation

Substitution variables are:

*{0}*Key part type
*{1}*Key part description
*{2}*Key part label

5416 **A key part of type *{0}* with description *{1}* and label *{2}* failed to load into TKE workstation key storage.**

Explanation

Substitution variables are:

*{0}*Key part type
*{1}*Key part description
*{2}*Key part label

5417 **Key part register labeled *{0}* failed completion.**

Explanation

Substitution variables are:

*{0}*Key label

5418 **Operational key part register labeled *{0}* failed to be cleared.**

Explanation

Substitution variables are:

*{0}*Key label

5419 **Failed to clear *{0}* Register in domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*Domain index

5420 **Crypto module in index *{0}* failed to be disabled by authority index *{1}*, signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Key identifier

5421 **Failure issuing enable of crypto module in index *{0}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5422 **Failure cosigning enable of crypto module in index *{0}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5423 **Failure issuing zeroize of domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5424 **Failure issuing Load role to update domain controls for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5425 **Pending command *{2}* deletion failure by authority index *{1}* on host crypto module index *{0}*, TSN: *{3}*, Signature key ID: *{4}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Command type
*{3}*Tower serial number
*{4}*Key identifier

5426 **Pending command *{2}* cosign failure by authority index *{1}* on host crypto module index *{0}*, TSN: *{3}*, Signature key ID: *{4}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Command type
*{3}*Tower serial number
*{4}*Key identifier

5427 **Crypto module authentication failure for crypto module with ID *{0}*.**

Explanation

Substitution variables are:

*{0}*Crypto module identifier

5428 **Failure loading the *{0}* Register in domain *{1}*. *{2}***

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index
*{2}*Key part

5429 **Failure setting the *{0}* Register for domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index

5430 **Error in *{0}* task of configuration migration utility: *{1}***

Explanation

Substitution variables are:

*{0}*Task name
*{1}*Error reason

5431 **Error in collect task of configuration migration utility: *{0}***

Explanation

Substitution variables are:

*{0}*Error reason

5432 **Error in enroll task of configuration migration utility: *{0}***

Explanation

Substitution variables are:

*{0}*Error reason

5433 **IA smart card approval failed during apply task of configuration migration.**

5434 **KPH smart card approval failed during apply task of configuration migration.**

5435 **Error occurred when changing the default key wrapping method for *{0}* to *{1}* for domain *{2}*.**

Explanation

Substitution variables are:

*{0}*Token type
*{1}*Wrapping method
*{2}*Domain index

5436 **Activate decimalization tables failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5437 **Delete decimalization tables failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5438 **Load decimalization tables failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5439 **Activate restricted PINs failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5440 **Delete restricted PINs failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5441 **Load restricted PINs failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5442 **Data set *{0}* on host *{1}* allocation failed.**

Explanation

Substitution variables are:

*{0}*Data set name
*{1}*Host name

5443 **Coordinated change master key for data set type *{0}* domain *{1}* crypto module *{2}* host *{3}* failed.**

Explanation

Substitution variables are:

*{0}*Data set type
*{1}*Domain index
*{2}*Crypto module index
*{3}*Host name

5444 **Access control tracking *{0}* request failed for domain *{1}* by authority index *{2}* Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Request type
*{1}*Domain index
*{2}*Authority index
*{3}*Key identifier

5445 **Failure setting the clock on the crypto module on host *{0}* at index *{1}*.**

Explanation

Substitution variables are:

*{0}*Host Name
*{1}*Crypto module index

5446 **Certificate with label *{0}* activate request failed for domain *{1}* by authority index *{2}*, Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate label name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5447 **Failed request to change certificate label from *{0}* to *{1}* for domain *{2}* by authority index *{3}*, Signature key ID *{4}*.**

Explanation

Substitution variables are:

*{0}*Old certificate label name
*{1}*New certificate label name
*{2}*Domain index
*{3}*Authority index
*{4}*Signature key identifier

5448 **Failed request to delete certificate *{0}* for domain *{1}* by authority index *{2}*, Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5449 **Failed request to load certificate *{0}* for domain *{1}* by authority index *{2}*, Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5450 **Failed request to replace certificate *{0}* for domain *{1}* by authority index *{2}*, Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5451 **Failure issuing load role to create a domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5452 **Failure issuing load role to change a domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5453 **Failure issuing Delete domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description

*{2}*Domain index

5454 **Failure issuing Load authority to create a domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5455 **Failure issuing Load authority to change a domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telphone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5456 **Failure issuing Delete domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telphone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier

*{9}*Domain index

5457 **Failure cosigning load role to create a domain-specific role for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5458 **Failure cosigning load role to change a domain-specific role for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5459 **Failure cosigning delete domain-specific role for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5460 **Failure cosigning load authority to create a domain-specific authority for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5461 **Failure cosigning load authority to change a domain-specific authority for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5462 **Failure cosigning Delete domain-specific authority for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5463 **Failure cosigning load role to create a module-wide role.**

5464 **Failure cosigning load role to change a module-wide role.**

5465 **Failure cosigning Delete module-wide role.**

5466 **Failure cosigning load authority to create a module-wide authority.**

5467 **Failure cosigning Load authority to change a module-wide authority.**

5468 **Failure cosigning delete module-wide authority.**

5469 **Failure cosigning zeroize of domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5470 **Failure cosigning load role to update domain controls for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5471 **Failure issuing enter imprint mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5472 **Failure cosigning enter imprint mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5473 **Failure issuing enter PCI-compliant mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5474 **Failure cosigning enter PCI-compliant mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5475 **Failure issuing exit PCI-compliant mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5476 **Failure cosigning exit PCI-compliant mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5477 **Failure issuing enter migration mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5478 **Failure cosigning enter migration mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5479 **Failure issuing exit migration mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5480 **Failure cosigning exit migration mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5481 **Failure extending migration mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5482 **Failure issuing clear secure audit log for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5483 **Failure cosigning clear secure audit log for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5484 **Failure exiting imprint mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5500 **Added a crypto module administrator. Name: *{0}*, SKI: *{1}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Subject key identifier

5501 **Added an administrator to domain *{0}*. Name: *{1}*, SKI: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*name
*{2}*Subject key identifier

5502 **Cleared the current master key in domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5503 **Cleared the new master key in domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5504 **The new master key in domain *{0}* was committed. Verification pattern: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Verification pattern

5505 **A master key in domain *{0}* was set to a random value. Verification pattern: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Verification pattern

5506 **The crypto module at index *{0}* was disabled.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5507 **The crypto module at index *{0}* was enabled.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5508 **An importer key pair was generated for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5509 **An invalid signature key was provided for a command. Command target: *{0}*, Name: *{1}*, SKI: *{2}*.**

Explanation

Substitution variables are:

*{0}*Command target
*{1}*Name
*{2}*Subject key identifier

5510 **The new master key in domain *{0}* was loaded. Number of parts: *{1}*, Final verification pattern: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Number of parts
*{2}*Verification pattern

5511 **Removed a crypto module administrator. Name: *{0}*, SKI: *{1}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Subject key identifier

5512 **Removed an administrator from domain *{0}*. Name: *{1}*, SKI: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Name
*{2}*Subject key identifier

5513 **The EP11 Master Key Register for domain *{0}* was set. Verification pattern: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Verification pattern

5514 **Updated the crypto module attributes.**

5515 **Updated the attributes for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5516 **The control points for domain *{0}* were updated.**

Explanation

Substitution variables are:

*{0}*Domain index

5517 **The crypto module at index *{0}* was zeroized.**

Explanation

Substitution variables are:

*{0}*Domain index

5518 **Domain *{0}* was zeroized.**

Explanation

Substitution variables are:

*{0}*Domain index

5550 **Failure adding a crypto module administator. Name: *{0}*, SKI: *{1}*, Failure details: *{2}***

Explanation

Substitution variables are:

*{0}*Name
*{1}*Subject key identifier
*{2}*Failure details

5551 **Failure adding an administrator to domain *{0}*. Name: *{1}*, SKI: *{2}*, Failure details: *{3}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Name
*{2}*Subject key identifier
*{3}*Failure details

5552 **Failure clearing the current master key in domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5553 **Failure clearing the new master key in domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index

*{1}*Failure details

5554 **Failure committing the new master key in domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5555 **Failure setting a master key in domain *{0}* to a random value. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5556 **Failure disabling the crypto module at index *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5557 **Failure enabling the crypto module at index *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5558 **Failure generating an importer key pair for domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5559 **Failure loading new master key in domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5560 **Failure removing a crypto module administrator. Name: *{0}*, SKI: *{1}*, Failure details: *{2}***

Explanation

Substitution variables are:

*{0}*Name

*{1}*Subject key identifier
*{2}*Failure details

5561 **Failure removing an administrator from domain *{0}*. Name: *{1}*, SKI: *{2}*, Failure details: *{3}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Name
*{2}*Subject key identifier
*{3}*Failure details

5562 **Failure setting the EP11 master key register for domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5563 **Failure updating the crypto module attributes. Failure details: *{0}***

Explanation

Substitution variables are:

*{0}*Failure details

5564 **Failure updating the attributes for domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5565 **Failure updating the control points for domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5566 **Failure zeroizing the crypto module at index *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Failure details

5567 **Failure zeroizing domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5600	**DH Transport key policy set to: Always use current transport key.**

Messages 5601-5700

5601	**DH Transport key policy set to: Always establish new transport key based on current values of Diffie-Hellman modulus and generator.**
5602	**DH Transport key policy set to: Always generate new values of Diffie-Hellman modulus and generator and establish new transport key.**
5603	**Change protocol parameters button was selected. Current DH values have been cleared. New values will be generated when needed.**
5604	**New Diffie-Hellman transport key was generated.**
5605	**New Diffie-Hellman modulus and generator values were generated.**
5610	**DH Transport key policy setting failed: Always use current transport key.**
5611	**DH Transport key policy setting failed: Always establish new transport key based on current values of Diffie-Hellman modulus and generator.**
5612	**DH Transport key policy setting failed: Always generate new values of Diffie-Hellman modulus and generator and establish new transport key.**
5613	**Change protocol parameters button failed selection.**
5614	**New Diffie-Hellman transport key failed generation.**
5615	**New Diffie-Hellman modulus and generator values failed generation.**
5620	**ECDH Transport key policy set to: Always use current transport key.**
5621	**ECDH Transport key policy set to: Always establish new transport key.**
5622	**Change protocol parameters button was selected. Current ECDH parameters have been cleared. New parameters will be used when needed.**
5623	**New ECDH transport key was generated.**
5624	**New ECDH parameters were used.**
5630	**ECDH transport key policy setting failed: Always use current transport key.**
5631	**ECDH transport key policy setting failed: Always establish new transport key.**
5632	**Change protocol parameters button failed selection.**
5633	**New ECDH transport key failed generation.**
5634	**Use new ECDH parameters failed.**
5640	**The CCA CLU utility was opened.**
5641	**The CCA CLU utility was closed.**
5642	**The following CLU command was executed: *{0}***

Explanation

Substitution variables are:

*{0}*Command

5643	**The following CLU command failed during execution: *{0}***

Explanation

Substitution variables are:

*{0}*Command

5644	**The CCA CLU utility output log was cleared.**
5645	**The CCA CLU utility output log clear function failed.**
5646	**The CCA CLU utility command history was cleared.**
5647	**The CCA CLU utility command history clear function failed.**
5650	**Cryptographic node management batch initializer executing script from *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5651	**Cryptographic node management batch initializer job output.**
5652	**The Cryptographic node management batch initializer failed to execute successfully.**
5653	**A Failure occurred displaying cryptographic node management batch initializer output.**
5660	**CCA node management utility - Started *{0}* smart cards supported**

Explanation

Substitution variables are:

*{0}*Smart cards supported setting

5661	**CCA node management utility - Exited**
5662	**CCA node management utility exit failure.**
5670	**Workstation crypto adapter authorizations loaded from *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5671	**Workstation crypto adapter authorization load failure.**
5672	**Workstation crypto adapter existing authorizations cleared.**
5673	**Workstation crypto adapter authorization clear failure.**
5674	**Workstation crypto adapter intrusion latch was reset.**
5675	**Workstation crypto adapter intrusion latch reset failure.**
5676	**Time on workstation crypto adapter synchronized with workstation clock.**
5677	**Workstation crypto adapter time synchronization failure.**
5678	**Workstation crypto adapter was initialized.**
5679	**Workstation crypto adapter initialization failure.**
5680	**Environment ID *{0}* set on the workstation crypto adapter.**

Explanation

Substitution variables are:

*{0}*Environmental identifier

5681 **Workstation crypto adapter environment ID set failure.**

5690 **DES KEK key part *{0}* was opened from *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*File name

5691 **Failure occurred accessing DES KEK key part from *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5692 **DES KEK key part *{0}* was saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*File name

5693 **Failure occurred saving DES KEK key part *{0}* to *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*File name

5694 **DES KEK key part *{0}* loaded.**

Explanation

Substitution variables are:

*{0}*Key label

5695 **Failure occurred loading DES KEK key part *{0}*.**

Explanation

Substitution variables are:

*{0}*Key label

5696 **DES KEK key part *{0}* replaced existing key part.**

Explanation

Substitution variables are:

*{0}*Key label

5697 **Failure occurred replacing DES KEK key part *{0}*.**

Explanation

Substitution variables are:

*{0}*Key label

5698 **PKA key storage initialized to *{0}* by *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Caller

5699 **DES key storage initialized to *{0}* by *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Caller

5700 **AES key storage initialized to *{0}* by *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Caller

Messages 5701-5800

5701 **Failed to initialize PKA key storage.**

5702 **Failed to initialize DES key storage.**

5703 **Failed to initialize AES key storage.**

5704 **Key records in *{0}* key storage were re-enciphered.**

Explanation

Substitution variables are:

*{0}*Storage type

5705 ***{0}* key storage re-encipher failure.**

Explanation

Substitution variables are:

*{0}*Storage type

5706 **Key record in *{0}* key storage created.**

Explanation

Substitution variables are:

*{0}*Storage type

5707 ***{0}* key storage record create failure.**

Explanation

Substitution variables are:

*{0}*Key type

5708 ***{0}*** **key storage record deleted.**

Explanation

Substitution variables are:

*{0}*Key type

5709 ***{0}*** **key storage record delete failure.**

Explanation

Substitution variables are:

*{0}*Key type

5720 **Workstation crypto adapter** ***{0}*** **master** ***{1}*** **set.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key(s)

5721 **Workstation crypto adapter** ***{0}*** **master** ***{1}*** **set failed.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key(s)

5722 **Workstation crypto adapter random** ***{0}*** **master keys set.**

Explanation

Substitution variables are:

*{0}*Key type

5723 **Workstation crypto adapter random** ***{0}*** **master keys set failed.**

Explanation

Substitution variables are:

*{0}*Key type

5724 **Workstation crypto adapter new** ***{0}*** **master** ***{1}*** **successfully cleared.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key(s)

5725 **Workstation crypto adapter clear new *{0}* master *{1}* failed.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key(s)

5726 ***{0}* *{1}* master key part opened from *{2}*.**

Explanation

Substitution variables are:

*{0}*Key part
*{1}*Key type
*{2}*File name

5727 **Failure occurred opening *{0}* master key part from *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*File name

5728 **Workstation crypto adapter *{0}* master key part loaded.**

Explanation

Substitution variables are:

*{0}*Key type

5729 **Workstation crypto adapter *{0}* master key load failure.**

Explanation

Substitution variables are:

*{0}*Key type

5730 ***{0}* master key part saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*File name

5731 ***{0}* master key save failure.**

Explanation

Substitution variables are:

*{0}*Key type

5732 **Workstation crypto adapter *{0}* *{1}* master key part loaded from smart card, *{2}* (*{3}*).**

Explanation

Substitution variables are:

*{0}*Key part
*{1}*Register type
*{2}*Card name
*{3}*Card identifier

5733 **Workstation crypto adapter *{0}* master key part failed to load from smart card *{1}* (*{2}*).**

Explanation

Substitution variables are:

*{0}*Register type
*{1}*Card name
*{2}*Card identifier

5734 ***{0}* *{1}* workstation crypto adapter master key part generated on smart card, *{2}* (*{3}*).**

Explanation

Substitution variables are:

*{0}*Key part
*{1}*Register type
*{2}*Card name
*{3}*Card identifier

5735 **Workstation crypto adapter *{0}* master key part generation to smart card failed. Card ID: *{1}***

Explanation

Substitution variables are:

*{0}*Register type
*{1}*Card identifier

5740 **Workstation crypto adapter access control initialized.**

5741 **Workstation crypto adapter access control initialize failure.**

5742 **Profile (*{0}*) saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Storage medium

5743 **Profile save failure. *{0}***

Explanation

Substitution variables are:

*{0}*Profile name

5744 **Group profile (*{0}*) saved to *{1}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*Storage medium

5745 **Profile (*{0}*) replaced.**

Explanation

Substitution variables are:

*{0}*User name

5746 **Profile (*{0}*) created.**

Explanation

Substitution variables are:

*{0}*Profile name

5747 **Profile create failure.**

5748 **Group profile (*{0}*) replaced.**

Explanation

Substitution variables are:

*{0}*User name

5749 **Group profile (*{0}*) created.**

Explanation

Substitution variables are:

*{0}*User name

5750 **Profile (*{0}*) failure count reset.**

Explanation

Substitution variables are:

*{0}*User name

5751 **Profile failure count reset failure.**

5752 **Profile (*{0}*) passphrase changed.**

Explanation

Substitution variables are:

*{0}*User name

5753 **Profile passphrase change failure.**

5754 **Profile (*{0}*) deleted.**

Explanation

Substitution variables are:

*{0}*User name

5755 **Profile delete failure.**

5756 **Deleting group profile (*{0}*).**

Explanation

Substitution variables are:

*{0}*User name

5757 **Profile (*{0}*) opened from *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*File name

5758 **Group profile (*{0}*) opened from *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*File name

5759 **Failure occurred opening profile from *{0}***

Explanation

Substitution variables are:

*{0}*File name

5770 **Role (*{0}*) deleted.**

Explanation

Substitution variables are:

*{0}*Role identifier

5771 **Role delete failure.**

5772 **Role (*{0}*) saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*File name

5773 **Role Save Failure. (*{0}*)**

Explanation

Substitution variables are:

*{0}*Save error

5774 **Role (*{0}*) loaded to TKE workstation crypto adapter.**

Explanation

Substitution variables are:

*{0}*Role identifier

5775 **Load role failure.**

5776 ***{0}* (*{1}*) PIN changed.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier

5777 **Smart card PIN change failure.**

5778 **A *{0}* was copied to a smart card. Source card ID: *{1}*, Source zone ID: *{2}*, Target card ID: *{3}*, Target zone ID: *{4}***

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Card identifier
*{2}*Source zone identifier
*{3}*Target card identifier
*{4}*Target zone identifier

5779 **Failure during smart card copy. Source card ID: *{0}*, Source zone ID: *{1}*, Target card ID: *{2}*, Target zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Source card identifier
*{1}*Source zone identifier
*{2}*Target card identifier
*{3}*Target zone identifier

5780 **A logon key pair was generated on *{0}* (*{1}*).**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier

5781 **A logon key pair generation failure occurred.**

5782 **A *{0}* was deleted from a smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Card identifier
*{2}*Zone identifier

5783 **Failure during smart card delete. Card ID: *{0}*, Zone ID: *{1}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier

5800 **Smart card utility program - Started**

Messages 5801-5900

5801 **Smart card utility program - Start failed**

5802 **Smart card utility program - Exited**

5803 **Smart card utility program - Exit failed**

5804 **Failure getting smart card description.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5805 **Failure getting PIN information.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5806 **Failure getting zone information.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5807 **Failure getting authority information.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5808 **Failure querying for key parts.**

5809 **Failure getting crypto adapter logon information.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5810 ***{0}*** **PIN was set or changed on** ***{1}*****. Card ID:** ***{2}*****, Card description:** ***{3}*****.**

Explanation

Substitution variables are:

*{0}*Pin position
*{1}*Card type
*{2}*Card identifier
*{3}*Card description

5811 **Failed to set or change the PIN on** ***{0}*****.**

Explanation

Substitution variables are:

*{0}*Smart card type

5812 **The PIN was unblocked on** ***{0}*****. Card ID:** ***{1}*****, Card Description:** ***{2}*****.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Card description

5813 **Failure occurred unblocking** ***{0}*** **PIN.**

Explanation

Substitution variables are:

*{0}*Smart card type

5814 **Successfully backed up** ***{0}*****. Source card ID:** ***{1}*****, Source card description:** ***{2}*****, Target card ID:** ***{3}*****, Zone ID:** ***{4}*****, Zone description:** ***{5}*****.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Source identifier
*{2}*Source description
*{3}*Target identifier
*{4}*Zone identifier
*{5}*Zone description

5815 **Failed to back up** ***{0}*****.**

Explanation

Substitution variables are:

*{0}*Smart card type

5816 ***{0}*** **initialization complete. Card ID:** ***{1}*****, Zone ID:** ***{2}*****, Zone description:** ***{3}*****.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Zone identifier
*{3}*Zone description

5817 **Failure occurred initializing *{0}*.**

Explanation

Substitution variables are:

*{0}*Smart card type

5818 ***{0}* has been personalized. Card ID: *{1}*, Card description: *{2}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Card description

5819 **Failed to personalize *{0}*.**

Explanation

Substitution variables are:

*{0}*Card type

5820 ***{0}* initialization complete. Card description: *{1}*, Card ID: *{2}*, Zone ID: *{3}*, Zone description: *{4}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card description
*{2}*Card identifier
*{3}*Zone identifier
*{4}*Zone description

5821 **Failure occurred initializing *{0}*.**

Explanation

Substitution variables are:

*{0}*Smart card type

5822 ***{0}* enrollment with crypto adapter.**

Explanation

Substitution variables are:

*{0}*Location

5823	**Started ...**
5824	**Completed successfully.**
5825	**TKE smart card (*{0}*) enrolled in zone (*{1}*) successfully.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Zone identifier

5826	**TKE smart card enrollment with crypto adapter failed.**
5827	**Enrollment request from *{0}* for crypto adapter *{1}* was certified by CA smart card (*{2}*) and enrolled in zone (*{3}*)**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Serial number
*{2}*Card identifier
*{3}*Zone identifier

5828	**Saved enrollment request file to *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5829	**Remote enroll with crypto adapter.**
5830	**Remote enroll with crypto adapter failed.**
5831	**Begin remote enroll - Started**
5832	**Begin remote enroll - Failed\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5833	**User cancelled begin remote enroll**
5834	**Begin remote enroll\nUser is replacing certificate in zone (*{0}*)**

Explanation

Substitution variables are:

*{0}*Zone identifier

5835	**Begin remote enroll\nCrypto adapter enrollment request has been stored in file *{0}***

Explanation

Substitution variables are:

*{0}*File name

5836 **Complete remote enroll - Started**

5837 **Complete remote enroll - Failed\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5838 **User cancelled complete remote enroll**

5839 **Complete remote enroll\nUser is replacing certificate in zone (*{0}*)**

Explanation

Substitution variables are:

*{0}*Zode id

5840 **Complete remote enroll\nCrypto adapter *{0}* enrolled in zone (*{1}*) successfully from file (*{2}*)**

Explanation

Substitution variables are:

*{0}*Crypto adapter name
*{1}*Zone identifier
*{2}*File name

5841 **Enrolled *{0}* in alternate zone. Card ID: *{1}*, Card description: *{2}*, Alternate zone ID: *{3}*, Alternate zone description: *{4}*.**

Explanation

Substitution variables are:

*{0}*Card type name
*{1}*Card identifier
*{2}*Card description
*{3}*Alternate zone identifier
*{4}*Alternate zone description

5842 **Failure enrolling *{0}* in alternate zone.**

Explanation

Substitution variables are:

*{0}*Card type name

5843 **Removed alternate zone from *{0}*. Card ID: *{1}*, Card description: *{2}*.**

Explanation

Substitution variables are:

*{0}*Card type name
*{1}*Card identifier
*{2}*Card description

5844 **Failure removing alternate zone from *{0}*.**

Explanation

Substitution variables are:

*{0}*Card type name

5900	**The TKE audit configuration utility opened.**

Messages 5901-6000

5901	**The TKE audit configuration utility failed to open.**
5902	**The TKE audit configuration utility closed.**
5903	**The TKE audit configuration utility failed to close.**
5904	**The TKE audit configuration utility was modified.**
5905	**The auditing function for TKE was started.**
5906	**The auditing function for TKE was stopped.**
5907	**File *{0}* by the edit TKE files task.**

Explanation

Substitution variables are:

*{0}*File function

5908	**An error was encountered while opening the edit TKE files task: *{0}***

Explanation

Substitution variables are:

*{0}*Error message

5909	**Migrate previous TKE Version to TKE 8.1 task completed successfully.**
5910	**Migrate previous TKE Version to TKE 8.1 task failed: *{0}***

Explanation

Substitution variables are:

*{0}*Error message

5911	**The TKE file management utility opened.**
5912	**The TKE file management utility closed.**
5913	**The TKE file management utility failed to open.**
5914	**The TKE file management utility failed to close.**
5915	**File *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5916	**File copy failed: *{0}***

Explanation

Substitution variables are:

*{0}*Error message

5917 **The TKE restricted file chooser was opened.**

5918 **The TKE restricted file chooser failed to open.**

5919 **File *{0}* was saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Directory name

5920 **File save failed: *{0}***

Explanation

Substitution variables are:

*{0}*File name

5921 **File *{0}* from *{1}* was opened.LPAR_SEC_EXECUTION_ON**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Directory name

5922 **File open failed: *{0}***

Explanation

Substitution variables are:

*{0}*Rile name

5923 **File *{0}* was deleted from *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Directory name

5924 **File delete failed: *{0}***

Explanation

Substitution variables are:

*{0}*File name

5925 **File *{0}* was renamed to *{2}* in the *{1}*.**

Explanation

Substitution variables are:

*{0}*Old file name
*{1}*Directory name

*{2}*New file name

5926	**File rename failed: *{0}***

Explanation

Substitution variables are:

*{0}*File name

5927	**The TKE audit record upload configuration utility was opened.**
5928	**The TKE audit record upload configuration utility failed to open.**
5929	**The TKE audit record upload configuration utility was closed.**
5930	**The TKE Audit record upload configuration utility failed to close.**
5931	**TKE Audit record upload settings were modified. *{0}***

Explanation

Substitution variables are:

*{0}*Upload setting

5932	**Failure modifying TKE audit record upload settings.**
5933	**The saved upload timestamp for host *{0}* was reset.**

Explanation

Substitution variables are:

*{0}*Host name

5934	**Host *{0}* was removed from the list of other hosts.**

Explanation

Substitution variables are:

*{0}*Host name

5935	***{0}* was made the current host for audit uploads.**

Explanation

Substitution variables are:

*{0}*Host name

5936	**Host *{0}* was removed as the current host. No current host is selected.**

Explanation

Substitution variables are:

*{0}*Host name

5937	**The upload timestamp for the current host (*{0}*) was reset.**

Explanation

Substitution variables are:

*{0}*Host name

5938 **Host *{0}* was added to the list of other hosts.**

Explanation

Substitution variables are:

*{0}*Host name

5939 **Autostart of audit record upload was enabled.**

5940 **Autostart of audit record upload was disabled.**

5941 **Audit record upload to system *{0}* has started.**

Explanation

Substitution variables are:

*{0}*Host port

5942 **Audit record upload to system *{0}* failed. Status: *{1}*.**

Explanation

Substitution variables are:

*{0}*Host port
*{1}*Status

5943 **Audit record upload to system *{0}* has stopped.**

Explanation

Substitution variables are:

*{0}*Host port

5944 **Audit record upload to system *{0}* failed to stop.**

Explanation

Substitution variables are:

*{0}*Host port

5945 **The TKE configure displayed hash size utility was opened.**

5946 **The TKE configure displayed hash size utility failed to open.**

5947 **The TKE configure displayed hash size utility was closed.**

5948 **The TKE configure displayed hash size utility failed to close.**

5949 **The displayed hash size configuration was changed. *{0}***

Explanation

Substitution variables are:

*{0}*Displayed hash setting

5950 **Attempt to modify displayed hash size configuration failed: *{0}***

Explanation

Substitution variables are:

*{0}*Displayed hash setting

5951	**Hash truncation was enabled, and the maximum displayed hash size was set to *{0}*.**

Explanation

Substitution variables are:

*{0}*Hash size

5952	**Hash truncation was disabled, and full hashes will be displayed.**
5953	**The z/OS enhanced password encryption policy was enabled.**
5954	**The z/OS enhanced password encryption policy was disabled.**
5955	**The z/OS enhanced password encryption policy utility was opened.**
5956	**The z/OS enhanced password encryption policy utility was closed.**
5960	**An error was encountered while reading audit records due to incorrect parameters specified.**
5961	**An error was encountered while writing an audit record due to incorrect parameters specified.**
5962	**Heartbeat audit records will be created.**
5963	**Heartbeat audit interval *{0}* is not one of the pre-defined intervals.**

Explanation

Substitution variables are:

*{0}*Heartbeat interval in error

5964	**The TKE crypto adapter intrusion latch state has changed.**
5965	**The TKE workstation has started.**
5966	**A different TKE crypto adapter has been detected.**
5967	**Heartbeat audit record.**
5968	**Cannot connect to the TKE crypto adapter to check the crypto adapter serial number. There may not be a crypto adapter installed, the crypto adapter may not be reporting in, or the CLU utility may be running.**
5969	**The TKE crypto adapter battery level has changed.**
5997	**TKE audit record\n- TKE workstation profile: *{1}*\n- TKE crypto adapter profile: *{2}*\n- Authority index *{3}*, Key ID:\n*{4}*\n- Event information: *{0}***

Explanation

Substitution variables are:

*{0}*Event information
*{1}*TKE workstation profile
*{2}*Crypto adapter profile
*{3}*Authority index
*{4}*Key identifier

5998	**TKE audit record\n- TKE workstation profile: *{1}*\n- TKE crypto adapter profile: *{2}*\n- Authority index *{3}*, Key ID: *{4}*\n- Event information: *{0}***

Explanation

Substitution variables are:

*{0}*Event information
*{1}*TKE workstation profile
*{2}*Crypto adapter profile
*{3}*Authority index
*{4}*Key identifier

5999 **TKE Audit Record\n- TKE Workstation Profile: *{1}*\n- TKE Crypto Adapter Profile: *{2}*\n- Event Information: *{0}***

Explanation

Substitution variables are:

*{0}*Event information
*{1}*TKE Workstation profile
*{2}*Crypto adapter profile

Messages 6001-6100

6001 **RSF initiated an SSL connection with host *{1}* at address *{3}* authenticated as *{0}* with encryption cipher *{2}***

Explanation

Substitution variables are:

*{0}*Principal name
*{1}*Host name
*{2}*Cipher suite name
*{3}*IP address

6002 **RSF connection failed verification of server certificate at *{0}*, reason: *{1}***

Explanation

Substitution variables are:

*{0}*Host name
*{1}*Failure reason

6003 **RSF initiated an SSL connection with host *{0}***

Explanation

Substitution variables are:

*{0}*Host name

6005 **Call home connection for request *{0}* canceled.**

Explanation

Substitution variables are:

*{0}*Request description

6006 **Call home connection for request *{0}* released.**

Explanation

Substitution variables are:

*{0}*Request description

6007 **RSF request *{0}* will transmit *{1}* files to the Support System. The files may be compressed archives which contain other files that are not currently listed in this entry. The files are as follows:**

Explanation

Substitution variables are:

*{1}*Request description
*{2}*Number of files

6008 **Call home review has been configured to hold the following types of requests: \n *{0}***

Explanation

Substitution variables are:

*{0}*List of held request types

6009 **RSF request *{0}* will transmit no files to the support system.**

Explanation

Substitution variables are:

*{0}*Request description

6051 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}* against the *{4}* object named "*{5}*" (URI:*{6}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*The type of object that was targeted
*{5}*The displayable name of the targeted object (i.e 'Blade 1' or 'Blade 1 within enclosure Foo')
*{6}*The URI being rejected

6052 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}* against the *{4}* object named "*{5}*": *{6}* (URI:*{7}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*The type of object that was targeted
*{5}*The displayable name of the targeted object (i.e 'Blade 1' or 'Blade 1 within enclosure Foo')
*{6}*Provider specific details

*{7}*The URI being rejected

6053 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}* against the *{4}* object named "*{5}*". User does not have permission to the *{6}* named "*{7}*" (URI:*{8}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*The type of object that was targeted
*{5}*The displayable name of the targeted object (i.e 'Blade 1' or 'Blade 1 within enclosure Foo')
*{6}*The type of entity associated with the rejection (typically a 'Task')
*{7}*The displayable name of the entity associated with the rejection
*{8}*The URI being rejected

6054 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}*. User does not have permission to the *{4}* named "*{5}*" (URI:*{6}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*The type of entity associated with the rejection (typically a 'Task')
*{5}*The displayable name of the entity associated with the rejection
*{6}*The URI being rejected

6055 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}*: *{4}* (URI:*{5}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*Provider specific details
*{5}*The URI being rejected

6060 **A request was made by user *{0}* to change the Licensed Internal Code security mode from *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*Username of request initiator
*{1}*Previous Licensed Internal Code security mode
*{2}*New Licensed Internal Code security mode

6061 **An attempt to change the Licensed Internal Code Security mode on the *{0}* from *{1}* to *{2}* has failed.**

Explanation

Substitution variables are:

*{0}*Primary or Alternate system
*{1}*Previous Licensed Internal Code security mode
*{2}*New Licensed Internal Code security mode

6062 **The Licensed Internal Code security mode is *{0}*.**

Explanation

Substitution variables are:

*{0}*Current Licensed Internal Code security mode

6063 **The Primary Licensed Internal Code security mode is *{0}*. The Alternate Licensed Internal Code security mode is *{1}*.**

Explanation

Substitution variables are:

*{0}*Primary Licensed Internal Code security mode
*{1}*Alternate Licensed Internal Code security mode

6070 **Success importing Product Engineering access control file.**

6071 **Failure importing Product Engineering access control file with error: *{0}***

Explanation

Substitution variables are:

*{0}*Detailed error for access control file import failure

6072 **Success removing Product Engineering access control file.**

6073 **Success removing Product Engineering access control file due to expiration.**

Messages 6101-6200

6111 **A Change LPAR Group controls scheduled operation was started from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*NAU
*{1}*Network ID

6112 **Logical partition group control settings were changed by a scheduled operation.**

6120 **Sub-capacity frequency boost is on for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Partition number

6121 **Sub-capacity frequency boost is off for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Partition number

6122 **zIIP capacity boost is on for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*doc=Image name
*{1}*Partition number

6123 **zIIP capacity boost is off for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*doc=Image name
*{1}*Partition number

6124 **Secure execution is on for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*doc=Image name
*{1}*Partition number

6125 **Secure execution is off for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Partition number

6132 **Secure Execution for Linux is enabled for system *{0}*. The global key is *{1}* and the host key is *{2}*.**

Explanation

Substitution variables are:

*{0}*Cpc name
*{1}*global key installed
*{2}*host key installed

6133 **Secure Execution for Linux is disabled for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Cpc name

6140 **User *{0}* successfully started the Recovery Console Boot Server on interface(s) *{1}* using ISO file *{2}* for client with name *{3}*, system type *{4}*, and MAC address(es) *{5}*.**

Explanation

Substitution variables are:

*{0}*user name of user that started server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*name of client system
*{4}*type of client system
*{5}*client MAC address(es) involved in recovery

6141 **User *{0}* successfully started the Recovery Console Boot Server on interface(s) *{1}* using ISO file *{2}* for client with MAC address(es) *{3}*.**

Explanation

Substitution variables are:

*{0}*user name of user that started server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*client MAC address(es) involved in recovery

6142 **User *{0}* successfully stopped the Recovery Console Boot Server that was running on interface(s) *{1}* using ISO file *{2}* for client with name *{3}*, system type *{4}*, and MAC address(es) *{5}*.**

Explanation

Substitution variables are:

*{0}*user name of user that stopped server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*name of client system
*{4}*type of client system
*{5}*client MAC address(es) involved in recovery

6143 **User *{0}* successfully stopped the Recovery Console Boot Server that was running on interface(s) *{1}* using ISO file *{2}* for client with MAC address(es) *{3}*.**

Explanation

Substitution variables are:

*{0}*user name of user that stopped server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*client MAC address(es) involved in recovery

6144 **User *{0}* failed to start the Recovery Console Boot Server on interface(s) *{1}* using ISO file *{2}* for client with name *{3}*, system type *{4}*, and MAC address(es) *{5}*. Failure message: *{6}***

Explanation

Substitution variables are:

*{0}*user name of user that attempted to start server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*name of client system
*{4}*type of client system
*{5}*client MAC address(es) involved in recovery
*{6}*error messsage received from server code

6145 **User *{0}* failed to start the Recovery Console Boot Server on interface(s) *{1}* using ISO file *{2}* for client with MAC address(es) *{3}*. Failure message: *{4}***

Explanation

Substitution variables are:

*{0}*user name of user that attempted to start server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*client MAC address(es) involved in recovery
*{4}*error message received from server code

Additional Product Information

Accessibility, feedback information, notices and trademarks about this product can be found here.

Accessibility

Accessible publications for this product are offered in EPUB format and can be downloaded from Resource Link at http://www.ibm.com/servers/resourcelink.

If you experience any difficulty with the accessibility of any IBM Z and IBM LinuxONE information, go to Resource Link at http://www.ibm.com/servers/resourcelink and click **Feedback** from the navigation bar on the left. In the **Comments** input area, state your question or comment, the publication title and number, choose **General comment** as the category and click **Submit**. You can also send an email to reslink@us.ibm.com providing the same information.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Accessibility features

The following list includes the major accessibility features in IBM Z and IBM LinuxONE documentation, and on the Hardware Management Console and Support Element console:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Customizable display attributes such as color, contrast, and font size
- Communication of information independent of color
- Interfaces commonly used by screen magnifiers
- Interfaces that are free of flashing lights that could induce seizures due to photo-sensitivity.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Consult assistive technologies

Assistive technology products such as screen readers function with our publications, the Hardware Management Console, and the Support Element console. Consult the product information for the specific assistive technology product that is used to access the EPUB format publication or console.

IBM and accessibility

See http://www.ibm.com/able for more information about the commitment that IBM has to accessibility.

Accessibility features

The following list includes the major accessibility features in IBM Z documentation:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Customizable display attributes such as color, contrast, and font size
- Communication of information independent of color
- Interfaces commonly used by screen magnifiers
- Interfaces that are free of flashing lights that could induce seizures due to photo-sensitivity.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. Send your comments by using Resource Link at http://www.ibm.com/servers/resourcelink. Click **Feedback** on the navigation bar on the left. You can also send an email to reslink@us.ibm.com. Be sure to include the name of the book, the form number of the book, the version of the book, if applicable, and the specific location of the text you are commenting on (for example, a page number, table number, or a heading).

Notices

This information was developed for products and services that are offered in the USA. This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION " AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on http://www.ibm.com/trademark.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other product and service names might be trademarks of IBM or other companies.

Class A Notices

The following Class A statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55032. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Statement - Japan

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

The following is a summary of the Japanese VCCI statement above:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan JIS C 61000-3-2 Compliance

（一社）電子情報技術産業協会 高調波電流抑制対策実施要領に基づく定格入力電力値： Knowledge Centerの各製品の仕様ページ参照

For products less than or equal to 20 A per phase, the following statement applies:

高調波電流規格 JIS C 61000-3-2 適合品

For products greater than 20 A, single-phase, the following statements apply:

高調波電流規格 JIS C 61000-3-2 準用品

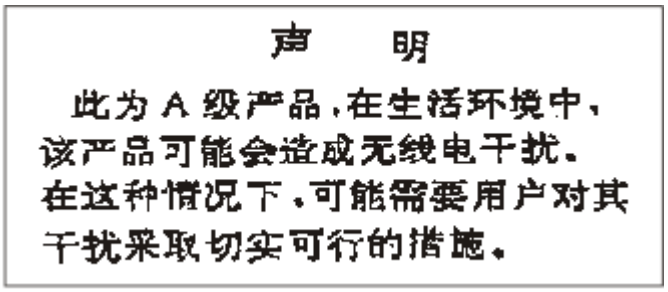
本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
回路分類：6（単相、ＰＦＣ回路付）
換算係数：0

For products greater than 20 A per phase, three-phase, the following statements apply:

高調波電流規格 JIS C 61000-3-2 準用品

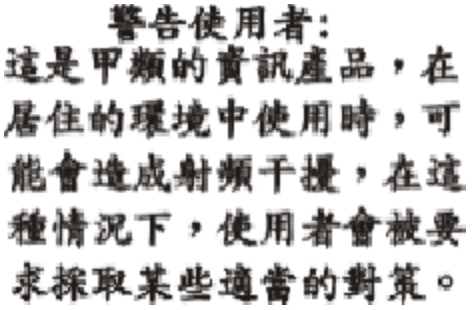
本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
回路分類 ：5（3相、ＰＦＣ回路付）
換算係数 ：0

Electromagnetic Interference (EMI) Statement - People's Republic of China



Declaration: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan



The following is a summary of the Taiwan EMI statement above:

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user will be required to take adequate measures.

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니
판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의
지역에서 사용하는 것을 목적으로 합니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) “. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

Tree Style User Interface

Tree Style User Interface

When you log in to the Hardware Management Console (HMC) for the first time, your browser displays a welcome screen for the Workspace Tour, which describes several improvements to the tree style user interface for this HMC version.

After you complete the tour or if you skip it, your browser display looks like Figure 18 on page 330, which outlines the major interface components of the workspace.

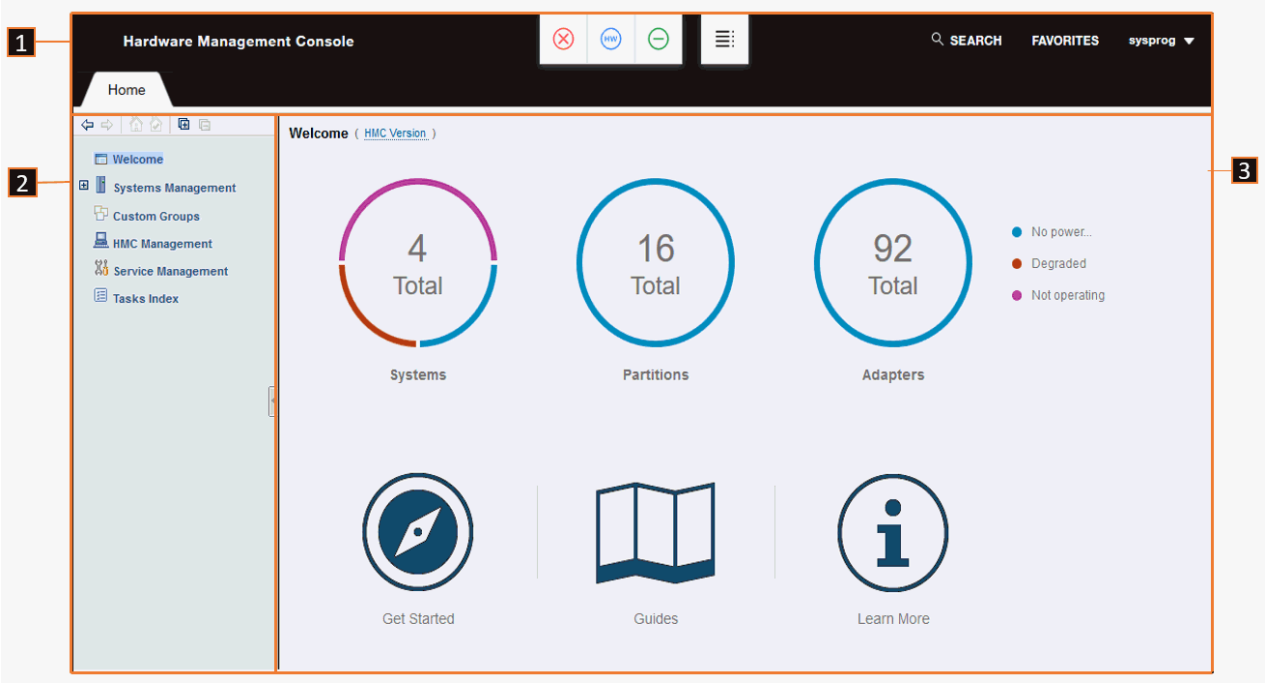


Figure 18. Major components of the HMC workspace

For more details about each workspace component, click the topic link in the list.

1. **Masthead:** The masthead, across the top of the workspace window, provides visual indicators of current overall system status, allows you to quickly find and open tasks; identifies the user name that you used to log in to the HMC; and includes easy access to your favorite tasks.
2. **Navigation pane:** The navigation pane, in the left portion of the workspace window, contains the primary navigation links for managing your system resources and the HMC itself. These links are called *nodes*. Displayed above the navigation pane is the navigation toolbar.
3. **Work pane:** The work pane, in the right portion of the workspace window, displays information based on the current selection from the navigation pane or status bar. The contents of the work pane can vary depending on the type of systems you are managing through the HMC. For example, on the Welcome window, the **Adapters** and **Get Started** icons are displayed only if you are managing one or more systems that have Dynamic Partition Manager (DPM) enabled.
   - For more information about the Welcome window, see Welcome. Note that you can start the Workspace Tour from the Guides link on the Welcome window; that link is highlighted in Figure 18 on page 330.
   - For more information about system and other object displays in the work pane, see Work pane.

You can resize the panes of the Hardware Management Console workspace by moving the mouse pointer over the border that separates the navigation pane from the work pane until the mouse pointer changes to a double-pointed arrow. When the pointer changes shape, press and hold the left mouse button that you drag the mouse pointer to the left or right. Release the button and your navigation pane or work pane is now larger or smaller in size.

Masthead

The HMC masthead, which is located across the top of the workspace window, consists of the four major elements shown in Figure 19 on page 331 .

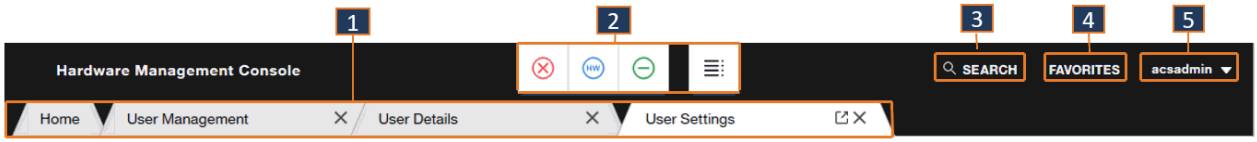


Figure 19. Elements of the HMC masthead

1. Tabbed tasks:
   - The **Home** tab remains on the left of the masthead and displays the tree style user interface for the console.
   - When a task opens, a new tab for that task is opened to the right of the **Home** tab.
   - You can close a task by selecting **X** on the tab.
   - You can open the task into a separate window by selecting the pop-out icon ( ). This capability allows you to view the task window in parallel on a single display, or you can move the task window to other physical displays. Then, you can return the task window back to the tabbed view by selecting the pop-in icon ( ).
   - Tabs of related tasks are grouped together. For example, in Figure 19 on page 331, User Management and User Details are related so their tabs overlap.
   - The following tasks open in a separate window, instead of a tab:
     - Classic System Activity Display
     - Integrated 3270 Console
     - Integrated ASCII Console
     - Open Graphical Console
     - Open Text Console
2. Status icons provide visual indicators of current overall system status. It also contains a status overview icon, which you can select to display more detailed status information in the work pane.
3. **SEARCH** allows you to search for a task by name. Begin typing the task name in the input area. When the task name is displayed, select it to open the task in a new tab.
4. **FAVORITES** is a list of frequently used tasks that you create. Through **FAVORITES**, you can add a task to the list; edit the list by changing a task name; change the order in which the tasks appear, by using the up and down arrows next to the task name; and delete a task from the list.
5. The user name field displays the user name that you used to log in to the HMC. By clicking the drop-down arrow, you can perform the following tasks.
   - Open the **User Settings** task.
   - Access the **Help** for the tree style user interface and expand the Table of contents to access all of the console help.
   - Select **Logout** to open the **Logoff or Disconnect** task.

Navigation Pane

The HMC navigation pane, which is located under the Home tab in the workspace window, contains the primary navigation links for managing your system resources and the Hardware Management Console. It also includes navigation methods that you can use when working with the tree-style workspace. The major elements of the navigation pane are shown in Figure 20 on page 332.

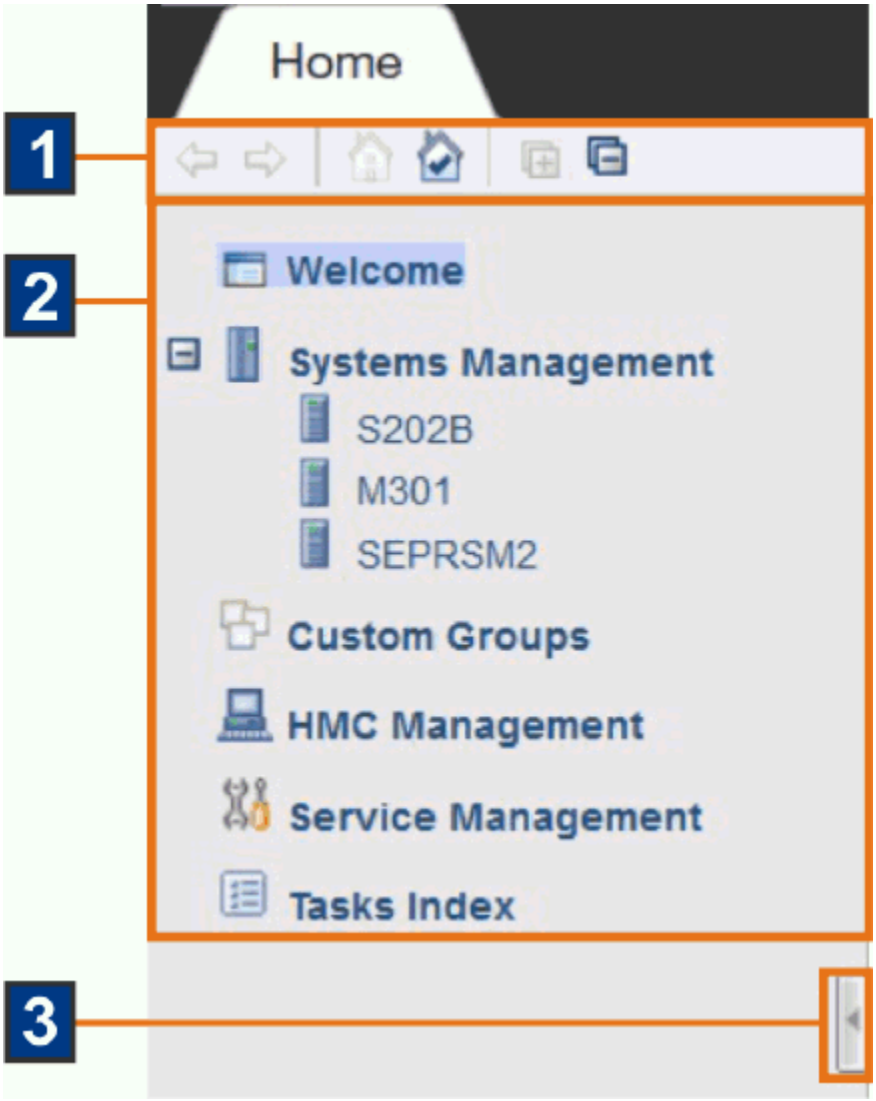


Figure 20. Elements of the HMC navigation pane

1. The toolbar contains several icons to change the navigation pane display.
   - To move forward and backward in the selection history for the work pane, use the forward and backward buttons.
   - To return to the home page during your session and establish a home page to return to every time you log on to the console, use the home page and set home page buttons.
   - To expand and collapse all of the nodes of the navigation pane, use the expand and collapse buttons.

   You can point your mouse over the icon buttons to get a description of the function.
2. The primary navigation links, which are also called *nodes*, change the work pane display so you can manage various system resources or the HMC, or access the list of all HMC tasks. For more details, click a topic link in the following list.
   - Welcome
   - Systems Management
   - “Custom Groups” on page 355
   - HMC Management
   - Service Management
   - Tasks Index

3. The navigation pane collapse and expand controls are provided on the border between the navigation pane and the work pane. You can click these controls to collapse or expand the navigation pane that allows more work area in the work pane, if required. Hovering over these controls indicates whether you are hiding or displaying the navigation pane.

Welcome

When you click the **Welcome** link in the navigation pane, the Welcome window is displayed in the work pane. The major elements of the navigation pane are shown in Figure 21 on page 333.

Figure 21. Major elements of the HMC Welcome window

1. **HMC Version**, which is on the top left of the work pane, displays the current level of the HMC when you hover your cursor over the link.
2. The pie charts indicate the overall status of system resources that you can manage through this HMC. The **Adapters** pie chart is displayed only if you are managing one or more systems that have DPM enabled. For more details about working with the pie charts, see “Pie charts and status legend” on page 334.
3. The support area contains icons through which you can access additional information.

   Get Started
   Select to open the **Getting Started with Dynamic Partition Manager** task. The **Get Started** icon is displayed only if you are managing one or more systems that have DPM enabled.

   Guides
   Select or hover over the **Guides** icon to display a list of links to additional information.

   Note: Tutorials and videos are available only when you are accessing the HMC remotely.

   Tutorials
   Opens a new browser window to Resource Link (http://www.ibm.com/servers/resourcelink) to access the HMC tutorials.

   Videos
   Opens a new browser window to a website for videos.

   What's New?
   Starts the **What's New** information that provides a brief summary of the new functions of the Hardware Management Console.

Workspace Tour
Highlights improvements to the tree style user interface for this HMC version, such as search and favorites controls, task tabs, the resource status display, and more.

Learn More
Select or hover over the **Learn More** icon to display a list of links to additional information.

Note: The API and support links are available only when you are accessing the HMC remotely.

APIs
Opens a new browser window to Resource Link (http://www.ibm.com/servers/resourcelink) to access the API publications.

- *SNMP Application Programming Interfaces* - provides information for developing system management applications that will provide integrated hardware and software system management solutions using the application programming interfaces.
- *Hardware Management Console Web Services API* - defines, for reference purposes, the external interface of the Hardware Management Console (HMC) Web Services Application Programming Interface (Web Services API). This publication specifies the capabilities, input and output formats, and behaviors of the Web Services API as viewed by an application external to the HMC that is leveraging that interface.
- *Application Programming Interfaces for Java* publication is no longer available. You can access the javaapis.zip file from Resource Link. That file contains all of the Java documentation for the classes contained in the hwmcaapi.jar file. Go to Resource Link at http://www.ibm.com/servers/resourcelink, select **Services** from the left navigation pane, under **System management application development** select **IBM Z Application Programming Interfaces (API)**, then select **Java Files**. The Java Files window is displayed where you can access the javaapis.zip from the Download area.

Support
Opens a new browser window to Resource Link (http://www.ibm.com/servers/resourcelink) to access more support.

Pie charts and status legend

The *pie charts* display the total number of objects that you have permission to manage on this HMC. A list of the current status values and associated colors are listed next to the pie charts, as shown in Figure 22 on page 334.

Figure 22. Sample Welcome window pie charts

Systems
Displays the total number of managed systems that you have permission to manage, which can include systems that are running in standard mode (that is, with Processor Resource/System Manager or PR/SM) as well as systems that have DPM enabled. To manage those systems, click the **Systems** label, or click inside the **Systems** pie chart. Either action is equivalent to selecting the Systems Management node in the navigation pane: the **Systems** tab is displayed in the work pane.

Partitions
Displays the total number of DPM partitions and PR/SM logical partitions/images across all managed systems that you have permission to manage. To manage those partitions, click the **Partitions** label, or click inside the **Partitions** pie chart. The Systems Management **Partitions** tab is displayed in the work pane.

Adapters
Displays the total number of adapters across all DPM managed systems that you have permission to manage. The **Adapters** pie chart is displayed on the Welcome window only if you are managing one or more systems that have DPM enabled. To manage adapters, click the **Adapters** label, or click inside the **Adapters** pie chart. Either action opens the **Manage Adapters** task, displaying the **Adapters** tab.

The pie charts also identify the status of the respective objects as pie chart slices. The status pie charts are updated dynamically. In some cases, multiple status values map to the same color; for example, the Active and Operating status values apply when you are managing both standard-mode (PR/SM) and DPM systems. Transitional status values do not affect the status ring colors. Status ring colors do not change until a new state is achieved as a result of a transitional state. You can hover over the pie chart slices. The pie chart slices represent the status, the number of objects with each status, and relative percentage of the pie as shown in Figure 22 on page 334.

The following list describes status values that can be displayed in the pie charts and legend.

Active
Indicates that all systems and partitions are operating.

Communications not active
Indicates that the HMC is not communicating with the Support Element (SE).

Degraded
Indicates that the partition is up and running but one or more of its virtual resources are not in a good state. The actual physical adapter that is backing such a virtual resource does not have a good status. One or more of the channels that are used by this partition is not in a good state.

Note: Reservation error applies to a stopped partition.

Exceptions
Indicates that multiple system statuses and at least one system is operating. At least one partition is running and at least one partition is not running.

No power
Indicates that the system power is off.

Not activated
Indicates that the PR/SM partition is not known on the PR/SM level. It exists only as an image on the SE or HMC.

Not active
Indicates that the DPM adapters are not operating.

Not operating
Indicates that all systems are not operating or the LPAR image is known to PR/SM but no processors are running.

Operating
Indicates that all systems and processors are running.

Paused

Indicates the all the processors of the partition are stopped by the user.

Service

Indicates that an operator enabled service status for the system.

Service required

Indicates that the system is still operating but is using the last redundant part of a particular type.

Status check

Indicates that the SE cannot communicate to the system.

Stopped

Indicates that the partition exists only as "definition" within the object model on the SE.

Terminated

Indicates that all processors are in disabled wait.

The *status legend*, which is shown in Figure 23 on page 336, displays only the status values that correspond to those status values currently shown in the pie charts. A status color is displayed once in the legend. The order of the status values in the legend is the same as the chart color ordering.

When multiple status values exist for the same color, the following conditions apply.

- One of the status values, first in alphabetical order, is displayed with an ellipsis appended. The ellipsis (for example, Not activated...) indicates that more status values exist.
- Hover text for the status label displays the complete list of status values represented by the color, in alphabetical order as shown in Figure 23 on page 336.

Figure 23. Status legend

Systems Management

Systems Management is used to manage and view system resources. Selecting the expand icon from the navigation pane displays a tree view of managed systems and unmanaged systems, as highlighted in Figure 24 on page 337.

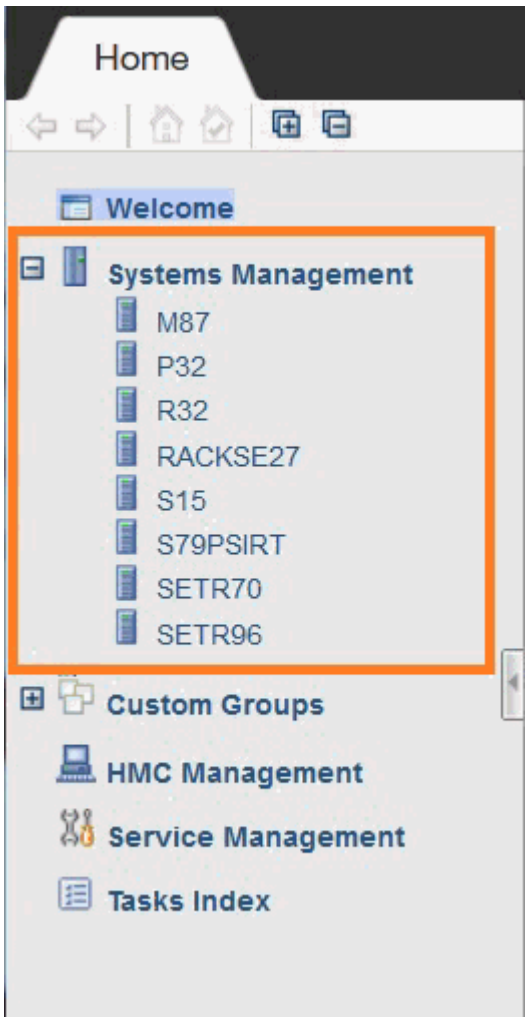


Figure 24. Sample view of the expanded Systems Management node

Note: The **Unmanaged Systems** node is available only if your user ID is based on the access administrator or service representative task roles.

The **Systems Management** node represents all the resources that are managed by this Hardware Management Console. When you select the **Systems Management** node from the navigation pane, all managed and unmanaged objects are displayed in the work pane, as shown in Figure 25 on page 337.

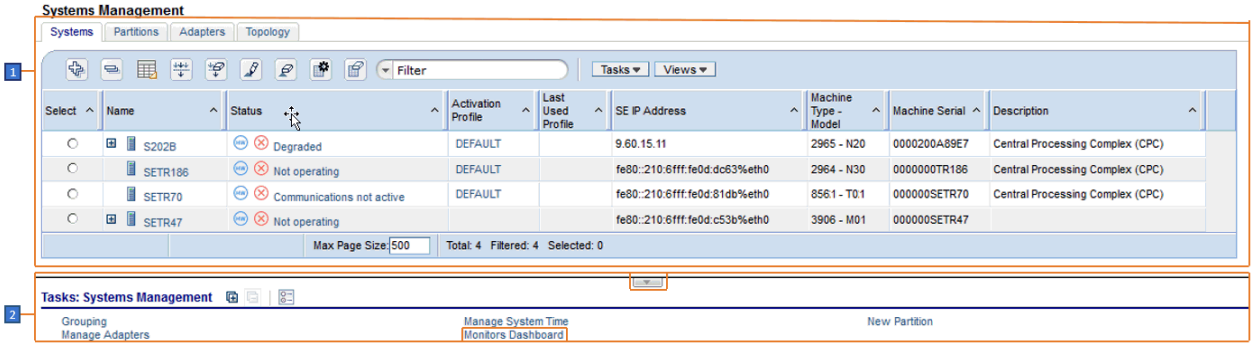


Figure 25. Sample Systems Management view in the work pane

1. **System Management** tabs. Figure 25 on page 337 shows one possible combination of tabs. The following list briefly describes the tabs that can be displayed in this view.

Systems
Displays, in a table format, all managed systems, which can include systems that are running in standard mode (that is, with Processor Resource/System Manager or PR/SM) and systems that have DPM enabled. For more information on systems, see Systems

Partitions
Displays, in a table format, a list of all DPM partitions and PR/SM logical partitions/images that are defined across all systems. An extra **System** column in the table identifies the system to which each partition is defined.

Note: The partitions are available from the **Systems** tab in a hierarchical format where you can sort or filter to get a similar view as from the **Partitions** tab.

For more information on partitions, see Partitions.

Topology
Displays the objects by using a graphical relationship-based model instead of the default table format. For more information, see Topology.

Monitor
Displays details about a system that has DPM enabled. The **Monitor** tab is displayed only if you are managing one or more systems that have DPM enabled, and have selected one of those systems on the **Systems** tab. For more information, see "DPM System Monitoring" on page 343.

2. Task pad. This area of the work pane lists the tasks that you can select and open, based on the content of the selected **System Management** tab. The listed tasks can change when you make a selection in the tab display.

Note:

- You can use the collapse control, which is highlighted in Figure 25 on page 337, to hide the task pad.
- You can resize the areas within the Systems Management work pane by moving the mouse pointer over the border that separates the tab displays from the tasks pad. When the pointer changes shape, press and hold the left mouse button and drag the mouse pointer up or down. Release the button and the tab display or task pad is now larger or smaller in size.
- You can select the Monitors Dashboard task, which is highlighted in Figure 25 on page 337, to access more information about standard-mode (PR/SM) systems; the information is equivalent to the **Monitor** tab content for systems that have DPM enabled.

Systems

Note: The terms *system*, *server*, *object*, and *CPC* are used interchangeably.

To work with a system, you can perform one of the following actions:

- Select a system under the **Systems Management** node from the navigation pane
- Select a system name from the work pane table
- Click in the **Select** column next to the system name in the work pane table.

Note: Working with one system at a time is the default, and is used in the examples throughout this Help information. However, if you want to work with more than one system you can go to the **User Settings** task, select the **Controls** tab, deselect the **Single object selection** option, and click **Apply**. Now you can choose multiple systems to manage.

Tasks cannot be performed on a system until it is defined. The undefined servers are listed under the **Unmanaged Systems** node (see Unmanaged Systems). To define a server, see the **Add Object Definition** task.

You can find more detailed help on the following:

Opening Tasks for the System

After you have chosen the systems to work with you are ready to perform tasks on them. The following task categories (groups) that are applicable to the systems you have chosen are displayed in the tasks pad. Task categories (groups) represent categories of tasks and are not tasks themselves.

- Daily
- Recovery
- Service
- Change Management
- Remote Customization
- Operational Customization
- Object Definition
- Configuration
- Energy Management
- Monitor

You can select a task from these task groups in a variety of ways:

- Use the tasks pad below the systems work pane, see Tasks Pad.
- Click the context menu icon that is displayed next to the server name, see Context Menu.
- Click the **Tasks** menu from the work pane table toolbar, see Tasks Menu.
- Right-click in the cell containing the name of the object to display the context menu.

Note: If a particular task cannot be performed on an object the task is not displayed.

You can find more detailed help on the following:

Tasks Pad

The Hardware Management Console displays the tasks pad below the work pane table after you have selected the managed objects with which you want to work.

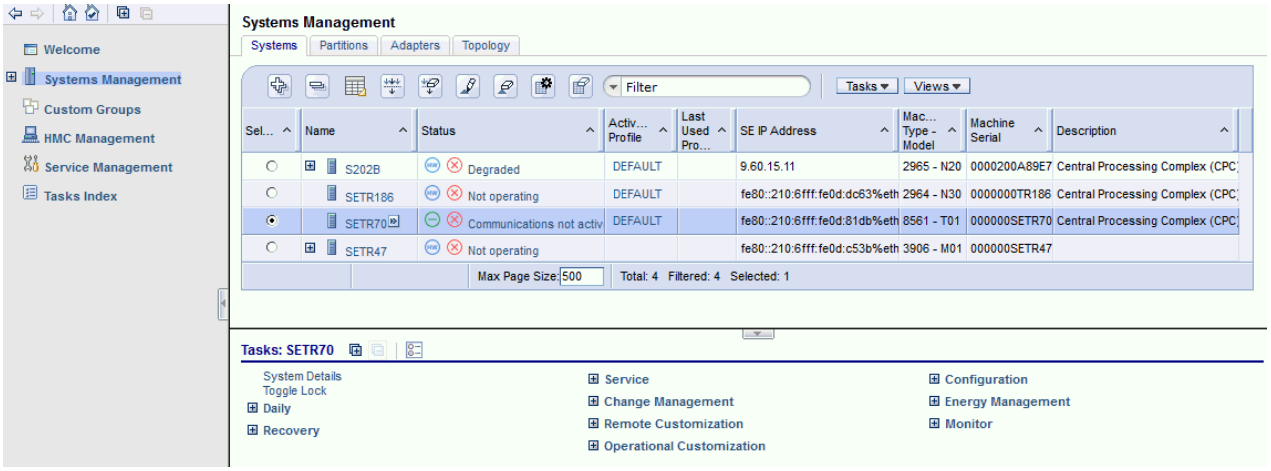
The following figure shows an example of tasks in the tasks pad that are available for the selected managed objects and applicable for the current user.

By default, the tasks pad is displayed. You can choose to hide the tasks pad by using the **User Settings** task.

To change the display of the tasks pad setting you can go to the **User Settings** task by selecting:

- **Task Index** or **HMC Management** on the navigation pane, then open the **User Settings** task, or
- The user ID from the task bar to access the **User Settings** task to change the setting, or
- The **Close Tasks Pad** icon from the right side of the tasks pad title bar.

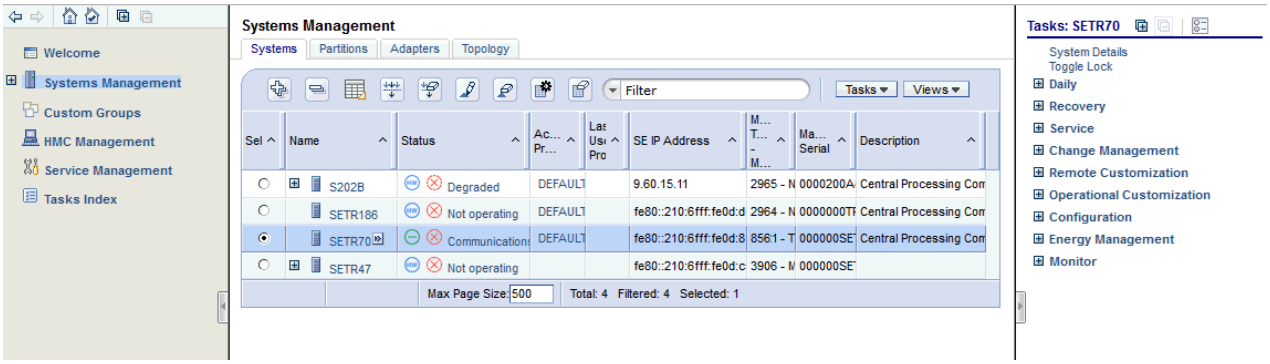
Note: To reset a closed tasks pad you must use the **User Settings** task.



Additional characteristics of using the tasks pad include:

- Resize the tasks pad by moving the mouse pointer over the border that separates the work pane table from the tasks pad.
- Use the collapse and expand controls icon that is provided on the border between the tasks pad and the work pane. You can click on these controls to collapse or expand the tasks pad allowing you more work area in the work pane, if required. Hovering over these controls indicates whether you will be hiding or displaying the tasks pad.
- Expand or collapse all the task groups in the tasks pad by selecting the **Expand All** icon or the **Collapse All** icon from the tasks pad title bar.
- Organize the tasks pad display by using the **Settings** icon from the tasks pad title bar. This option allows you to arrange the displayed tasks in a viewing format you prefer and in addition:
  - **Number of task columns** - Using the up and down arrows, select the number of columns you want displayed for the list of tasks.
  - **Expand task groups by default** - The task groups are expanded to display applicable tasks.
  - **Sort tasks alphabetically** - The tasks from all the task groups are sorted alphabetically.
  - **Position tasks pad vertically** - The tasks pad is rendered to the right of the work pane's table frame (see the following figure for an example).

    Note: When the tasks pad displays vertically the column count is not available.



This view displays the objects you selected from either the navigation pane tree or the work pane table view. Multiple objects are selected in the work pane table, therefore, the intersection of the selected objects' tasks are displayed.

If there are no objects selected in the work pane table, tasks are displayed in the tasks pad for the object selected in the navigation pane. Additionally, the tasks that displayed in the tasks pad are those available to the user currently logged in.

An example of using the tasks pad method:

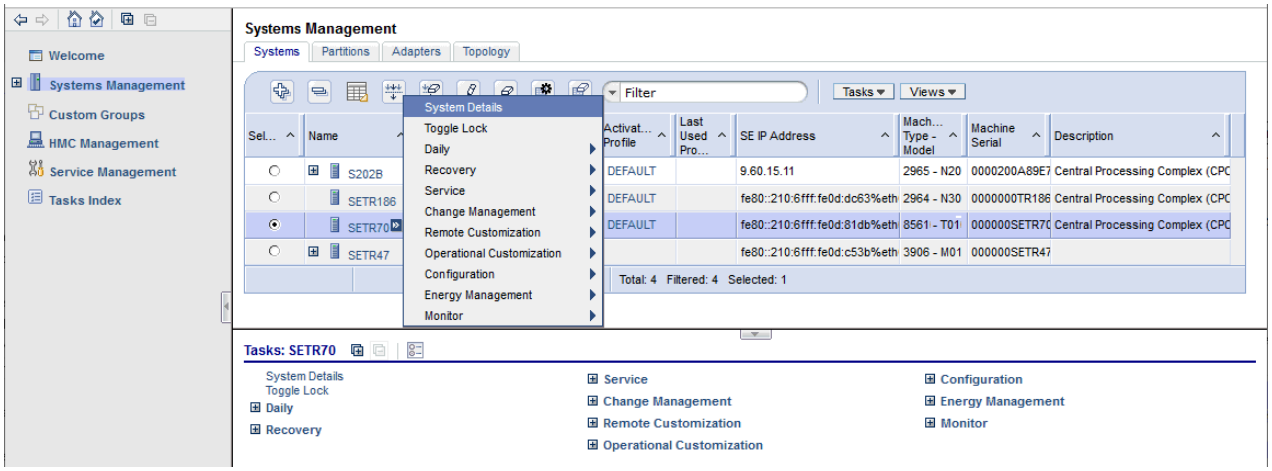
1. Select a server in the work pane table (click the **Select** column).
2. Select a task group from the tasks pad (click the expand button or click the group name).

   Note: After you have expanded the task groups, those groups remain open so that you can repeatedly open other tasks without having to reopen the task groups.
3. From the task group, select the task that you want to perform.
4. The task window is displayed.

Context Menu

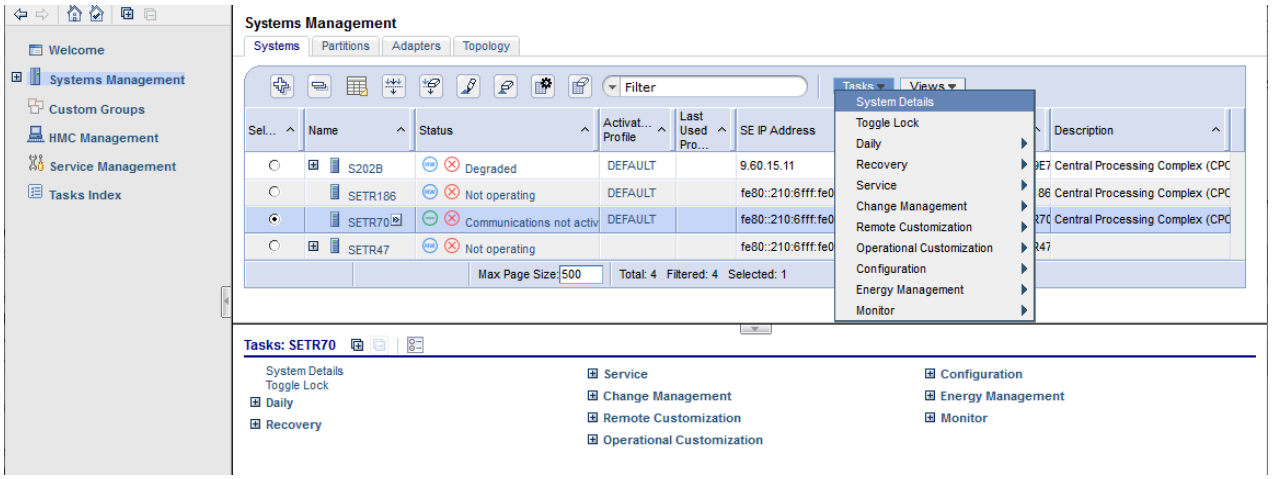
The context menu is a pop-up menu that lists the task groups associated with the selected object or objects. Context menus are available only for table selections. For example, in the **Select** column of the Systems work pane table, select the object or objects you want to work with. The context menu button (double right arrows) is displayed next to the object name you have selected. Click the button and the task groups menu is displayed for that particular object, as shown in the following figure. You can also right click within the table cell of the object name to display the context menu. Then select a task to open for

the object. If more than one object is selected, the tasks that are displayed in the context menu apply to all selections.



Tasks Menu

The **Tasks** menu is displayed on the work pane table toolbar, as shown in the following figure. The tasks menu is available only for table selections. For example, in the **Select** column of the Systems work pane table, select the object you want to work with. Click **Tasks** for the list of the applicable task groups for the selected objects in the table. Select a task group, then select a task to open for the object. If more than one object is selected, the tasks that are displayed in the tasks menu apply to all selections.



Status

The **Status** column of the Systems work pane table displays the current status of the server. If you select the status text, the help information for that status is displayed. Status icons can also be displayed in the status column next to the status text. Depending on the icon that is displayed, you can get the Hardware Messages task window or the Operating Systems Messages task window.

Displaying System Details

All system details can be displayed by using one of the following methods:

- Click the object name from the work pane table.
- Select the object name from the work pane table then:
  - Click **Details** from the tasks pad, or
  - Click the arrow icon next to the object name, then click **Details** from the context menu, or
  - Right-click in the object name table cell, then click **Details** from the context menu.

While you are in the **Details** window, you can also lock out disruptive tasks, or by clicking **Toggle Lock** in the tasks pad or from the context menu.

Note: Object locking cannot be applied to IBM Dynamic Partition Manager (DPM) objects.

The Systems Management work pane table includes additional information about the systems such as the activation profile name, last profile the server used, the machine type, and serial number of the server.

You can use the "Views Menu" on page 364 to customize the information that is displayed in the work pane table or the **Configure Columns** icon on the work pane table toolbar.

Partitions

If partitions are defined for a particular system, then they are displayed in the Systems Management work pane under the **Partitions** tab. The contextual tasks that are associated with a particular partition are displayed in the tasks pad. You can also view the partitions that are associated with a system by selecting a system in the navigation pane so that the partitions are displayed in the work pane table under the **Partitions** tab (see the following figure).

You can open tasks on the partitions the same way you open them on the systems. For more information, see Opening Tasks for the System.

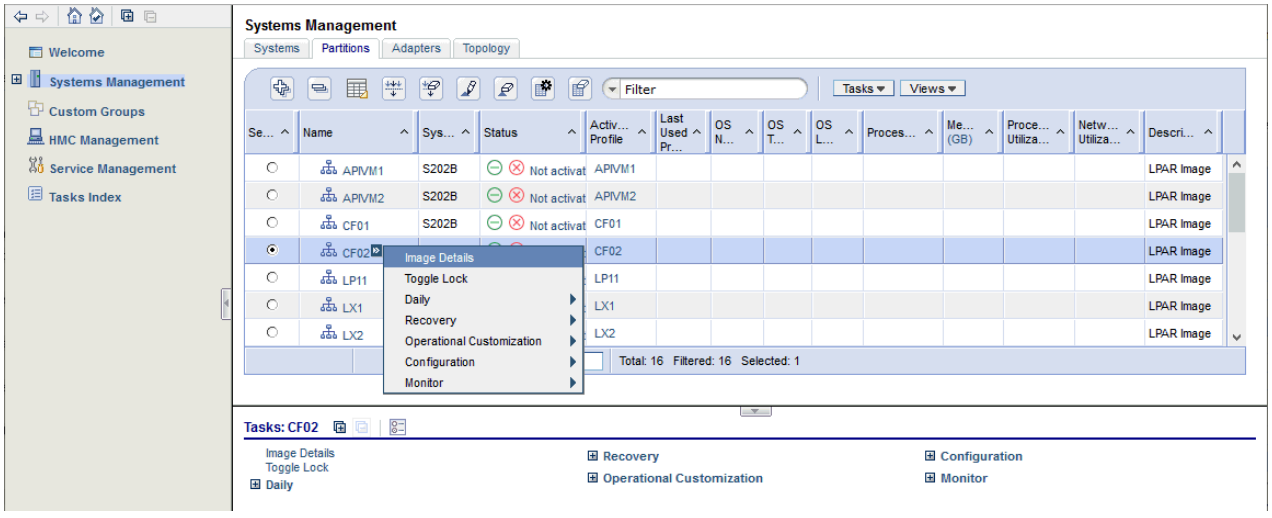
To display details about a partition from the Systems Management work pane table:

- Click the partition name from the **Name** column, or
- Click in the **Select** column next to the partition name to either:
  - Click **Image Details** in the tasks pad, or
  - Click the arrow icon next to the partition name and select **Image Details** from the context menu (see the following figure), or
  - Right-click the table cell of the partition name and select **Image Details** from the context menu.

In all cases, the **Details** window is displayed.

The Partitions work pane table includes additional information about the partitions such as the activation profile name, last profile the image used, the operating system name, type, and level for the partition.

You can use the **Views** menu to customize the information that is displayed in the work pane table or the **Configure Columns** icon on the work pane table toolbar.



You can find more detailed help on the following:

Unmanaged Systems

The **Unmanaged Systems** node represents the Systems that are not defined to the Hardware Management Console.

Note: The **Unmanaged Systems** node is available only if your user ID is based on the access administrator or service representative task roles.

Systems

The systems associated with **Unmanaged Systems**:

- Are physically installed
- Have their Support Element powered on
- Have the same domain name and domain security as the Hardware Management Console
- Are not managed by your Hardware Management Console.

A system in this group must be defined before tasks can be performed on it. Status is not reported for systems in the **Unmanaged Systems** group. To define systems, use the **Add Object Definition** task:

1. Select a system by clicking in the **Select** column of the Unmanaged Systems work pane table.
2. Open the **Add Object Definition** task from the tasks pad. The **Add or Change Object** window is displayed.
3. Click **Save** to add the system to the group of managed systems.

In addition, this group also contains **System Manual Definition**. Local Hardware Management Consoles can automatically detect the presence of Support Elements and automatically set up all the necessary internal configuration information for communication without additional information from the users. For remote Hardware Management Consoles, users must provide additional addressing information to perform this configuration.

Use **System Manual Definition** to define a system when TCP/IP connectivity exists between the Hardware Management Console and the system:

1. Select **Unmanaged Systems** from the navigation pane.
2. Open the **Manual Add Object Definition** task from the Unmanaged Systems task pad. The **Manual Add Object Definition** window is displayed.
3. Specify the TCP/IP address in the **TCP/IP address** field and click **OK**. The Hardware Management Console tries to contact the Support Element and exchange the remaining information necessary to complete the configuration process.

   Note: The **Manual Add Object Definition** window remains displayed with the last entered TCP/IP address until you have added the appropriate systems. When you have completed this task, click **Cancel**.

After a system is defined, it is removed from the **Unmanaged Systems** node and added to the **Systems Management** node on the navigation pane. From the **Systems** tab, the system can be grouped into one or more user-defined groups. A defined system will remain as part of **Systems** until its definition is removed, regardless of its power state.

DPM System Monitoring

To enable system monitoring for a Dynamic Partition Manager (DPM) system, you can select the system from the navigation pane, then select the Monitor tab from the work pane area. Your selections and settings within the elements of the Monitor tab are saved for the duration of the session, per system. If there are multiple DPM systems, their selections and settings within their Monitor tabs are independent of one another, but are saved in such a way that if you switch navigation node or tab selection or if you disconnect and reconnect, then each system's settings pick up where they left off.

The **Monitor** tab work area contains:

“Overview Row” on page 344

Displays overall system monitoring data for the various components that make up the system. By default, the overview row is in the expanded state. In this state, charts and additional wording is shown in each button. Use the expand and collapse buttons depending on what view you want.

“Details Area” on page 346
Displays specific information from your selection on the Overview row.

You can click on each area for more information that is displayed in the **Details** area. You can also hover over each of the components for summarized information. The following figure is an example of the Monitor tab work area and identifies the Overview Row and Details Area.

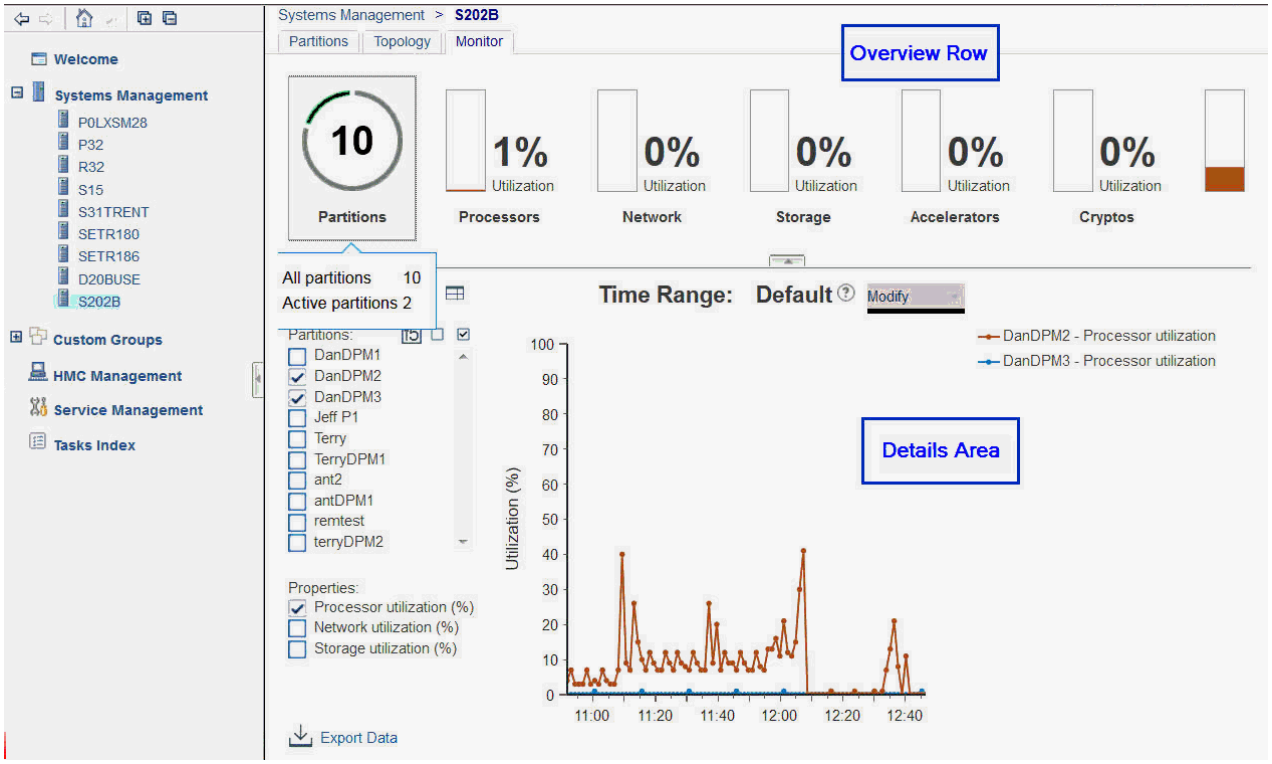


Figure 26. DPM System Monitoring

Overview Row

The *overview row* consists of the following charts.

Partitions pie chart
Displays active (any Active status color) and not active status (gray color) of the partitions defined to the system. The number displayed is the total number of partitions defined to the system. You can mouse over the chart icon to display the following chart values:

All partitions
Displays the number of all the defined partitions to the system.

Active partitions
Displays the number of partitions which have Active status.

Processors chart
Displays the maximum active configured utilization which is a percentage of the maximum system entitled utilization (represented by the full chart height) and the current utilization as a percentage of the active configured. Note that the current utilization value is therefore not a percentage of the full chart height, but rather of the configured max line. For processors, because allocating any shared processors can use any and all processors in the shared pool, which is all non-dedicated entitled processors, the configured maximum is usually 100%. The exception cases are if there are no active partitions, in which case both values are 0%, or there are only dedicated partitions active. Both chart values should be updated every minute with new data. The text value of current utilization is rounded to the nearest percent.

You can hover over the chart icon to display the following chart values, use the ? icon to display a more detailed explanation:

Configure maximum utilization
Displays the percentage of the maximum utilization of the system that can be reached based on active partitions.

Current utilization
Displays the percentage of the utilization of the resources by active partitions over the last minute.

Network chart
Represents OSD, RoCE, and HiperSockets adapters. This chart displays the maximum active configured utilization which is a percentage of the maximum system entitled utilization (represented by the full chart height), and the current utilization as a percentage of the active configured. Note that the current utilization value is therefore not a percentage of the full chart height, but rather of the configured maximum line. For Network adapters, an adapter's bandwidth is considered part of the configured maximum if it has at least one NIC allocated to it from an active partition. Both chart values should be updated every minute with new data. The text value of current utilization is rounded to the nearest percent.

You can hover over the chart icon to display the following chart values, use the ? icon to display a more detailed explanation:

Configure maximum utilization
Displays the percentage of the maximum utilization of the system that can be reached based on active partitions.

Current utilization
Displays the percentage of the utilization of the resources by active partitions over the last minute.

Storage chart
Represents FCP adapters. This chart displays the maximum active configured utilization which is a percentage of the maximum system entitled utilization (represented by the full chart height), and the current utilization as a percentage of the active configured. Note that the current utilization value is therefore not a percentage of the full chart height, but rather of the configured maximum line. For Storage adapters, an adapter's bandwidth is considered part of the configured maximum if it has at least one HBA allocated to it from an active partition. Both chart values should be updated every minute with new data. The text value of current utilization is rounded to the nearest percent.

You can hover over the chart icon to display the following chart values, use the ? icon to display a more detailed explanation:

Configure maximum utilization
Displays the percentage of the maximum utilization of the system that can be reached based on active partitions.

Current utilization
Displays the percentage of the utilization of the resources by active partitions over the last minute.

Accelerators chart
Represents zEDC adapters. This chart displays the maximum active configured utilization which is a percentage of the maximum system entitled utilization (represented by the full chart height), and the current utilization as a percentage of the active configured. Note that the current utilization value is therefore not a percentage of the full chart height, but rather of the configured maximum line. For Accelerator adapters, an adapter's bandwidth is considered part of the configured maximum if it has at least one virtual function allocated to it from an active partition. Both chart values should be updated every minute with new data. The text value of current utilization is rounded to the nearest percent. This chart icon appears only when accelerator data is in the monitoring database.

You can hover over the chart icon to display the following chart values, use the ? icon to display a more detailed explanation:

Configure maximum utilization
Displays the percentage of the maximum utilization of the system that can be reached based on active partitions.

Current utilization
Displays the percentage of the utilization of the resources by active partitions over the last minute.

Cryptos chart
Represents Crypto adapters. This chart displays the maximum active configured utilization which is a percentage of the maximum system entitled utilization (represented by the full chart height), and the current utilization as a percentage of the active configured. Note that the current utilization value is therefore not a percentage of the full chart height, but rather of the configured maximum line. For Crypto adapters, an adapter's bandwidth is considered part of the configured maximum if it has at least one active partition. Both chart values should be updated every minute with new data. The text value of current utilization is rounded to the nearest percent. This chart icon appears only when crypto data is in the monitoring database.

You can hover over the chart icon to display the following chart values, use the ? icon to display a more detailed explanation:

Configure maximum utilization
Displays the percentage of the maximum utilization of the system that can be reached based on active partitions.

Current utilization
Displays the percentage of the utilization of the resources by active partitions over the last minute.

Power chart
Displays the power rating of the system. The bar value represents the current power consumption. This chart also displays the power capping value if it is entitled and enabled. The chart values are updated every minute with new data. The text value of power consumption is rounded to the nearest hundredth in kW.

You can hover over the chart icon to display the following chart values:

- Power rating
- Maximum potential power (kW)
- Power capping (kW) - only displays if entitled or enabled
- Power consumption (kW)

Environmentals chart
Displays the ambient temperature of the system. The full chart height represents the range from 0 to 50 degrees Celsius (32 to 122 degrees Fahrenheit). The current ambient temperature is therefore represented as a bar which is a percentage of that temperature. The text value of the current ambient temperature is rounded to the nearest degree.

You can hover over the chart icon to display the ambient temperature. The default temperature that is displayed is based on the country of your locale. You can change the unit value by selecting **ºF** or **ºC**.

Note: Fahrenheit remains the official scale and therefore is the default for the following countries:

- Bahamas
- Belize
- Cayman Islands
- Palau
- United States
- Associated territories: Puerto Rico, Guam, and the U.S. Virgin Islands

All other countries default to Celsius. Changing the unit changes the display in all places it is shown.

Details Area

As you make a selection in the overview row a *details area* is displayed. Generally, this includes the following information:

Title area
Displayed at the top of the details area. The title is based on the chart icon you selected from the overview area. If the selection supports more than one view (for example, chart and table views), then

toggle buttons are provided for the different views. The default selection for all areas is the chart view. The views are:

Chart view

 Contains a list of options to include in the chart. This will change depending on the selection in the overview row. All areas support the chart view. The chart view displays the following:

Export Data

 Allows you to export the data to a device. The Export Data window is displayed, click **OK** to continue with the task.

Center of the chart area
Displays the actual chart itself. All charts have a granularity of one minute data points when showing two hours or less of data. When you are showing more than two hours of data, each data point is 15 minutes.

Chart legend
Identifies the chart colors that are used in the chart.

Table view

 This view is supported by Partitions, Processors, Network, Storage, Accelerators, and Cryptos.

Export icon drop-down
Select this icon to export the data of this table to a .csv file type or .html file type.

Print icon

 Select this icon to print the content of the table.

Actions drop-down
Select the drop-down to Print or Export the contents of the table.

Search

 Select this icon after you have provided a filter string in the input area.

Properties view

 This view is supported by Systems Overview (default), Power, and Environmentals. The half-moon gauges are used to display this information.

Time range
Identifies the current time range selection for all details areas. The values could be:

- **Default** - the default selection for all areas and views, which, for all chart views is defined as the last two hours and for all table and property views is defined as the last known (current) value.
- **Last *x* minutes**
- **Last *x* hours**
- ***x* to *y***

where *x* and *y* are the selected date/time strings of the custom range, as they are set from the **Modify** drop down. You can select the **Custom...** time range option, the Select Time Range window is displayed. You can choose the following options from this window:

Default
Data is updated every minute. Chart views display data for the last two hours. Table and property views display the last known values.

Now - Last
Data is updated every minute if the time range is two hours or less. Otherwise, data is updated every 15 minutes. Charts display all data over the time range. Table and property views display the average data over the time range.

Set Time Range
Data is not updated. Charts display all data over the time range. Table and property views display the average data over the table range.

Note: The time range must be set between 1 minute and 36 hours.

To save your changes, click **OK**. Otherwise, click **Cancel** to keep the original settings.

System Views

The overall System details area contains the following views.

Chart View

The System chart view displays the available system properties that can be included or omitted from the line chart and chart legend by selecting or deselecting the options. By default, all utilizations are selected. You can only select two of the three unit types simultaneously. Additionally, Accelerator utilization (%) and Crypto utilization (%) are unavailable if there is no data for them.

Property View

The System statistics are rendered as half-moon gauges in the property view.

Power Utilization, Network Utilization, and Storage Utilization
Gauge extents are 0-100%. These are status-less, value only gauges.

Accelerator Utilization and Crypto Utilization
Gauge extents are unavailable if there is no data for them.

Power Consumption
Gauge extents are 0 kW to the lesser of the maximum power and power cap, if available. This is a status-less, value only gauge.

Ambient Temperature
Gauge extents are 32ºF/0ºC to 122ºF/50ºC. The red and green status areas are based on the ASHRAE class of the system. The ranges are as follows:

- Below allowable (red/critical)
- Lower allowable, upper allowable, or allowable, as applicable (green/normal)
- Recommended, if applicable (green/normal)
- Above allowable (red/critical)

Partitions Views

The Partitions details area displays a “Chart view” on page 348 and “Table view” on page 349.

Chart view

The Partitions chart view displays a list of partitions that you can select from in the monitoring database for the current time range. When you select a partition from the list that partition is added to the chart and the chart legend. If you deselect a partition, it is removed from the chart and the chart legend. By default, the five partitions with the highest current utilization are selected. The **Partitions** list contains the following icons:

Select Top 5

 Sets the list selection to be exactly five partitions with the highest current utilization at the time of the action, and sets only them in the chart and chart legend.

Deselect All

 Clears all selections and removes them from the chart and chart legend.

Select All

 Selects all processors and adds them to the chart and its legend.

The **Properties** list displays the available properties. The properties that are listed are also reflected in the chart and the chart legend when a property is selected. The properties might include:

Processor utilization (%)
This property is always available and selected by default.

Network utilization (%)
This property is available and can be selected if there is data. It is the average utilization of all the Network adapters the partition has access to.

Storage utilization (%)
This property is available and can be selected if there is data. It is the average utilization of all the Storage adapters the partition has access to.

Accelerator utilization (%)
This property is available and can be selected if there is data. It is the average utilization of all the Accelerator adapters the partition has access to.

Crypto utilization (%)
This property is available and can be selected if there is data. It is the average utilization of all the Crypto adapters the partition has access to.

Table view

The Partitions table view displays all the partitions that have an entry in the monitoring database for the current time range. The **Name** column displays the partition name and is a hyperlink that opens the **Partition Details** in a separate task window. The utilizations are rendered as a progress bar and is the average usage over the current time range, or the current value if **Default** is selected. Accelerator utilization (%) and Crypto utilization (%) columns are unavailable if they have no data. Network utilization (%), Storage utilization (%), Accelerator utilization (%), and Crypto utilization (%) columns are unavailable if they have no data.

Processors Views

The Processors details area contains a **View by** selection. The default is Processor.

Chart view

The Processors processor chart view contains a list of processors that you can select from in the monitoring database for the current time range. When you select a processor from the list that processor is added to the chart and the chart legend. If you deselect a processor it is removed from the chart and the chart legend. By default, the five processors with the highest current utilization are selected. The Processors list contains the following button icons:

Select Top 5

 Sets the list selection to be exactly five processors with the highest current utilization at the time of the action, and sets only them in the chart and chart legend.

Deselect All

 Clears all selections and removes them from the chart and chart legend.

Select All

 Selects all processors and adds them to the chart and its legend.

The **Properties** list contains a list of the properties and is reflected in chart and chart legend as a property has been selected or deselected. By default, only Processor utilization (%) is selected.

Type Chart view

The Processors type chart view provides the following:

Types list
Contains a list of every processor type, in addition to, an **All types** selection you can select from in the monitoring database for the current time range. When you make a selection from this list those types are added to the chart and the chart legend. If you deselect a type they are removed from the chart and the chart legend. By default **All types** is selected.

Properties list
Contains a list of the properties and is reflected in chart and chart legend as a property has been selected or deselected. By default, **All processor utilization** is selected.

Table view

The Processors table view contains all the processors which have an entry in the monitoring database for the current time range. The **Name** column displays the processor name. The utilizations are rendered as a progress bar and is the average utilization over the current time range, or the current value if **Default** is selected.

Type Table view

The Processors type table view contains all the processor types which have an entry in the monitoring database for the current time range. If there is only one type, then just the type is shown. The utilizations are rendered as a progress bar and is the average utilization over the current time range, or the current value if **Default** is selected.

Network Views

The Network details area contains a **View by** selection for “Adapters” on page 350, “Ports and Switches” on page 351, and “NICs” on page 351.

Adapters

Chart view
The Network Adapters chart view contains a list of adapters which includes all OSD and RoCE type adapters that you can select from in the monitoring database for the current time range. OSM adapters are included if you are logged in with the SERVICE default user ID or a user ID with service roles. When you select an adapter from the list that adapter is added to the chart and the chart legend. If you deselect an adapter it is removed from the chart and the chart legend. By default, the five adapters with the highest current utilization are selected. The Adapters list contains the following button icons:

Select Top 5

 Sets the list selection to be exactly five adapters with the highest current utilization at the time of the action, and sets only them in the chart and chart legend.

Deselect All

 Clears all selections and removes them from the chart and chart legend.

Select All

 Selects all processors and adds them to the chart and its legend.

Table view

The Network Adapters table view contains a list of adapters which includes all OSD and RoCE type adapters that you can select from in the monitoring database for the current time range. OSM adapters are included if you are logged in with the SERVICE default user ID or a user ID with service roles. The **Adapter** column displays the adapter name and is a hyperlink which opens the **Adapter Details** in a separate task window. The **Type** column is the configured adapter type. The utilization is

displayed as a progress bar and is the average utilization over the current time range, or the current value if **Default** is selected.

Ports and Switches

Chart view

The Network Ports and Switches chart view contains a list of ports and switches which includes all OSD and RoCE type adapter ports/switches that you can select from in the monitoring database for the current time range. When you select a port or switch from the list that port or switch is added to the chart and the chart legend. If you deselect a port or switch it is removed from the chart and the chart legend. By default, the five ports or switches with the highest current utilization are selected. The Ports and Switches list contains the following button icons:

Select Top 5


Sets the list selection to be exactly five ports and switches with the highest current utilization at the time of the action, and sets only them in the chart and chart legend.

Deselect All


Clears all selections and removes them from the chart and chart legend.

Select All


Selects all processors and adds them to the chart and its legend.

The **Properties** list contains a list of the properties and is reflected in chart and chart legend as a property has been selected or deselected. By default, only Utilization (%) is selected. Utilization is calculated as the percentage usage of the port's bandwidth. You can choose two of the unit types simultaneously.

Note: A Utilization entry in the chart legend is a hyperlink and opens the Utilization Details window for the port or switch. On this window, a chart displays an entry for every NIC that is defined to the target port or switch. A **Manage Adapters** hyperlink opens the Manage Adapters task in a new task window. To close the Utilization Details window and return to the main **Monitor** tab window, click **Close**.

Table view

The Network Ports and Switches table view contains a list of ports and switches which includes all OSD and RoCE type adapter ports/switches that you can select from in the monitoring database for the current time range. From the Actions drop-down you can choose the following:

Utilization Details
Opens the Utilization Details window for the target.

Adapter Details
Opens the Adapter Details window.

The **Adapter Name** column displays the adapter name and is a hyperlink which opens the **Adapter Details** in a separate task window. The **Type** column is the adapter port/switch type. The utilization is displayed as a progress bar and is the average utilization over the current time range, or the current value if **Default** is selected. For OSD and RoCE this is the physical port utilization.

NICs

Chart view

The Network NICs chart view contains a list of NICs that you can select from in the monitoring database for the current time range. When you select a NIC from the list that NIC is added to the chart and the chart legend. If you deselect a NIC it is removed from the chart and the chart legend. By default, the five NICs with the highest current utilization are selected. The NICs list contains the following button icons:

Select Top 5


Sets the list selection to be exactly five NICs with the highest current utilization at the time of the action, and sets only them in the chart and chart legend.

Deselect All

Clears all selections and removes them from the chart and chart legend.

Select All

Selects all processors and adds them to the chart and its legend.

The **Properties** list contains a list of the properties and is reflected in chart and chart legend as a property has been selected or deselected. By default, only Utilization (%) is selected. You can choose two of the unit types simultaneously.

Note: Utilization is only available if a non-HiperSockets NIC is selected.

Table view

The Network NICs table view contains all the NICs which have an entry in the monitoring database for the current time range. The **Partition** column displays the partition's name and is a hyperlink which opens the **Partitions Details** window. The **Type** column is the NIC type. The utilizations are displayed as a progress bar and is the average utilization over the current time range, or the current value if **Default** is selected.

Note: HiperSockets do not have utilization values.

Storage Views

The Storage details area contains the following views.

Chart view

The Storage chart view contains a list of adapters which represents every FCP adapter that you can select from in the monitoring database for the current time range. When you select an adapter from the list that adapter is added to the chart and the chart legend. If you deselect an adapter it is removed from the chart and the chart legend. By default, the five adapters with the highest current utilization are selected. The **Adapters** list contains the following button icons:

Select Top 5


Sets the list selection to be exactly five adapters with the highest current utilization at the time of the action, and sets only them in the chart and chart legend.

Deselect All

Clears all selections and removes them from the chart and chart legend.

Select All

Selects all processors and adds them to the chart and its legend.

Table view

The Storage table view contains all the adapters which represents every FCP adapter that has an entry in the monitoring database for the current time range. The **Adapter** column displays the adapter name and is a hyperlink which opens the **Adapter Details** in a separate task window. The utilization is displayed as a progress bar and is the average utilization over the current time range, or the current value if **Default** is selected.

Accelerators Views

The Accelerators details area contains the following views.

Chart view

The Accelerators chart view contains a list of adapters which represents every zEDC adapter that you can select from in the monitoring database for the current time range. When you select an adapter from the list that adapter is added to the chart and the chart legend. If you deselect an adapter it is removed from

the chart and the chart legend. By default, the five adapters with the highest current utilization are selected. The **Adapters** list contains the following button icons:

Select Top 5

 Sets the list selection to be exactly five adapters with the highest current utilization at the time of the action, and sets only them in the chart and chart legend.

Deselect All

 Clears all selections and removes them from the chart and chart legend.

Select All

 Selects all processors and adds them to the chart and its legend.

Table view

The Accelerators table view contains all the adapters which represents every zEDC adapter that has an entry in the monitoring database for the current time range. The **Adapter** column displays the adapter name and is a hyperlink which opens the **Adapter Details** in a separate task window. The utilization is rendered as a progress bar and is the average utilization over the current time range, or the current value if **Default** is selected.

Cryptos Views

The Cryptos details area contains the following views.

Chart view

The Cryptos chart view contains a list of adapters which represents crypto type adapters that you can select from in the monitoring database for the current time range. When you select an adapter from the list that adapter is added to the chart and the chart legend. If you deselect an adapter it is removed from the chart and the chart legend. By default, the five adapters with the highest current utilization are selected. The **Adapters** list contains the following button icons:

Select Top 5

 Sets the list selection to be exactly five adapters with the highest current utilization at the time of the action, and sets only them in the chart and chart legend.

Deselect All

 Clears all selections and removes them from the chart and chart legend.

Select All

 Selects all processors and adds them to the chart and its legend.

Table view

The Cryptos table view contains all the adapters which represent crypto type adapters that has an entry in the monitoring database for the current time range. The **Adapter** column displays the adapter name and is a hyperlink which opens the **Adapter Details** in a separate task window. The **Type** column refers to the crypto type. The utilization is displayed as a progress bar and is the average utilization over the current time range, or the current value if **Default** is selected.

Power Views

The Power details area contains the following views.

Chart View

The Power chart view displays the available system properties that can be included or omitted from the line chart and chart legend by selecting or deselecting the options. By default, Power® Consumption (kW) and Heat Loads are selected. The Heat load - water (BTU/hr) is not available if the system is not water cooled. The Average voltage (V) and the three Line currents are hidden unless you are logged in with the SERVICE default user ID or a user ID with service roles. If you have service access you can only choose two of the four unit types simultaneously.

Property View

The Power statistics are rendered as half-moon gauges in the property view.

Power Consumption
Gauge extents are 0 kW to the lesser of the maximum power and power cap, if available. This is a status-less, value only gauge.

Heat Load
All gauge extents are 0 kW to the lesser of the maximum power and power cap, if available, but in Btu/hr. This is a status-less, value only gauge. The Heat load - water (BTU/hr) is not available if the system is not water cooled.

Average Voltage
Gauge extents are 0 V to 100 V. This is a status-less, value only gauge.

Line Current
Gauge extents are 0 amps to 100 amps. This is a status-less, value only gauge.

Environmentals Views

The Environmentals details area contains the following views.

Chart View

The Environmentals chart view displays the available system properties that can be included or omitted from the line chart and chart legend by selecting or deselecting the options. By default, all temperature options and the Humidity are selected. The Air Pressure is hidden unless you are logged in with the SERVICE default user ID or a user ID with service roles. If you have service access you can only choose two of the three unit types simultaneously.

Property View

The Environmentals statistics are rendered as half-moon gauges in the property view.

Ambient Temperature
Gauge extents are 32ºF/0ºC to 122ºF/50ºC. The red and green status areas are based on the ASHRAE class of the system. The ranges are as follows:

- Below allowable (red/critical)
- Lower allowable, upper allowable, or allowable, as applicable (green/normal)
- Recommended, if applicable (green/normal)
- Above allowable (red/critical)

Exhaust Temperature
Gauge extents are 32ºF/0ºC to 122ºF/50ºC. There is no allowable or recommended ranges, this is a status-less, value only gauge.

Dew Point
Gauge extents are 32ºF/0ºC to 122ºF/50ºC. The red and green status areas are based on the ASHRAE class of the system, and each has its own hover text. The ranges are as follows:

- Allowable (green/normal)

- Above allowable (red/critical)

Humidity

Gauge extents are 0-100%. The red and green status areas are based on the ASHRAE class of the system and its allowable relative humidity range specification, and each has its own hover text. The ranges are as follows:

- Below allowable (red/critical)
- Allowable (green/normal)
- Above allowable (red/critical)

Air Pressure

Gauge extents are 500-1500 hPa. There is no allowable or recommended ranges, this is a status-less, value only gauge.

Note: This gauge is only available if you are logged in with the SERVICE default user ID or a user ID with service roles.

Custom Groups

The **Custom Groups** node provides a mechanism for you to group system resources together in a single view. In addition, groups may be nested to create custom "topologies" of system resources.

You perform tasks on objects in a group by selecting the group in the navigation pane and clicking on the check boxes in the **Select** column of the table. To perform tasks on all of those objects, click **Select All** from the table toolbar.

For group status information, status is displayed in the **Status** column in the work pane table. Status icons are displayed appropriately. If a group has both Hardware Messages and Operating System Messages, a message overlay icon is displayed indicating that both messages exist.

You can find more detailed help on the following:

User-Defined Groups

You can use the **Grouping** task under the Daily task group on the tasks pad to create your own group that you want to work with. This task allows you to create new groups and manage existing ones. To create a group:

1. Select one or more objects that you want to include in the group you want to work with.
2. Open the **Grouping** task from the **Daily** tasks pad. The **Manage Groups** window is displayed.
3. From the **Manage Groups** window select, **Create a new group**, specify a group name and description, click **OK** to complete.
4. The new user-defined group is displayed in the navigation pane under the **Custom Groups** node.

You can also create a group by using the pattern match method:

1. Without selecting an object you can open the **Grouping** task from the Custom Groups or Systems Management tasks pad.
2. From the **Create Pattern Match Group** window, select one or more group types that you want to create, specify a group name, description, and the pattern used to determine if an object should be part of the group, click **OK** to complete.
3. The new user-defined group is displayed in the navigation pane under the **Custom Groups** node.

   Note: Patterns specified in the **Managed Resource Pattern** input field are regular expressions. For example, if you specified **abc.***, all the resources that begin with **abc** will be included in that group.

HMC Management

HMC Management performs tasks that are associated with the management of this console. When you select **HMC Management** from the navigation pane the work pane contains a view of Hardware Management Console management tasks and their descriptions. These tasks are used for setting up the Hardware Management Console and securing the Hardware Management Console. Most likely, you will not use these actions on a regular basis.

To see what level of the HMC you are currently working with, point your mouse over **HMC Version** found at the top of the work pane.

To display the tasks in the work pane:

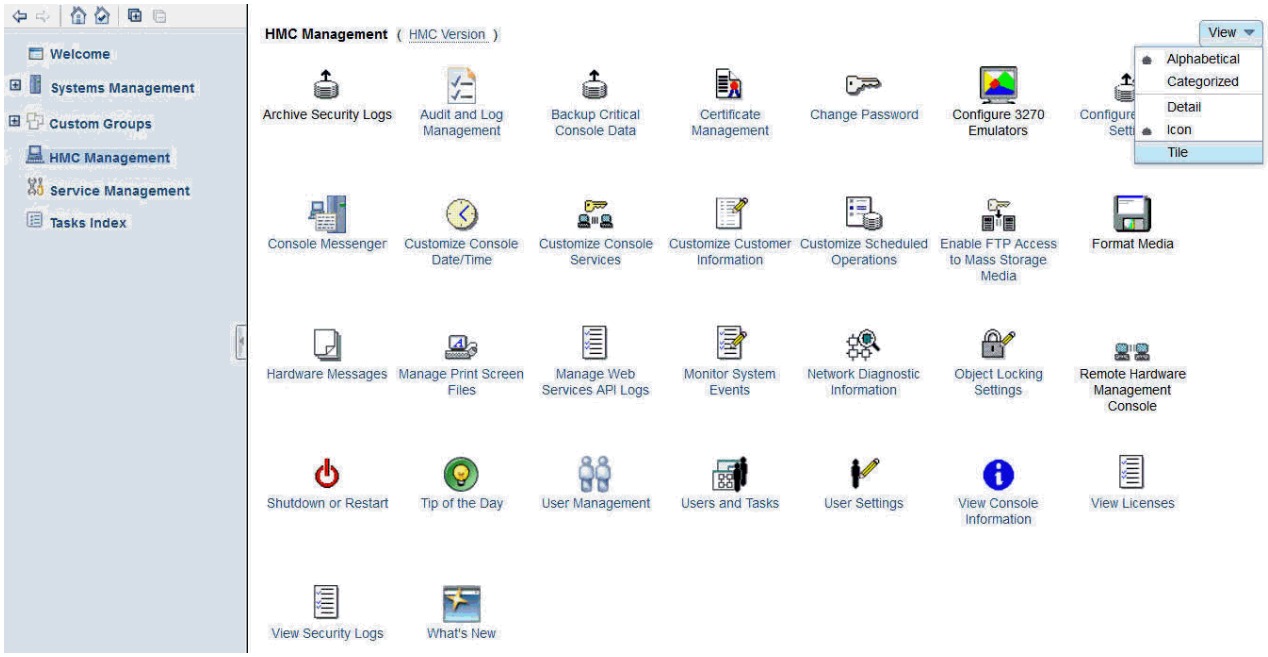
1. Select the **HMC Management** node in the navigation pane.
2. From the work pane, click the task you want to perform.
3. By default, a categorized listing of the tasks is displayed. The tasks are arranged in groups, which include:
   - Configuration
   - Security
4. From the work pane, click the task you want to perform.

If you want an alphabetic listing of the tasks, go to the **View** drop-down menu in the upper right corner of the work pane, and click **Alphabetical**. Click **Categorized** to go back to the task groups.

In addition, for each of the **Alphabetical** and **Categorized** sorts you can also choose a style of view:

- **Detail** displays a small task icon followed by the task name and description in two columns.
- **Icon** displays large task icons above the task name.
- **Tile** displays tasks that use large icons next to each task's name and description to help you find tasks by icon while still providing task descriptions.

See the following figure for an example of an alphabetical sort of the HMC management tasks that use the icon style.



The following HMC Management tasks, in alphabetic order, are displayed in the work pane depending on the task roles that are defined to your user ID. Some tasks cannot be opened if you are accessing the Hardware Management Console remotely.

Archive Security Logs
Audit and Log Management

Backup Critical Console Data
Certificate Management
Change Password
Configure 3270 Emulators
Configure Backup Settings
Configure Data Replication
Console Default User Settings
Console Messenger
Create Welcome Text
Customize API Settings
Customize Automatic Logon
Customize Console Date/Time
Customize Console Services
Customize Customer Information
Customize Network Settings
Customize Scheduled Operations
Domain Security
Enable FTP Access to Mass Storage Media
Format Media
Hardware Messages
HMC Mobile Settings
Manage Print Screen Files
Manage SSH Keys
Manage Web Services API Logs
Manage Syslog Servers
Monitor System Events
Network Diagnostic Information
Object Locking Settings
Reassign Hardware Management Console
Save/Restore Customizable Console Data
Save Upgrade Data
Power Off or Restart
Tip of the Day
Users and Tasks
User Management
User Settings
View Console Information
View Licenses
View PMV Records
View Security Logs
What's New

Service Management

Service Management performs tasks that are associated with servicing this console. When you select **Service Management** from the navigation pane the work pane contains a view of tasks and their descriptions. These tasks are used to service the Hardware Management Console and maintain its internal code.

To see what level of the HMC you are currently working with, point your mouse over **HMC Version** found at the top of the work pane.

To display the tasks in the work pane:

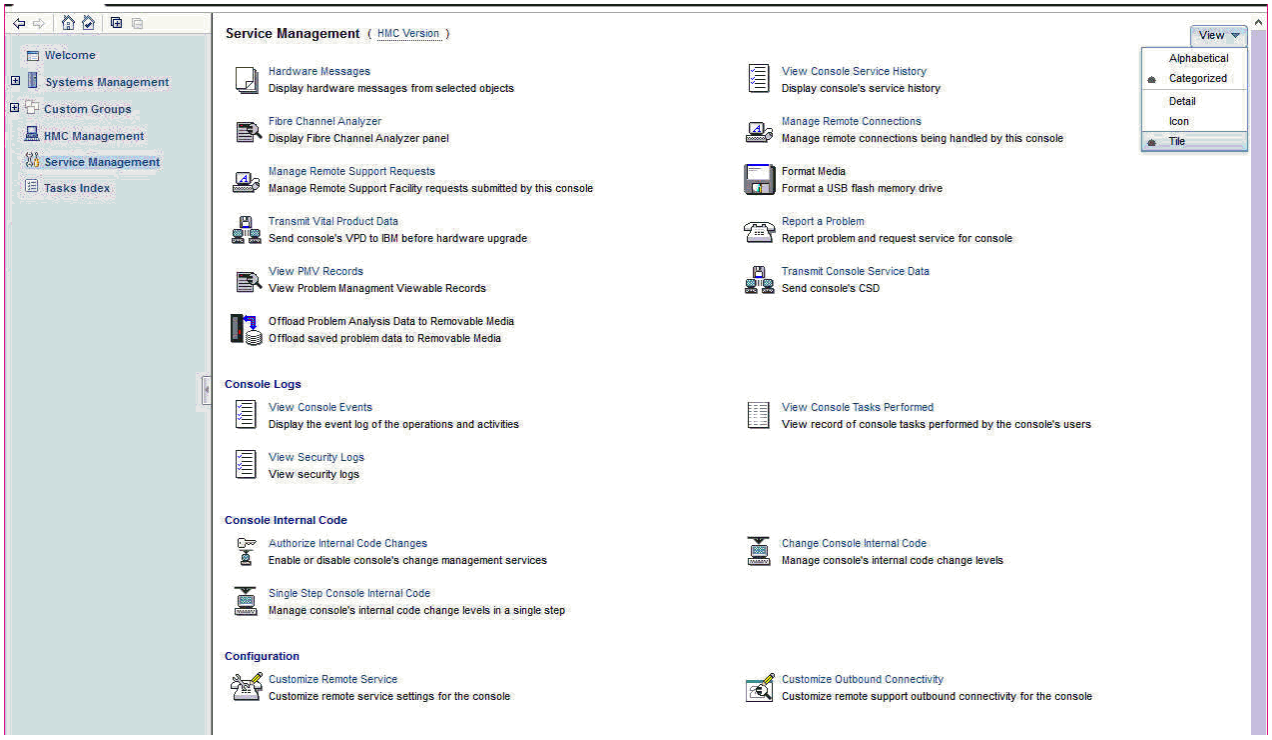
1. Select the **Service Management** node in the navigation pane.
2. From the work pane, click the task you want to perform.
3. By default, a categorized listing of the tasks is displayed. The groups include:
   - Console Logs
   - Console Internal Code
   - Configuration
4. From the work pane, click the task you want to perform.

If you want an alphabetic listing of the tasks, go to the **View** drop-down menu in the upper right corner of the work pane, and click **Alphabetical**. Click **Categorized** to go back to the task groups.

In addition, for each of the **Alphabetical** and **Categorized** sorts you can also choose a style of view:

- **Detail** displays a small task icon followed by the task name and description in two columns.
- **Icon** displays large task icons above the task name.
- **Tile** displays tasks that use large icons next to each task's name and description to help you find tasks by icon while still providing task descriptions.

See the following figure for an example of a categorized sort of the service management tasks that use the tile style. Some tasks cannot be opened if you are accessing the Hardware Management Console remotely.



Analyze Console Internal Code
Authorize Internal Code Changes
Block Automatic Licensed Internal Code Installation
Change Console Internal Code
Copy Console Logs to Media
Customize Outbound Connectivity
Customize Product Engineering Access

Customize Remote Service
Fibre Channel Analyzer
Format Media
Hardware Messages
Installation Complete Report
Manage Console Recovery
Manage Remote Connections
Manage Remote Support Requests
Offload Problem Analysis Data to Removable Media
Perform a Console Repair Action
Reassign Hardware Management Console
Rebuild Vital Product Data
Report a Problem
Single Step Console Internal Code
Transmit Console Service Data
Transmit Vital Product Data
View Console Events
View Console Service History
View Console Tasks Performed
View PMV Records
View Security Logs

Tasks Index

Tasks Index performs tasks by selecting them from the list. When you select **Tasks Index** from the navigation pane the work pane contains an alphabetical listing of the tasks available for the user ID you are logged in as. For an example of the tasks index, see the following figure. You can open these tasks by clicking on the task name from the table. The table includes the following information:

Name
Names the task. The icon associated with the task can be hidden by disabling the work pane icons from the **User Settings** task.

Permitted Objects
Lists the objects for which the task is applicable. The **HMC Management** and **Service Management** tasks require no targets, therefore permitted objects are not specified.

You can filter on this column to display only the tasks permitted by particular objects. For example, if you want to display only the tasks that are acceptable on a partition, you can do the following:

1. Select the **Show Filter Row** icon. The filter row is displayed.
2. Click **Filter** under **Permitted Objects**. The **Item** drop-down is displayed.
3. Click the drop-down arrow and select **Partitions**. Click **OK** to continue. A list of all tasks that apply to partitions is displayed.

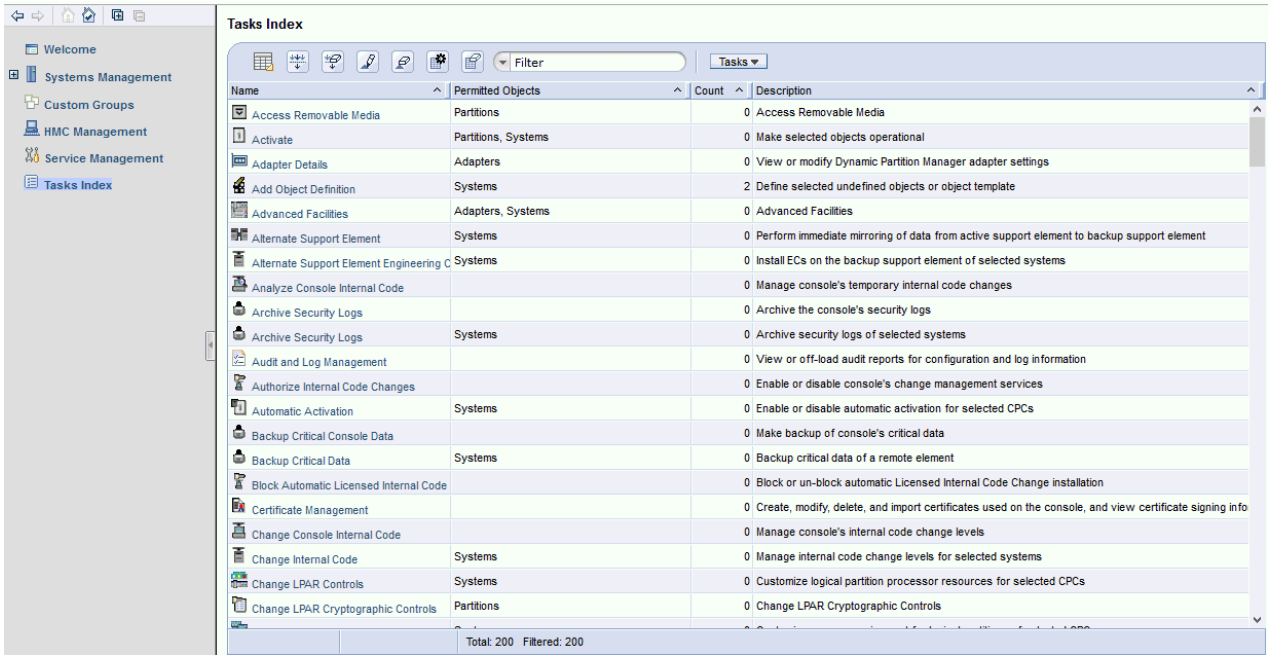
Count
Displays the number of times the task was opened by the current user.

Description
Describes the task.

Notes:

- If a task (for example, Activate) is applicable to more than one targeted object, a secondary panel is displayed for target selection.
- The **HMC Management** and **Service Management** tasks are opened without prompting for targets.

- Each time you open a task, the count increments by one. The values in the **Count** column may be reset to zero by clicking **Tasks** from the work pane table toolbar, then selecting **Reset Task Launch Count** (see the following figure).
- You can use the work pane table toolbar icons for selecting, filtering, sorting, and arranging the information in the table. See Work Pane Table Toolbar for more detailed information about using the icons and the quick filter function.

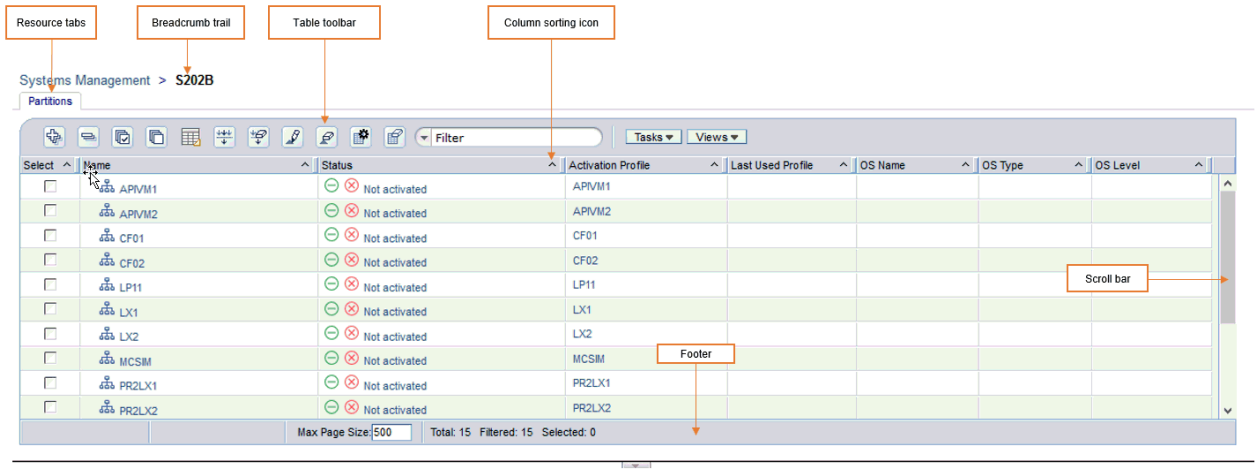


Work Pane

The work pane displays information based on the current selection from the navigation pane, resource tabs, or status bar. The work pane that is described in this section discusses the functions of the **Systems Management** work pane.

Selecting an object from the navigation pane displays a resources (configurable) table in the work pane as shown in the following figure. This figure identifies some of the areas of the configurable table.

Note: You can click on the name of an object in the work pane table to display the **Details** window.



You can find more detailed help on the work pane:

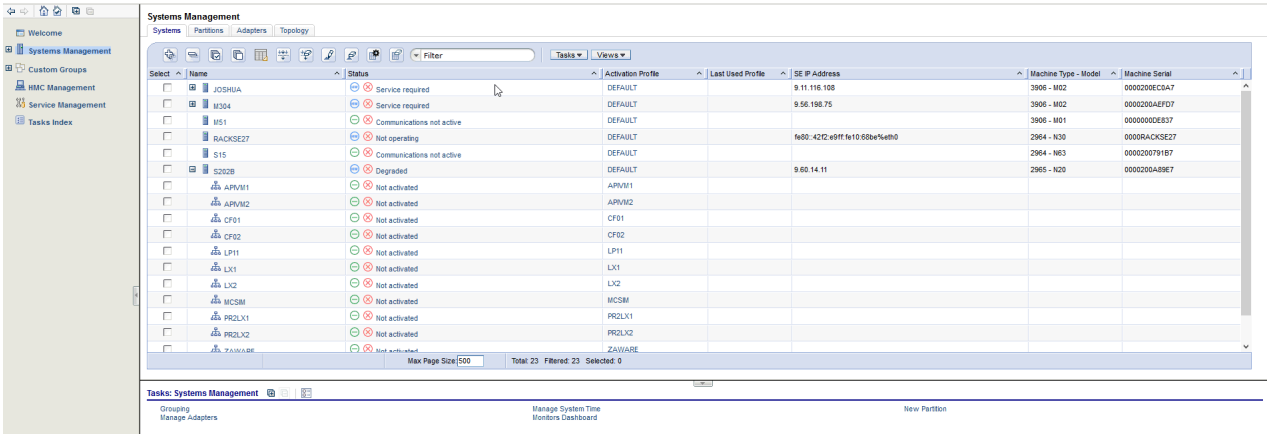
Work Pane Table

The information that is displayed in the work pane table allows you to view an object and its children in the same table including its hierarchical relationships. Initially, all the objects of the navigation pane display a default predefined table view. These tables provide sorting, filtering, and column configuration of the data and allow for customization of which managed objects are displayed in which order. See Work Pane Table Toolbar for customization of the managed objects.

If an object in the **Name** column contains additional objects, an icon to expand (+) or collapse (-) the item is located before the object name. This allows you to view all the additional objects within the object. You can continue to perform tasks on the expanded objects. As you place the cursor over the icon, help information is displayed. This information describes the function of the icon. If you have been sorting or filtering in the work pane table, the help information indicates that you are unable to expand or collapse the object.

You can customize these tables using the **Manage Views** option from the **Views** menu, see Creating a Custom Work Pane Table View.

For an example of the work pane table, see the following figure.



You can also reorder the columns of the tree view work pane table by using the drag and drop method:

1. Place the cursor on the heading of the column you want to move. You will see the cursor change to a cross hair indicating it can be moved.

   Note: The **Select** and **Name** columns are the only columns that cannot be moved.
2. Hold down the left mouse button and drag the column to the desired placement in the table. You cannot drag a column past the **Name** column.
3. The column settings are saved for you. If you want to go back to the original column settings, click the **Reset Column Order, Visibility, and Widths** icon.

You can find more detailed help on the following:

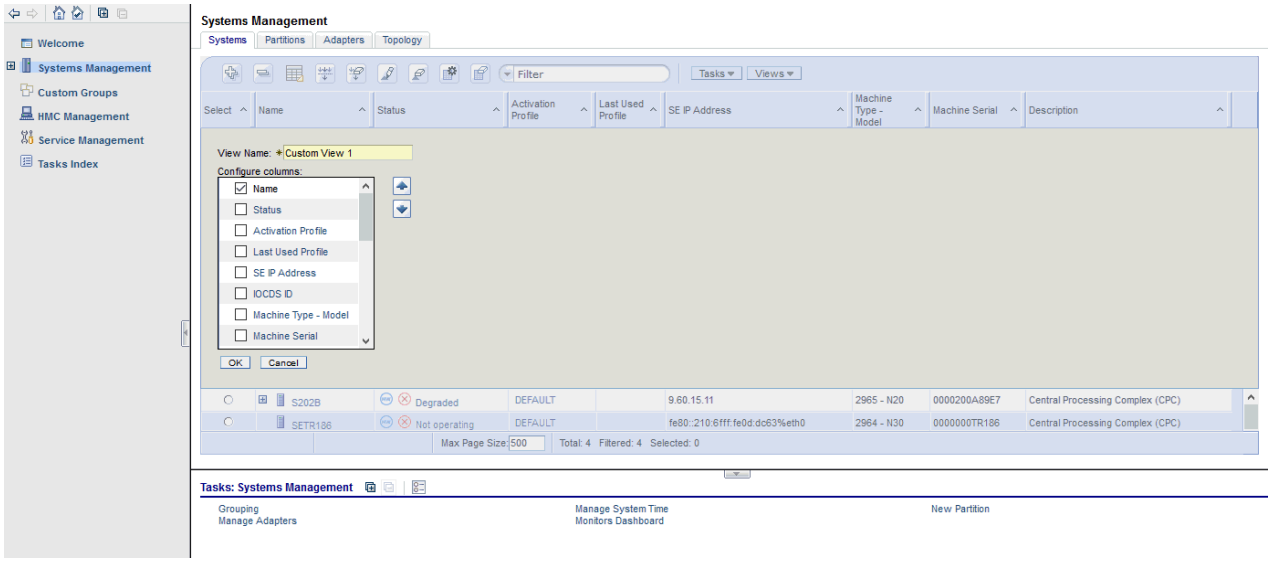
Creating a Custom Work Pane Table View

The columns that are available when you create customized views are an aggregate of its default table columns and the default table columns of all children. You can create your own user-defined column sets by selecting the **Manage Views** option from the **Views** menu.

If you are creating a new table view for the first time, perform the following steps:

1. Select the **Manage Views** option from the toolbar's **Views** menu.
2. Click **New** from the **Manage Views Dialog** that is displayed above the resources table.
3. You can specify a unique name for your custom view in the **View Name:** input field (see the following figure).

4. Select the items and order from the **Configure columns:** list that you want included in your view. Use the arrows to manage the order of the columns. Note, **Name** cannot be moved or hidden in the column configuration.
5. Click **OK** when you have completed the customization of your view. The new table view that you created is displayed when you select the **Views** menu.



Renaming a Custom Work Pane Table View

To rename a work pane table view, perform the following steps:

1. Select the **Manage Views** option from the toolbar's **Views** menu.
2. Select the custom table view name that you want to rename from the **Custom Table Views** list.
3. Click **Rename** in the **Manage Views Dialog**.
4. Specify a unique name for the selected custom table view name.
5. Click **OK** to save your new custom table view name.
6. The new name is displayed in the **View** menu.

Deleting a Custom Work Pane Table View

To delete a work pane table view, perform the following steps:

1. Select the **Manage Views** option from the toolbar's **Views** menu.
2. Select the custom table view name that you want to delete from the **Custom Table Views** list.
3. Click **Delete** in the **Manage Views Dialog**.
4. If a confirmation panel displays, click **OK** to confirm the deletion.
5. The selected name is not displayed in the **Views** menu.

Changing a Custom Work Pane Table View

The columns that are available when you create customized views are an aggregate of its default table columns and the default table columns of all children. To load the selected custom view and configure the columns in the table view, perform the following steps:

1. Select the **Manage Views** option from the toolbar's **Views** menu.
2. Select the custom table view name that you want to configure from the **Custom Table Views** list.
3. Click **Configure** in the **Manage Views Dialog**.
4. Change column selections and column order.
5. Click **OK** to save your changes.

6. The table is displayed as specified by your selections.

Work Pane Title and Breadcrumb Trail

The work pane title is displayed directly above the work pane table resource tabs. It identifies the Systems Management group. Once you begin drilling down to more specific objects from the navigation pane, a breadcrumb trail is displayed on the work pane title line. These breadcrumbs identify the navigation path that led you to the current work pane resources table. You can use the links from the navigation path to go to the previous pages. The resource tabs that are displayed in the work pane depends on the resource selected from the navigation pane.

Work Pane Table Footer

The table footer located at the bottom of the work pane table includes information about the number of pages of information included for the displayed table. It also displays additional summary information such as the number of items selected in the work pane table, filtered total, or the row count of the number of rows displayed in the current page.

You can change the number of items you want displayed on each page of the table by specifying a number in the **Max Page Size** input field, then press Enter. If more than one page of information is available a page count is displayed and you have the ability to go to a page directly by specifying a page number in the entry field, then press Enter.

Work Pane Table Toolbar

The toolbar at the top of the Systems Management work pane all resources table contains icons used to expand, collapse, export, select, filter, sort, and arrange the entries in the resources table. Hovering over the toolbar buttons displays their functions. The toolbar also includes **Tasks** and **Views** menus that can be used with the information displayed in the resources tables.

You can find more detailed help on the following:

Expanding and Collapsing Resources

The **Expand All** icon allows you to list all the resource groups. The **Collapse All** icon allows you to collapse all the resource groups. these icons work on all those objects that have additional objects associated with them in the table.

Note: These icons are disabled if you are sorting, filtering, or quick filtering. In addition, the table hierarchy is removed.

Selecting Rows

You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table. The table summary at the bottom of the table (work pane table footer) includes the total number of items that are selected.

Note: These icons are displayed only if you have chosen to select multiple objects. To set the object selection mode use the **User Settings** task.

Export Data

The **Export Data** icon allows for table data to be downloaded in a Comma Separated Values (CSV) file. This downloaded CSV file can then be imported into most spreadsheet applications.

Filtering

If you click **Filter Row**, a row is displayed under the title row of the table. Click **Filter** under a column to define a filter for that column that limits the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the desired filter in the filter row. Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria and the total number of items.

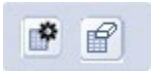
Note: When you are filtering within the work pane table the objects cannot be expanded.

Sorting

Edit Sort and **Clear All Sorts** perform multicolumn sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, you can perform single column sorting by selecting the ^ in the column header to change from ascending to descending order. Click **Clear All Sorts** to return to the default ordering.

Note: When you are sorting within the work pane table the objects cannot be expanded.

Column Configuration



Use the column configuration buttons to manage the columns displayed in the Systems Management tree view. Click **Configure Columns** to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns. When you have completed the configuration of the columns, click **OK**. The columns are displayed in the table as you specified. If you want to go back to the original layout of the table, click **Reset Column Order, Visibility, and Widths** on the table toolbar. Select one or more of the properties to reset to their original layout, and click **OK**.

Quick Filter

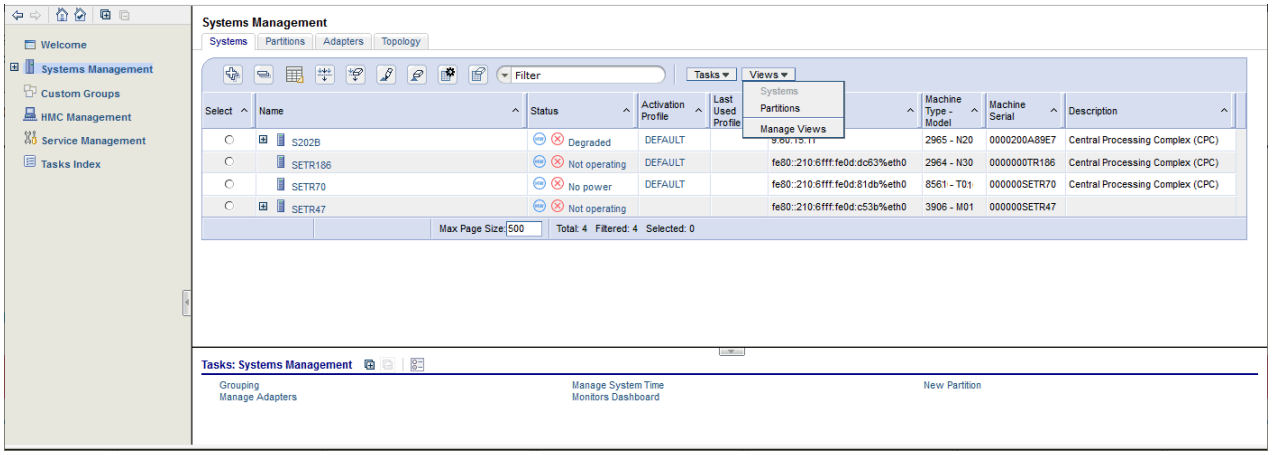
Use the quick filter function to enter a filter string in the Filter input field, and then press Enter to apply the filter. By default all the columns are filtered, showing only rows containing a cell whose value includes the filter text. Clicking the arrow displays a menu that restricts the columns to which the filter is applied.

Note: When you are sorting or filtering within the work pane table the objects cannot be expanded.

Views Menu

The **Views** menu is displayed on the work pane table toolbar when working with managed objects and custom groups. Use this menu to display different sets of attributes (columns) in the table. The following figure shows an example of the **Views** options when you are working with servers.

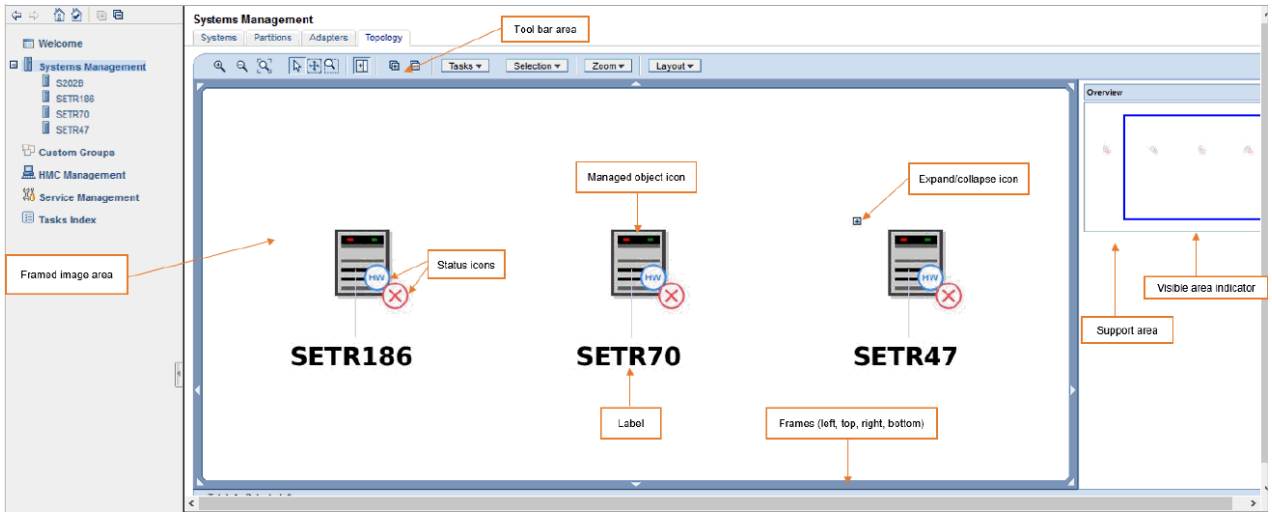
For information on defining your own table view, see Creating a Custom Work Pane Table View.



Topology

The information that is displayed from the **Topology** resource tab is a graphical relationship-based view of the objects. It is composed of the Toolbar, Framed image, and Support areas, some of which are identified in the following figure.

Note: When an object's status changes or new objects have been added or removed the image is updated and the new content automatically fits in the current work pane area.



Toolbar

This area of the topology work pane consists of several icons and drop-down menus for controlling the appearance and actions of the topology view. You can mouse over the toolbar icons for short descriptions of the respective actions.

Icons

The toolbar icons are divided into the following groups:

- Content zoom and fit control - used for enlarging and shrinking the images and automatically fitting the image content within the work pane area:
  - **Zoom In**
  - **Zoom Out**
  - **Fit Contents to Viewport**
- Mouse modes - controls the function of the mouse.
  - **Select Mouse Mode** (default) - clicking on an object causes it's selection to be toggled.

- When a node is selected, the tasks context menu icon is displayed and the tasks in the **Tasks** drop-down menu are also updated.
- When multiple selection is enabled, press (Ctrl +) left mouse button to select multiple nodes. Left clicking in a blank area of the work pane area de-selects all selected nodes.

– **Pan Mouse Mode** - scroll the objects in the frame up, down, left, or right using direct manipulation. After you release the mouse button, the mouse mode is automatically changed back to the selection mode.

– **Zoom Mouse Mode** - creates a viewport to zoom into. The mouse is used to select a rectangular area (a blue box is displayed to indicate the area) as part of the image frame to zoom into. The objects in the area are enlarged. After you release the mouse button, the mouse mode is automatically changed back to the selection mode.

- **Toggle Support Area Visibility** - toggles the visibility of the support area, which displays the image Overview.
- **Expand All** / **Collapse All** icons - expand (display) or collapse (hide) the children of all objects.

Drop-down Menus

The drop-down menus include:

- **Tasks** - when one or more objects are selected the tasks available for the objects are displayed. These same tasks are displayed in the context menu and tasks pad.
- **Selection** - allows you to select all the objects, deselect all the objects, or invert selection.
- **Zoom** - allows you to change the content size:

  Fit Content
  Automatically fits the objects in the framed image area.

  50%
  Size of each object is displayed as half it's actual size.

  100%
  Size of each object is displayed as the actual size.

  200%
  Size of each object is displayed as twice the actual size.
- **Layout** - allows you to select the preferred object layout:

  Rerun Current
  Redraws the image using the current layout.

  Tree
  Displays objects in a hierarchical tree format.

  Hierarchical
  Arranges the nodes so that the majority of links are short and flow uniformly in the same direction.

  Circular
  Objects are automatically grouped into either a ring or star topology.

  Uniform length
  Searches for a configuration of the graph where the length of the links are the same.

  Grid
  Objects are placed into a grid.

Framed Image

This area displays graphical representations of managed objects. Each object is represented with a graphic which displays the object's name, it's status, it's tasks (in a context menu), and an expand/collapse button if it has children. Note some of the following characteristics as you work in the framed image:

- If an object is selected, the label uses black font color and blue background color, the background of the object icon also turns blue.

- The status icon overlay is a combination of the system status icon, hardware messages icon, and the operating system messages icon.
- If an object is locked, the lock icon is displayed.
- If an object is busy, the busy icon is displayed.
- Click on a frame segment to redraw the image that has been panned in the associated direction.
- Click the right mouse button in an empty area of the images frame to display a context menu with the following additional options (similar to the toolbar functions):
  - **Collapse All**
  - **Expand All**
  - **Selection**
  - **Zoom**
  - **Layout**
  - **Center here** - centers you on the current mouse position.
  - **Move here** - moves the selected object into the current mouse position. (This option displays only when exactly one object is selected.)
- Click the right mouse button or click the double arrow icon on a selected object to display a context menu with the following additional options:
  - **Zoom To** - zooms into the object in the center of the viewer display area.
  - **Center here** - centers you on this object.
  - **Expand** - expands the object by displaying any children if an object is collapsed.
  - **Collapse** - collapses the object by hiding it's children if an object is expanded.

Support

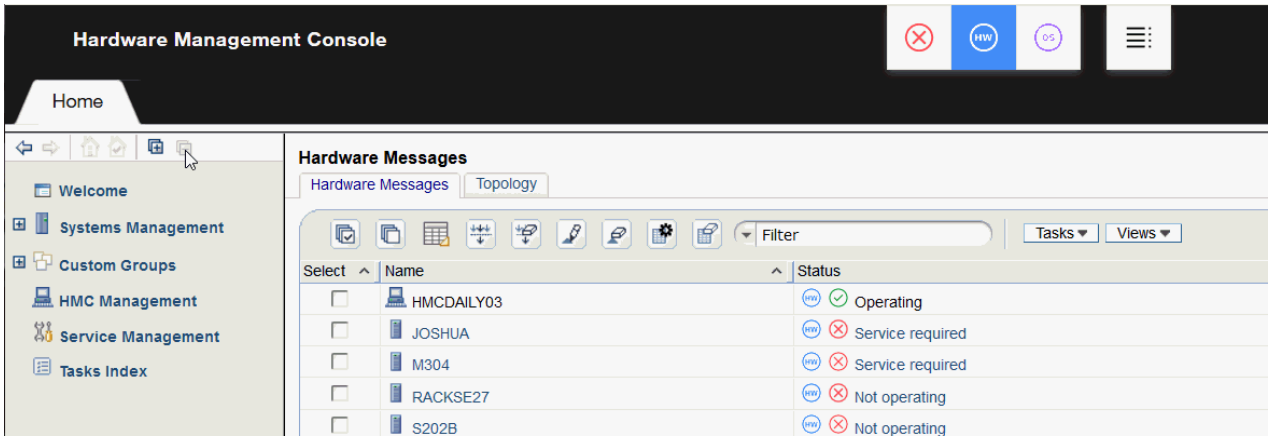
This optional area (click **Toggle Support Area Visibility** icon on the toolbar) is used to display a high level view of the topology of the entire system configuration with only the status of managed resources represented. Moving the rectangle changes what is displayed in greater detail in the image viewer area.

Status Bar

The status bar, located in the masthead, provides an "at a glance" view of the indicators (icons) for exceptions, hardware messages, operating system messages, and overall system status. When no objects exist with a given status icon, then the icons are green to convey a positive status.

When objects exist with a status icon other than green they are represented by red for exceptions, blue for hardware messages, and purple for operating system messages. Icons are displayed in the work pane table next to a managed object when it is in an Exception State or when it receives a hardware or operating system message.

Click any of the individual icons in the status bar to view a listing of resources. For example, select the **Hardware Messages** icon to view all resources with a hardware message state in the work pane, as shown in the following figure.



You can find more detailed help on the following elements of the status bar:

Exceptions

If any managed object is in unacceptable state, the Exceptions indicator (icon) is displayed on the status bar. When you select the Exceptions indicator(icon), it displays a table in the work pane of the objects in an unacceptable state.

Hardware Messages

If a managed object or the Hardware Management Console receives a hardware message, the Hardware Message indicator (icon) is displayed on the status bar. When you select the **Hardware Messages** icon, it displays a table in the work pane of the objects with hardware messages. The table includes the object name, status, and description. To view the hardware message for a particular object you can click the Hardware Message icon in the **Status** column or you can select the object by clicking in the **Select** column next to one or more object names, click **Daily** in the tasks pad, and click **Hardware Messages**. The **Hardware Messages** window is displayed. Now you can work with its messages.

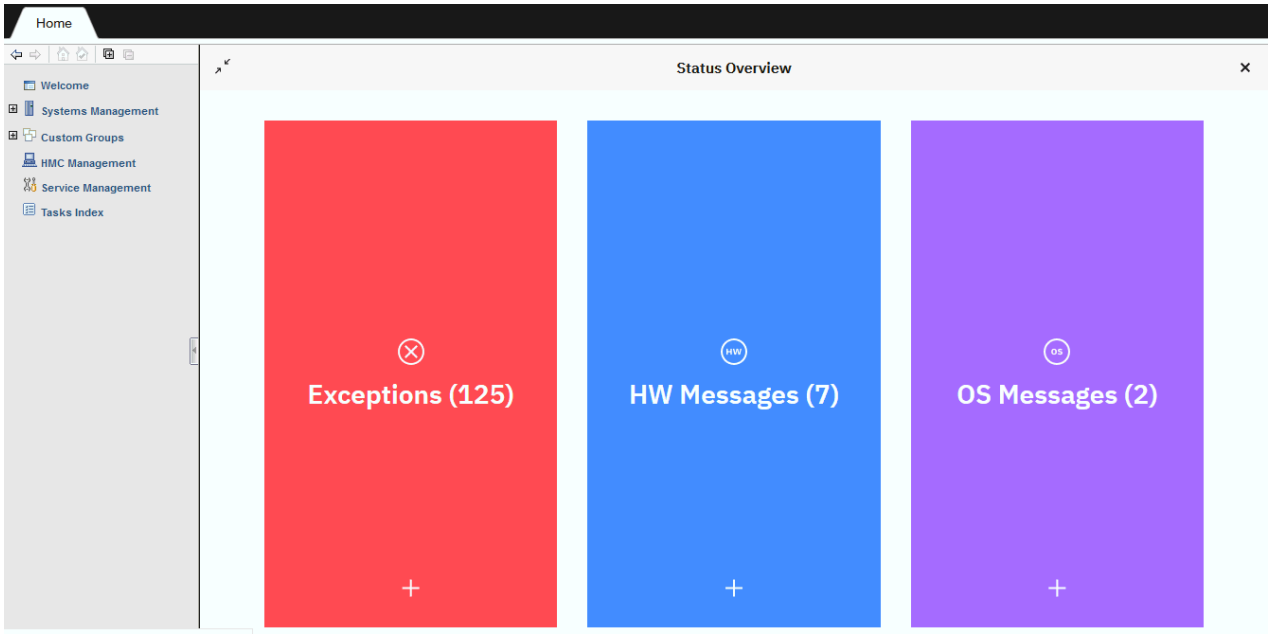
Operating System Messages

If a managed object receives an operating system message, the Operating System Message indicator (icon) is displayed on the Status Bar. When you select the **Operating System Messages** indicator (icon), it displays only objects with unviewed operating system messages that require attention. The table includes the object name, status, and description. To view the operating system messages for a particular object you can click the Operating System Messages icon in the **Status** column or you can select the object by clicking in the **Select** column next to one or more object names, click **Daily** in the tasks pad, and click **Operating System Messages**. The **Operating System Messages** window is displayed. Now you can work with your messages.

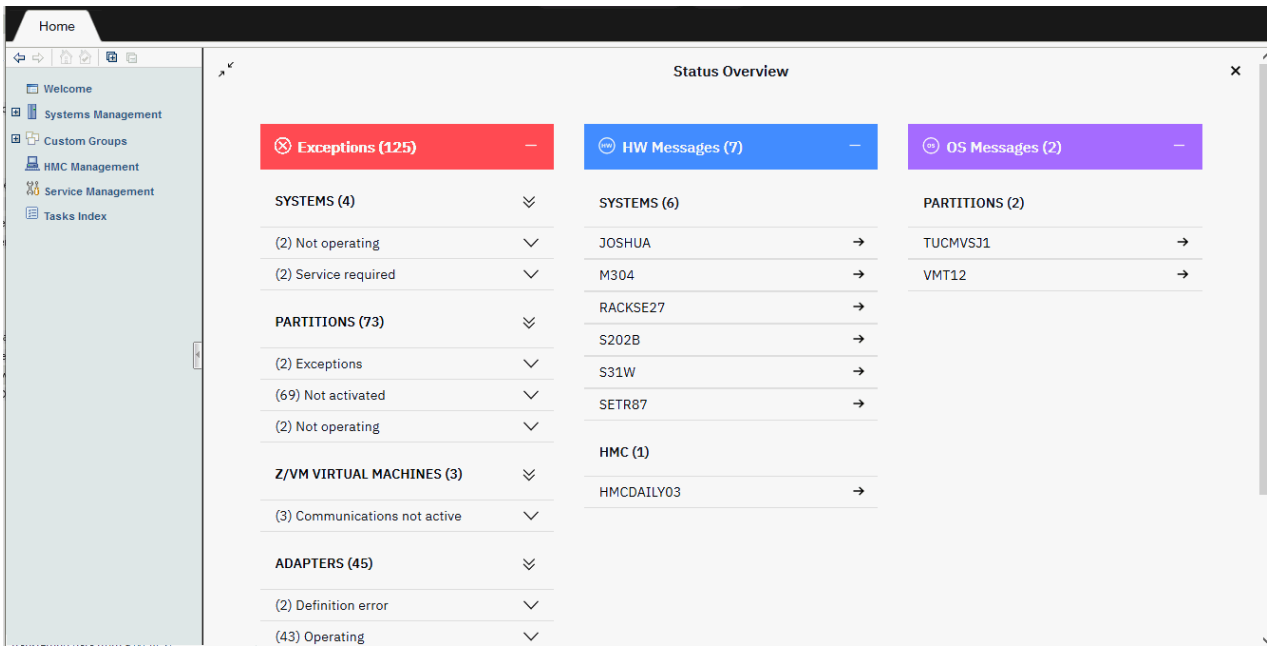
Status Overview

When you select the **Status Overview** icon, it displays a more detailed view of overall status in the work pane. It summarizes the total number of exceptions, hardware messages, and operating system messages by objects. Then, you can select a link from the work pane to display all objects with the particular state in the work pane. Following are some examples of the Status Overview function.

If you select the **Status Overview** icon when the Home tab is selected, the Status Overview is expanded in the work area, as shown in the following example.



If you select **Exceptions**, **HW Messages**, or **OS Messages**, content that is applicable for each appears as it would if you selected the icons form the Status Bar in the masthead area. If you select the plus sign (+) for each, the content is expanded with more detailed information as shown in the following example.



You can use these additional icons from the **Status Overview** area:

Expand or Collapse All

Select this icon to view (expand) all the objects in an unacceptable state. You can select it again to hide (collapse) all the objects.

Expand or Collapse

Select this icon to view (expand) the objects for that specific unacceptable state. You can select it again to hide (collapse) the objects for that specific unacceptable state.

View message

Select this icon to view the hardware messages and operating system messages that are associated with the particular system.

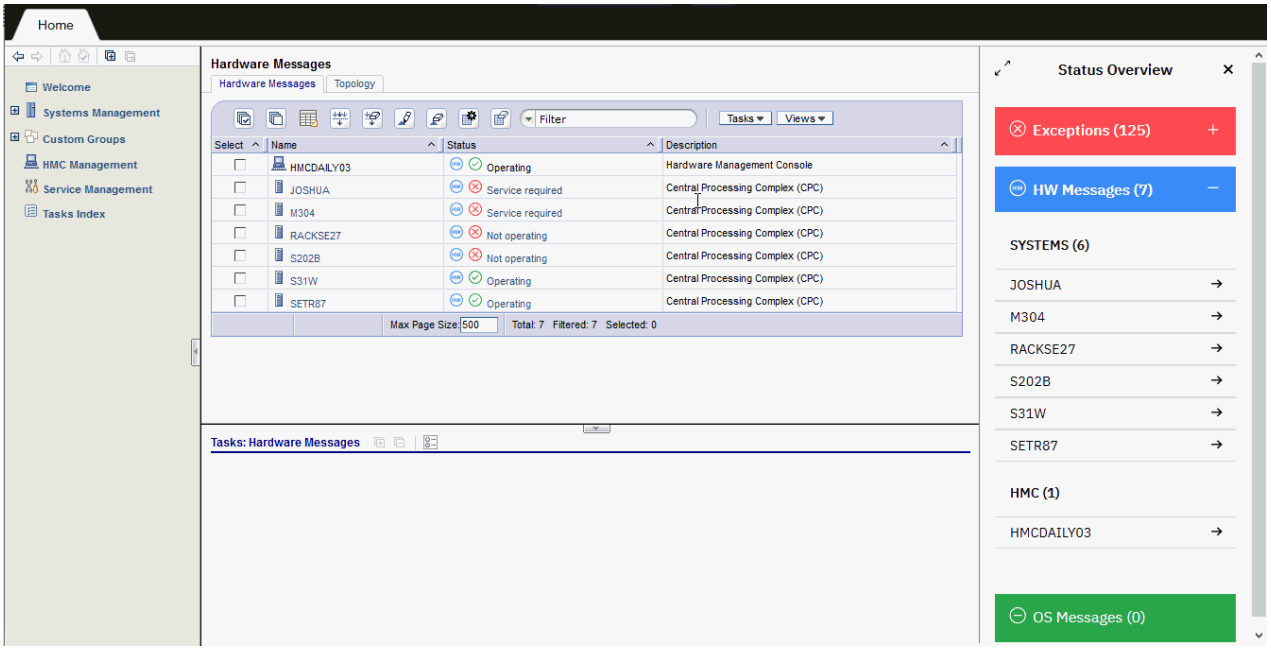
Status Overview - Close

Select this icon to close the Status Overview area.

Collapse or Expand Status Overview

Select this icon to collapse the Status Overview area where it appears along the right side of the user interface, as seen in the following example. You can select it again to make it viewable (expand) again in the work pane.

Note: When the Status Overview is collapsed, it is always visible whether the Home tab or a task tab is selected.



Object Locking for Disruptive Tasks

You can tell when a server or server image is locked because a small lock icon is displayed next to the server name in the work pane. In the topology view the icon is displayed as an overlay of the object icon.

Note: Object locking cannot be applied to IBM Dynamic Partition Manager (DPM) objects.

The setting of a server or server image's toggle lock determines whether you can perform a disruptive task on the server or server image. You can lock an individual object or automatically lock all objects.

To individually lock (or unlock) a server or server image:

1. Select the server from the table that you want to lock (or unlock).
2. Click **System Details** from the tasks pad, the **System Details** window is displayed.
3. You can select **Yes** or **No** for **Lock out disruptive tasks**.
4. Click **Apply** to make the change.

An alternate way to lock (or unlock) an individual object is to:

1. Select the object from the table that you want to lock (or unlock).
2. Click **Toggle Lock** from the tasks pad.

To lock (or unlock) more than one server or server image:

1. You must have multiple selections enabled from the **Controls** tab of the **User Settings** task.
2. Select all the servers from the table that you want locked (or unlocked).
3. Click **Toggle Lock** in the tasks pad.
4. The icons in the table will change to either a server icon or a small lock icon, depending on what action you want to perform on that server or server image.

There is also an automatic way to lock all the servers and server images that are displayed on the workspace at one time. Unlike the previous ways for locking an object, using this method can cause the object to be relocked automatically if it was unlocked to perform a task on it. To use this method, you must have a user ID with the predefined user roles of an *Advanced Operator, System Programmer, Access Administrator*, or *Service Representative* for the Hardware Management Console.

1. Open the **Object Locking Settings** task from the **HMC Management** work pane. The **Locking** window is displayed.
2. Select **Automatically lock all managed objects** or **Relock after a task has been run** or both.

Tasks

HMC Tasks

You can use the Table of Contents for more information on the Hardware Management Console (HMC) tasks.

Access Removable Media

Accessing the Access Removable Media task

Use this task for installing Linux, or other software as specified in its information from removable media as a guest of z/VM, if the z/VM support running in the logical partition supports this capability. This task is available only on System z10® or later.

To install Linux or other software from removable media as a guest of z/VM:

1. Properly insert removable media.
2. Select a partition.
3. Open the **Access Removable Media** task. The Access to Removable Media window is displayed.

4. Select the removable media that you want the specified partition to access, then insert the media into the Hardware Management Console.
5. Click **OK** to proceed with assigning the selected removable media for use by the partition. The confirmation window is displayed.

Access Removable Media

Use this window for installing Linux, or other software as specified in its information, from removable media as a guest of z/VM.

Available Removable Media
This table lists the removable media devices that you can use. Select the removable media that you want to assign for use by the specified partition, then insert the media into the Hardware Management Console.

Note: The selected partition needs to have an operating system running that supports this capability.

The possible media choices include:

- DVD-RAM
- USB flash memory drive (if inserted)

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

OK
To continue with assigning the selected removable media for use by the partition, click **OK**.

The **Access Removable Media Task Confirmation** window is displayed. Click **Yes** if you want to allow the selected partition access to the media, otherwise click **No**.

Cancel
To close this window and end the task without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Activate

Accessing the Activate task when targeting one or more CPCs or objects

Notes:

- This task is not available when one or more managed systems have DPM enabled.
- Activate is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task controls starting up the system including power-on reset, partition activation, and initial program load of your operating system software. Activate is your primary function for CPC or CPC image start up. Activate senses the status of the object, then performs only those actions necessary to get the object to an operational state. For example, if the CPC is already in the power-on reset complete state, Activate skips the power-on reset step and proceeds with the load of the operating system.

If the CPC allows activation to include a power-on and the CPC is powered-off, Activate powers it on from the Hardware Management Console.

The Activate function uses profiles, which contain the parameters needed to put the system in an operational state. The profiles are stored in each CPC Support Element. A set of default activation profiles are shipped with the CPC. The values contained in these profiles might not be correct for your environment. See "Activation Profiles" for a description of activation profiles. See the **Customize/Delete Activation Profiles** task for information about creating and modifying activation profiles.

To start activation:

1. Select one or more CPCs or CPC images.
2. Open the **Activate** task.

   Note: If one or more of the selected CPCs have associated secondary objects (for example, an image or coupling facility image), a Secondary Object Notification for Disruptive Task message window is displayed with a list of the active secondary objects. Review the list before proceeding. If you click **Yes** to proceed, the Activate Task Confirmation window is displayed. Review the confirmation text to decide whether to proceed with the task.
3. If you want to review the profile that is used for activation, click **View Activation Profile...**; the View Activation Profiles window is displayed, showing the values that are set.
4. If you want to continue this task, click **Yes**. If you want to end the task, click **No**. If you click **Yes**, the Activate Progress window is displayed indicating the progress of the activation and the outcome.
5. Click **OK** to close the window when the activation completes successfully.

   Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Activate Task Confirmation

Note: This task is not available when one or more managed systems have DPM enabled.

Use this window to verify the objects and if they support activation profiles, the activation profiles to be used for each object.

Profile information for each object that supports profiles can be obtained by selecting an object and clicking **View Details...**.

Activate Table

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions:

Show Filter Row
If you select the **Show Filter Row** button a row is displayed under the title row of the table. Select Filter under a column to define a filter for that column to limit the entries in a table. Tables can be filtered to show only those entries most important to you. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row.

Clear All Filters
Select the **Clear All Filters** button to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
The **Edit Sort** button is used to perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Following are descriptions for the columns displayed in the Activate table:

Object Name
Displays the names of the objects that have been selected for the **Activate** task.

Type
Displays the processing environment of the selected objects.

Activation Profile
Displays the profiles for the selected objects.

Last Used Profile
Displays the name of the last profile used by **Activate**. If no previous profile has been used, the message "Not set via Activate" appears in place of a profile name.

Confirmation Text
Displays additional information about the selected object.

You can choose the following actions from this window:

Yes
To activate the selected object(s), click **Yes**.

No
To cancel your request to activate this object, click **No**.

View Details...
To display the values of the profile settings, click **View Details...**.

Help
To display help for the current window, click **Help**.

Activation Profiles List

Customize/Delete or View Activation Profiles List

Use this window to view, change, create, and delete activation profiles for the selected objects.

List of profiles for *object-name*
Lists the activation profiles for the CPC or image selected.

The toolbar at the top of the Overview table contains icons used to select, filter, sort, and arrange the columns in the Overview table.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. Filter the data you would like to appear in the Overview table by manipulating the information in the table. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions:

Select All
The **Select All** icon allows you to select all the objects in the Overview table.

Deselect All
The **Deselect All** icon allows you to deselect all the objects in the Overview table.

Show Filter Row
The **Show Filter Row** icon allows you to define a filter for a table column to limit the entries in a table. Tables can be filtered to show only those entries most important to you. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row.

Clear All Filters
The **Clear All Filters** icon allows you to return to the complete table summary. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
The **Edit Sort** icon allows you to perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
The **Clear All Sorts** icon allows you to return to the default ordering.

Configure Columns
The **Configure Columns** icon allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns.

Select one Profile Name from the list, then click on the task you want to perform.

Profile Name
Displays the name of the profile.

Type
Identifies the general contents and use of the profile.

Profile Description
Displays additional information about the profile, such as its specific contents or use.

Note: A description is an optional profile parameter; some profiles may not have one. When you customize the profile you can provide or omit its description.

Additional information is available from this window:

New image profile (Customize/Delete only)
To display the new image profile wizard to guide you through the process of creating a new image profile for the selected new image profile, click **New image profile**.

Customize profile (Customize/Delete only)
To select a reset, load, image, group, or list of image profiles that will allow you to modify certain parameters and then be applied to those selected profiles, click **Customize profile**.

Notes:

- If two or more profiles are selected and they are not all image profiles, **Customize profile** is grayed out.
- If an IOCDS **D0** image profile is selected, this image profile displays in view only.

Delete (Customize/Delete only)
To erase the selected activation profile, click **Delete**.

Notes:

- You cannot delete the activation profiles named **DEFAULT** and **DEFAULTLOAD**.
- When you click **Delete** to delete the selected activation profile, you will delete the profile for the object on the current window only.

  Deleting the selected activation profile will *not* affect profiles with the same name for other objects in other windows.

View (View only)
To view the current information and settings of the selected activation profile for the CPC, click **View**.

Close
To close the window when you are finished working with activation profiles for the selected object, click **Close**.

Closing the window does *not* affect any profiles you deleted.

Help
To display help for the current window, click **Help**.

View LPAR Weights

Use the View LPAR Weights window to check the partitions initial processing weights for the selected active IOCDS. You can use the drop-down menu to select a different IOCDS.

An initial processing weight represents the share of resources guaranteed to a logical partition when all processor resources are in use. Otherwise, when excess processor resources are available, the logical partition can use them if necessary. When a logical partition is not using its share of processor resources, other active logical partitions can use them. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

Image Name
Specifies the name of the partitions assigned to the selected IOCDS.

Processor Type
Specifies the processor types for each partition in the selected ICODS.

Initial Weight
Specifies the relative amount of shared processor resources assigned to each partition.

Additional functions on this window include:

Close
To close this window, click **Close**.

Help
To display help for the current window, click **Help**.

Change Object Options

Use this window to assign a profile for the next activation of this object or to view the profile you have selected. The setting applies to the instance of the object contained in the group specified on the **Instance Information** tab of its **Details** task. More than one system defined or user-defined custom group can contain a unique instance of the same object; this situation allows assigning different activation profiles to different instances of the same system or image. You can set different activation profiles for a single system or image by invoking its **Details** task from the different groups containing the object and selecting **Change Options...**.

Currently assigned profile
Specifies the profile name that has been assigned to this object for this group.

Profile to be assigned

Specifies the profile name you supplied or selected from the list provided.

Profile Name
Displays the name of the profile.

Type
Identifies the general contents and use of the profile.

Image
Indicates the profile can be used to activate an image of a CPC.

Load
Indicates the profile can be used to activate a Central Processor Complex (CPC) or an image and load a control program or operating system.

Reset
Indicates the profile can be used to activate a CPC.

Profile Description
Displays additional information about the profile, such as its specific contents or use.

Note: A description is an optional profile parameter; some profiles may not have one. The person who customizes the profile provides or omits its description.

OK
To assign the selected profile to be used during system activation, click **OK**.

View
To view the contents of the selected activation profile, click **View**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Adapter Details

Accessing the Adapter Details task

Use this task for information about the selected adapter that is enabled. This window displays the current instance information and acceptable status settings for a selected adapter.

You can access this task from the main console page by selecting the Systems Management node, by selecting a specific adapter(from the Adapters tab), or by selecting this task in the Tasks index. You can use either the default SYSPROG user ID or any user IDs that a system administrator has authorized to this task through customization controls in the **User Management** task.

To display and view the details for the selected adapter, complete the following steps.

1. Select the PCHID you want to view adapter details.
2. Open the **Adapter Details** task. The Adapter Details window is displayed.
3. Review the settings under Acceptable Status. Optionally, use its check boxes and click **Apply** to change the acceptable status settings.

Adapter details

This window displays current information and acceptable status settings for the selected adapter.

- **General** includes general information about the adapter's operating conditions and characteristics.
- **Status** includes the current status, state, and acceptable status. Acceptable status settings determine which of the adapter statuses are acceptable and which statuses are unacceptable.

  Review the settings under **Acceptable status**. Optionally, use its check boxes and click **Apply** to change the acceptable status settings.
- **Partitions** includes information on the associated CHPIDs, Cryptos, or FIDs defined for the selected adapter for all partitions.

General

Use the General details section to view information for the selected adapter:

Name:
Indicates the name of the target adapter, which can be 1 - 64 characters in length. Supported characters are alphanumeric, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. An adapter name must uniquely identify the adapter from all other adapters defined on the same system.

System:
Displays the name for the system.

Location:
Displays the location number of the cage and card slot in which the adapter's hardware is installed. Displays the position number on the card in the slot of the adapter's jack.

Type:
Displays the adapter type of the target adapter.

Size (GiB)
Displays the NVMe adapter size in Gibibyte.

Vendor ID
Displays the manufacturer of the installed SSD for the target NVMe adapter.

Subsystem vendor ID
indicates the manufacturer of the installed SSD for the target NVMe adapter.

Serial number
Displays the serial number of the installed SSD for the target NVMe adapter.

Model number
Displays the model number of the installed SSD for the target NVMe adapter.

Swapped with:
Displays the name of the adapter that it is swapped with. If the adapter is not swapped, this field displays none (displays for FICON Express).

Operation mode:
Displays mode of operation for the targeted adapter (displays for Internal Couplings, FICON Express, OSA-Express, Coupling Express LR Channel, Integrated Coupling Adapter SR, HiperSockets).

Network IDs:
Identifies the physical layer 2 LAN fabric or physical broadcast domain. You can use this value to logically associate the system features, adapters, and ports to be physically connected to your network (displays for Internal Shared Memory, OSA-Express, RoCE adapters).

Physical adapter ID:
Indicates the physical adapter ID for the selected adapter (displays for Coupling Express LR, Integrated Coupling Adapter SR).

Port:
Displays the adapter port number (displays for Coupling Express LR, Integrated Coupling Adapter SR).

Status

Status settings determine which of the adapter statuses are acceptable and which statuses are unacceptable:

Status

Indicates the status of the target adapter. This field can indicate Operating or Not Operating. This field is updated dynamically, so that it always reflects the current status of the target adapter.

State

Indicates the state of the adapter. This field can indicate Online or Offline. This field is updated dynamically, so that it always reflects the current state of the target adapter.

Acceptable status

This term indicates the summarized status of the adapters.

- Acceptable statuses, indicated by check marks in their check boxes, are not reported as exceptions.
- Unacceptable statuses, indicated by empty check boxes, are reported as exceptions.
- Check boxes are disabled, if the user does not have **Adapter Details** task permission.

Settings determine which of the adapter statuses are acceptable and which statuses are unacceptable. Setting the adapter's acceptable status settings allows you to control which statuses are reported as exceptions. The following adapter status values can be summarized as acceptable:

Operating
The adapter is operating.

Suspended
The adapter is suspended. The adapter is not operating.

No Power
The power is off for the hardware that supports the adapter. The adapter is not operating.

Service
The adapter is in single channel service (SCS) mode and is not in the active I/O configuration. The adapter is not operating.

Not Defined
The adapter is not defined in the active IOCDS. The adapter is not operating.

Definition error
The adapter specified in the active input/output configuration data set (IOCDS) does not match the characteristics of the installed adapter, or the adapter type is incompatible with the current storage allocation, or the level of the installed adapter hardware does not support the definition in the IOCD. The adapter is not operating.

Wrap block
A wrap block is installed on the adapter's interface.

Note: Wrap blocks are used during special diagnostic tests performed on the adapter. Wrap blocks must be removed prior to system initialization to allow the adapter to initialize completely. The adapter is not operating.

Check stopped
The adapter is unavailable due to a permanent machine error affecting the adapter hardware. The adapter is not operating.

Permanent error
The adapter is unavailable due to a permanent outboard error. The adapter is not operating.

Loss of signal
The adapter detected a link-signal error. The level of the signal on the link is below the value specified for reliable communication.

Loss of synchronization
The adapter detected a link-signal error. The bit synchronization with the signal was lost. The adapter is not operating

Not operational link
The adapter detected a link failure due to a not-operational sequence. The channel path is not operating.

Sequence time-out
The channel path detected a link failure due to a sequence time out. The adapter is not operating.

Sequence not permitted
The adapter detected a link failure due to an illegal sequence for a link. The adapter is not operating.

Terminal condition
The adapter is not available due to an interface-hung condition. This can occur after an interface or adapter error if the control unit or device fails to disconnect from the interface when requested by the adapter. The adapter is not operating

Offline signal received
The adapter detected an offline sequence, indicating that the sender is in offline mode and subsequent link-signal errors detected by the adapter are not to be reported. For an ES conversion adapter, this condition can occur only when the adapter is wrongly attached to another adapter, switch, or control unit instead of an ESCON Converter. The adapter is not operating.

Initializing
The firmware is being loaded into the adapter card and then the adapter card is starting.

Degraded
A degraded status indicates that, although the adapter is still operating, some conditions are causing a degraded status.

Test mode
The adapter is in test mode. The adapter is not operating

Bit error threshold exceeded
The number of bit errors the adapter detected while receiving or sending data is more than the threshold set for its bit error counter. The adapter is not operating

IFCC threshold exceeded
The number of interface control checks (IFCCs) the adapter detected is more than the threshold set for its IFCC counter. IFCCs may continue to occur, but their error logs will not be created and sent to the Support Element.

Stopped
The channel path is not operating.

I/O suppressed
The adapter has input/output (I/O) suppression active. I/O suppression prevents the adapter subsystem from selecting any device and fetching the first adapter command word (CCW) of a adapter program. The adapter is not operating.

Fabric login sequence failure
This condition means that the adapter detected a failure during that fabric login procedure

Port login sequence failure
This condition means that the adapter detected a failure during the registration procedure. In order for a FICON® adapter to communicate with devices on a control unit, it must perform a Port Login with that control unit.

State change registration failure
This condition means that the adapter detected a failure during the registration procedure. A FICON adapter is required to register with the switch to receive state change notification

Invalid attachment failure
Occurs when the adapter determines that it is connected to a switch, but the IOCDS specifies that is should be directly connected to a control unit or the contrary.

Note: The settings of each adapter determine whether the adapter status values are summarized as not operating or acceptable.

Apply acceptable status settings to all adapters
Select this to apply all the selected status settings.

Note: Only applies to adapters that share the same CPC.

Partitions

The Partitions section displays the Channel Path IDs (CHPIDs), Crypto, or FID depending on the type of adapter defined for the selected adapter for all partitions:

Partition Name
Displays the name of the partition for the targeted adapter.

Partition Status
Indicates the status of the partition for the targeted adapter.

CSS.CHPID/Crypto/FID
Displays all the CSS.CHPIDs, Cryptos, or FIDs associated with that physical channel identifier (PCHID). A CSS identifies which channel subsystems the CHPID belongs to.

The navigation pane also can include the following links to related tasks depending on the selected adapter type:

Advanced facilities
Opens the **Advanced facilities** task for the selected adapter.

Channel problem determination
Opens the **Channel problem determination** task for the selected adapter.

View adapter security
Opens the **View adapter security** window for some selected adapters.

Additional functions on this window include:

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Apply
To apply changes you made to the adapter's acceptable status settings, click **Apply**. The **Apply** button is not displayed in view-only mode.

Help
To display help for the current window, click **Help**.

Add or Change Object Definition

Accessing the Add Object Definition task

Notes:

- An object with a domain name that is different from the domain name of the Hardware Management Console will not communicate with the Hardware Management Console or appear on any of the Hardware Management Console windows.
- This task will not be successful if a mirroring operation is in progress.

This task enables you to define a system that is currently not defined and was automatically discovered by the Hardware Management Console. After a system is defined it becomes part of **Systems Management**. Each object must have a unique name and TCP/IP address.

To add an object to a defined group:

1. Select an undefined object from **Systems Management > Unmanaged Systems**.
2. Open the **Add Object Definition** task. The Add or Change Object window is displayed.
3. Select the Hardware Management settings required for this system.
4. Click **OK** to add the object to your group of defined objects.

   Note: The "Replace Object Confirmation" on page 383 window is displayed when a CPC is added to the HMC and the Object Definition Panel window is displayed which provides information on how the new system can be defined as a time source.

You can also use this task to provide the additional addressing information to configure Support Elements to remote Hardware Management Consoles. At the remote Hardware Management Console:

1. Select **Systems Management > Unmanaged Systems**.
2. Open the **Manual Add Object Definition** task. The Manual Add Object Definition window is displayed.
3. Specify the TCP/IP address in the **Addressing Information** field and click **OK**. The Hardware Management Console tries to contact the Support Element and exchange the remaining information necessary to complete the configuration process.

   Note: The Manual Add Object Definition window remains displayed with the last entered TCP/IP address until you have added the appropriate systems. When you have completed this task, click **Cancel**.
4. All objects that you added appear in **Systems Management**.

Accessing the Change Object Definition task

Note: The Alternate Support Element must be operational and not mirroring to allow change.

This task enables you to change the definition of any object that is defined. After the change is complete, the object's definition will be changed in all groups that contain the object. Each object must have a unique name and TCP/IP address.

To change a object:

1. Select a defined object from **Systems Management**.
2. Open the **Change Object Definition** task. The Add or Change Object window is displayed.
3. Make any necessary changes to the object, click **OK** to save the changes for the object.

Add or Change Object Definition

The **Add Object Definition** task defines a system that is currently part of the **Unmanaged Systems** group. Once a system is defined, it is removed from the **Unmanaged Systems** group and added to the **Systems Management** group.

Each object should have a unique name and TCP/IP address.

- A system must be defined to the Hardware Management Console before any other action can be taken on that system.
- An object with a domain name that is different from the domain name of the Hardware Management Console will not communicate with the Hardware Management Console or appear on any of the Hardware Management Console windows.

The **Change Object Definition** task changes the definition of any object that is defined. Once the change is complete, the object's definition will be changed in all groups that contain the object.

Network name
Displays the name of the network to which the system is connected through its Support Element.

System name
Displays the name of the currently defined system on the Hardware Management Console.

Hardware Management Console Setting for this System
Use this section to customize options that control how the Hardware Management Console and the system interact.

Act as a call-home server
Displays whether or not the system should use this Hardware Management Console as a call-home server. It is recommended that systems only use as call-home servers Hardware Management Consoles that are in reasonably close geographic proximity.

Report loss of communication
Displays whether or not this Hardware Management Console should report the loss of communication with the system as a problem. It is recommended that this option only be enabled for systems that are in reasonably close geographic proximity to the Hardware Management Console.

Product Information
This section displays product information about the system and the machine in which it is located.

A *machine* is a particular configuration of hardware designed to provide specific operational capabilities and characteristics. A machine includes at least one CPC in a frame, but can include one or more frames with one or two CPCs in each frame.

Machine serial
Displays the serial number of the machine.

System serial
Displays the serial number of the system.

System location
Displays the four character device location of the system. It identifies the system's frame and its location, in EIA units, within the frame.

OK
To save the settings currently displayed in this window, click **OK**.

Cancel
To close the window and exit the task without saving new changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Replace Object Confirmation

Use this window to verify whether or not the system you are adding or changing as a defined system replaces an existing machine.

You can choose one of the following:

Yes
If you select **Yes**, then a table is displayed listing the available defined system. Select a system and then select one of the following options from the drop-down menu:

Clone Information
If you select **Clone Information**, then the new or existing system being defined uses the definitions of the system you selected from this table. The new system is added to all the same user defined groups and assigned the same user defined roles and event monitors that the selected system resides in. Both systems exist with the same definitions.

Replace Information
If you select **Replace Information**, then the new system being defined replaces the system you selected from this table. The new or existing system is assigned to the user defined groups, user defined roles, and event monitors the selected system had been assigned to. The selected system no longer appears.

No
If you select **No**, then the selected system that you are adding or changing as a defined system does not replace an existing machine.

Additional information on the elements of this window includes:

System table
This table lists the available systems, identified by **System Name** and **System Serial Number**. The information used from one of the selected systems in this table can be copied or replaced with the system that is being added or changed.

OK
To proceed with your selection, click **OK**.

Cancel
To close window and exit the task without saving new changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add or Change Object

The **Add Object Definition** task defines a system that is currently part of the **Unmanaged Systems** group. Once a system is defined, it is removed from the **Unmanaged Systems** group and added to the **Systems Management** group.

Each object should have a unique name and TCP/IP address.

- A system must be defined to the Hardware Management Console before any other action can be taken on that system.
- An object with a domain name that is different from the domain name of the Hardware Management Console will not communicate with the Hardware Management Console or appear on any of the Hardware Management Console windows.

The **Change Object Definition** task changes the definition of any object that is defined. Once the change is complete, the object's definition will be changed in all groups that contain the object.

Network name
Displays the name of the network to which the system is connected through its Support Element.

System name
Displays the name of the currently defined system on the Hardware Management Console.

Hardware Management Console Setting for this System
Use this section to customize options that control how the Hardware Management Console and the system interact.

Act as a call-home server
Displays whether or not the system should use this Hardware Management Console as a call-home server. It is recommended that systems only use as call-home servers Hardware Management Consoles that are in reasonably close geographic proximity.

Report loss of communications
Displays whether or not this Hardware Management Console should report the loss of communication with the system as a problem. It is recommended that this option only be enabled for systems that are in reasonably close geographic proximity to the Hardware Management Console.

Product Information
This section displays product information about the system and the machine in which it is located.

A *machine* is a particular configuration of hardware designed to provide specific operational capabilities and characteristics. A machine includes at least one CPC in a frame, but can include one or more frames with one or two CPCs in each frame.

Machine serial
Displays the serial number of the machine.

System serial
Displays the serial number of the system.

System location
Displays the four character device location of the system. It identifies the system's frame and its location, in EIA units, within the frame.

OK
To save the settings currently displayed in this window, click **OK**.

Cancel
To close the window and exit the task without saving new changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Manual Add Object Definition

Use this window to confirm or cancel your request to manually identify and define a system in the domain of the Hardware Management Console.

A system must be identified for it to be represented by an object, referred to as a **system** under **Unmanaged Systems**. If the system is not identified automatically by the console, you must identify it manually. Afterwards you must define the undefined system so you can use the console to monitor and operate it.

Automatically identified systems

Ordinarily, the Hardware Management Console automatically identifies all systems in its domain and in the same Local Area Network (LAN).

All systems automatically identified by the console become objects in the **Unmanaged Systems** group. You do **not** need to manually identify a system if it is already represented by an object in the **Unmanaged Systems** group. You must only define the undefined system.

Click **Cancel** to end this task if an object already represents the undefined system you want to define. Then use the undefined system's object, rather than the **System Manual Definition**, to start the **Add Object Definition** task for defining it.

Manually identifying systems

You need to manually identify a system only if it is **not** already represented by an object in the **Unmanaged Systems** group. Such a system typically is not in the same LAN as the Hardware Management Console. You can manually identify the system if it is in the console's domain and if the system's network can use TCP/IP for network communications.

If the system you want to identify and define met that condition, click **OK** to continue this task.

Additional information on the elements of this window includes:

Addressing Information
Use this window to confirm or cancel your request to manually identify and define a system in the domain of the Hardware Management Console. Manually identify a system to the Hardware Management Console if the system is not in the same Local Area Network (LAN) as the console.

Specify the addressing information the Hardware Management Console requires for network communications with the system.

TCP/IP
Specify an IPv4 or IPv6 Transmission Control Protocol/Internet Protocol (TCP/IP) address of the system you want to define.

The IPv4 address is written as four decimal numbers, representing the four bytes of the IP address, separated by periods (for example, `9.60.12.123`). The IPv6 address can be written as eight groups of four hexadecimal digits, separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

Note: For IPv6 simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or you can use a double colon in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

OK
To confirm your request to manually identify and define a system, click **OK**.

Confirming your request displays a window you can use to manually identify the system to the Hardware Management Console by providing the information required for the console to communicate with the system.

Cancel
To cancel your request and exit the task without manually identifying or defining a system, click **Cancel**.

Help
To display help for the current window, click **Help**.

Advanced Facilities

Accessing the OSA Advanced Facilities task

The Open Systems Adapter (OSA) is an integrated hardware feature plug-in as a channel card, becoming an integral component of the I/O subsystem, enabling convenient Local Area Network (LAN) attachment. This brings the strengths of the architecture to the client/server environment: security, availability, enterprise-wide access to data, and systems management.

Note: Depending on your user task role, you may only be able to view this task.

You can use the Hardware Management Console to open a facility for monitoring, operating, and customizing an OSA channel.

To work with an OSA channel:

1. Select a CPC (server).
2. Open the **OSA Advanced Facilities** task. The OSA Advanced Facilities window is displayed.
3. The OSA Advanced Facilities window displays.

4. Use the OSA Advanced Facilities table and drop-down actions to launch OSA channel tasks.

OSA Advanced Facilities

The Open Systems Adapter (OSA) is an integrated hardware feature plug-in as a channel card, becoming an integral component of the I/O subsystem, enabling convenient Local Area Network (LAN) attachment. This brings the strengths of the architecture to the client/server environment: security, availability, enterprise-wide access to data, and systems management. Use this window to select the Open System Adapter (OSA) channel you want to work with.

The window lists all OSA channels for the Central Processor Complex (CPC).

PCHID
Displays the PCHID assigned to the OSA channels

Hardware Type
Displays the hardware types for the OSA channels

Status
Displays the status for the OSA channels

CHPID Type
Displays the CHPID type for the OSA channels

Code Level
Displays the machine code level for the OSA channels

Port 0 Status
Displays the Port 0 status for the OSA channels

Port 0 MAC Address
Displays the Media Access Control (MAC) Port 0 for the OSA channels

Port 1 Status
Displays the Port 1 status for the OSA channels

Port 1 MAC Address
Displays the Port 1 Media Access Control (MAC) Port 1 for the OSA channels.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Note: Most drop-down menu actions are not available when OSA channels are offline.

- “View port parameters” on page 387
- “Display OSA Address Table (OAT) Entries” on page 388
- “Export adapter diagnostic data” on page 387
- Card Trace/Log/Dump Facilities
- “Card Specific Advanced Facilities” on page 391
- Reset To Defaults

The icons perform the following functions in the PCI service partition table:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their

column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Close
To close the window and exit the task, click **Close.**

Help
To display help for the current window, click **Help**.

View port parameters

The view port parameters window displays various information about the selected port on the channel. This information (which varies based on channel hardware type and specified CHPID type) can contain current connection speed/mode, configured speed/mode, counter for various data items processed, as well as counters for various errors detected.

Additional functions on this window include:

Close
To close the current window, click **Close**.

Export to USB Flash Memory Drive
To export the selected channel port parameter data to a USB Flash Memory Drive, click **Export to USB Flash Memory Drive**.

Export to FTP Location
To export the selected channel port parameter data to an FTP location, click **Export to FTP Location**.

Help
To display help for the current window, click **Help**.

View port parameters

The view port parameters window displays information about the selected port on the channel.

Channel Path:
Identifies the channel path for the selected port on the channel.

LAN port type:
Identifies the LAN port type for the selected port on the channel.

Physical port identifier:
Enter the port identifier or use the drop-down arrow to select an existing port identifier.

Additional functions on this window include:

OK
To display details of the selected physical port identifier, click **OK**.

Cancel
To close the window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Export adapter diagnostic data

Use this window to export all the adapter diagnostic data for the OSA channels defined on the system. Verify the **User name** is the specific FTP destination. Use the **File path** field to type the fully qualified path destination.

The export function copies of a source file from the console to the FTP destination:

Host name
Specify the host computer of the FTP source.

User name
Specify the user name for the target FTP destination.

Password
Specify the password for the user ID.

Protocol
Select this option to enable a secure FTP connection to your server.

File path
Specify the fully qualified file path for the target file.

Additional functions on this window include:

Export
To export the OSA channel diagnostic data to an FTP location, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel**.

Help
To display help for the current window, click **Help**.

Display OSA Address Table (OAT) Entries

Use this window to configure the OSA for the OSE, OSD, or OSN defined channel type in TCP/IP Passthru, SNA modes, or both concurrently.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSE, OSD, or OSN defined channel type.

LAN port type
Identifies the type of network the selected OSE, OSD, or OSN defined channel type can be connected to through cable connections to its port or ports.

The Edit OSA Address Table (OAT) entries define

CSS
Displays the channel subsystem (CSS) for the selected OSE, OSD, or OSN defined channel type.

IID
Displays the logical partition ID assigned to the selected OSE, OSD, or OSN defined channel type.

Unit Address
Displays the unit address assigned to the selected OSE, OSD, or OSN defined channel type.

Device Number
Displays a unique number that is assigned for each device that was defined in the IOCDS for the OSE, OSD, or OSN defined channel type.

LPAR Name
Displays the name of the logical partition assigned to the OAT entry.

Port Number
Displays the number that uniquely identifies the port for the selected OSE, OSD, or OSN defined channel type.

Session Type
Displays one of the following active session types for the selected OSE, OSD, or OSN defined channel type:

- TCP/IP
- SNA

IP Address
Indicates the client's IP address for the selected OSE, OSD, or OSN defined channel type.

Isolated
Indicates if the OAT entries are in isolation mode.

Router Indicator
Indicates the router identifier.

The icons perform the following functions for the selected OSE, OSD, or OSN defined channel type in the Edit OAT Entries table:

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this downloaded CSV file into most spreadsheet applications.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Additional functions on this window include:

Save
To save the configuration values for selected OSA defined OCE channel type, click **Save**.

Cancel
To close the window without saving the current selected changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit OSA Address Table (OAT) Entries

Use the Edit OSA Address Table (OAT) Entry window to define which devices the OSA for the selected OSE defined channel type uses to transfer data and commands to/from each attached host. For a TCP/IP Passthru mode, an OSA transfers data between a host IP program, to which it is defined, and certain clients on the networks. For SNA mode, an OSA acts as a SNA passthru agent to the clients that use the SNA protocol on the LAN that is directly attached to the OSA.

Port Number
Use the drop down box to select or type the port number for the selected OSE defined channel type.

CSS
Use the drop down box to select or type the channel subsystem (CSS) for the selected OSE defined channel type.

Image Number
Use the drop down box to select or type the logical partition number of the LPAR for the selected OSE defined channel type.

Unit Address
Use the drop down box to select or type the address for the selected port for the OSE defined channel type..

Default entry indicator
Select Primary for one of the LPARs using the selected OSA port for the OSE defined channel type. The LPAR designated as the Primary receives any datagrams that are not specifically addressed to any of the home IP addresses associated with the selected OSA port.

Home IP address
Enter the TCP/IP Home IP addresses for the selected OSE defined channel type.

Additional functions on this window include:

OK
To save the new values, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Advanced Facilities

Use this window to select a function to monitor, operate, or customize a selected channel type for the system. The list of actions you can take from the list depends on the channel type selected. The list may include:

- Force error recovery log
- Card display or alter memory...
- View code level
- Card trace/log/dump facilities
- “Card Specific Advanced Facilities” on page 391
- Look up generic access...
- Reset to defaults...

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Force log

Use this window to select a force log function for the selected Integrated Coupling Adapter (ICA) SR channel type in the system.

Channel ID:
Displays a four-digit physical channel identifier (PCHID) of the selected Integrated Coupling Adapter (ICA) defined channel type.

Channel type:
Identifies specific channel type

Card description:
Displays the card description for the channel type.

Select a force log function for the selected Integrated Coupling Adapter channel type:

- Force adapter error recover log
- Force port error recover log
- Force channel error recover log
- Force adapter log
- Force channel log

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Card Specific Advanced Facilities

Use this window to select a card specific function for a selected channel type for the system. The list of card specific facilities actions you can take from the list depends on the channel type selected. The list may include:

- Query port status...
- Display or alter MAC address...
- Enable or disable ports...
- Run port diagnostics
- Set card mode...
- Display client connections...
- Display active sessions configuration...
- Display active server configuration...
- Panel configuration options...
- Manual configuration options...
- Activate configuration
- Display activate configuration errors...
- Debug utilities...
- Manage security certificates...

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Query port status

Displays the local area network (LAN) port record of each LAN port on the selected Open Systems Adapter (OSA)-Express® channel.

A LAN port record:

- Displays the port identifier
- Indicates whether the port is enabled or disabled
- Indicates whether the port is in Support Element control mode
- Indicates the source of the command that disabled the port if the port becomes disabled while it is not in Support Element control mode.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Query port table

First line list column:

Port ID
Displays the number that uniquely identifies the port on the OSA-Express card.

Type
Identifies the type of LAN supported by the port.

Port state
Indicates the current state of the port.

Disabled
Indicates if the port was disabled by the Support Element.

External disabled
Indicates if the port was disabled by an external LAN request.

Host program disabled
Indicates if the port was disabled by a host support program.

Second line list column:

Port ID
Displays the number that uniquely identifies the port on the OSA-Express card.

Support Element Control Mode
Indicates if the port accepts commands only from its Support Element.

Port Configuration Change
Indicates if the port has changed configuration.

Port Failure
Indicates if a licensed internal code problem has occurred which stops the port from being enabled.

Link Threshold Exceeded
Indicates if the port has been disabled because the number of link failures has exceeded the threshold.

Link Monitor
Describes why the port is in Link Monitor State. This is a bit field. The bits are numbered from left (bit 0) to right (bit 15).

- Bit 0: *loss of signal* - most likely cause is an improperly installed or broken cable. Please check your connection or cable.
- Bit 1: *not used*.
- Bit 2: *registration failure* - registration was rejected by ATM switch or the switch is not operational. This is most likely the result of the configuration not matching the configuration of the LES. Fix the configuration and make sure that the required switch is operational.
- Bit 3: *loss of SAAL connection* - this is set when there is a problem with the communication to the switch. Have your network person check the switch connection.
- Bit 4-15: *Reserved*

Definition Error Code
Describes why the port is in Definition Error State.

- "00" - Unspecified Error
- "01" - Invalid Type
- "02" - Invalid Parameter

Additional functions on this window include:

OK
To close the window when you finish reviewing the LAN port records, click **OK**.

Help
To display help for the current window, click **Help**.

Query port status

Displays the local area network (LAN) port record of each LAN port on the selected Open Systems Adapter (OSA)-Express channel.

A LAN port record:

- Displays the port identifier
- Indicates whether the port is enabled or disabled
- Indicates whether the port is in Support Element control mode
- Indicates the source of the command that disabled the port if the port becomes disabled while it is not in Support Element control mode.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Query port status table

Port Identifier
Displays the number that uniquely identifies the port on the OSA-Express card.

Type
Identifies the type of LAN supported by the port.

Port State
Indicates the current state of the port.

Disable
Indicates if the port was disabled by the Support Element.

Support Element Control Mode
Indicates if the port accepts commands only from its Support Element.

Port Block
Indicates the port was disabled by a LAN request.

External Disabled
Indicates if the port was disabled by an external LAN request.

Internal Port Failure
Indicates if a licensed internal code problem has occurred which stops the port from being enabled.

Additional functions on this window include:

OK
To close the window when you finish reviewing the LAN port records, click **OK**.

Help
To display help for the current window, click **Help**.

View port parameters

The view port parameters window displays various information about the selected port on the channel. This information (which varies based on channel hardware type and specified CHPID type) can contain state, current connection speed/mode, configured speed/mode, counter for various data items processed, as well as counters for various errors detected.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected zHyperLink or RoCE Express2 channel.

Port
Identify the physical port of the selected zHyperLink or RoCE Express2 channel.

Additional functions on this window include:

Close
To close the current window, click **Close**.

Export to USB Device
To export the selected channel port parameter data to a USB Device, click **Export to USB Device**.

Export to FTP Server
To export the selected channel port parameter data to an FTP Server, click **Export to FTP Server**.

Help
To display help for the current window, click **Help**.

Display or alter MAC address

Displays the medium access control (MAC) addresses of the ports on the selected Open Systems Adapter (OSA)-Express channel.

You can also use the window to change one or more MAC addresses.

Note: This window might only allow view only for some user task roles.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

MAC address LAN port *n*
Initially displays the current medium access control (MAC) address of port number *n*. Each field in the group displays the hexadecimal value of one byte in the 6-byte (48-bit) MAC address of the port. The leftmost field displays byte 0; the rightmost field displays byte 5.

Use the fields to change the MAC address of the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Retrieve Universal MAC
To display the universally administered medium access control (MAC) address of each port, click **Retrieve Universal MAC**.

Note: This only displays each port's universal MAC address in its **MAC address LAN port *n*** field.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Enable or disable port

Use this window to enable or disable the local area network (LAN) ports for the selected Open Systems Adapter (OSA)-Express channel and to set the Support Element control mode of the port.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Attention: Make sure the port is not being used by other partitions before it is disabled.

Port number
Identify the port of the selected Open Systems Adapter (OSA)-Express channel.

Port status commend

Enable port
Enable a port to allow it to communicate with other devices attached to the LAN. An enabled port can receive information from other devices attached to the LAN, and can send information to them.

Disable port
Disable a port to prevent it from communicating with other devices attached to the LAN.

Support Element control code command

Set control on
Set the Support Element control mode of a port on.

Set control off
Set the Support Element control mode of a port off.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Run port diagnostics

Use this window to test the hardware of local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express, IBM zHyperLink Express (zHyperLink), and RoCE Express2 channels.

Attention: A diagnostic test cannot be stopped once it has started.

When testing is complete, a message displays to indicate whether the test completed with errors or without errors. In either case, the tested port is displayed to show the results of the testing.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express, zHyperLink, or RoCE Express2 channel.

LAN port type
Identifies the type of network the selected OSA-Express, zHyperLink, or RoCE Express2 channel can be connected to through cable connections to its port or ports.

Physical Port Identifier
Identify the physical port of the selected OSA-Express, zHyperLink, or RoCE Express2 channel.

Diagnostic type

Select the type of test you want to perform:

Normal
Test port hardware that supports the internal operation of the specified port.

- The port must be disabled.
- All PCHIDs must be configured off.

Wrap plug test
Test port hardware that supports the external connection of the specified port to a local area network (LAN).

- The port must be disabled.
- A wrap plug must be installed on the port. Identify the part number of the correct wrap plug for each type of OSA-Express, zHyperLink, and RoCE Express2 port.

- All FIDs must be configured off.

Optical Power Measurement
Test port hardware that supports fiber optics of the specified port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Run port diagnostics

Use this window to view the sense data set during diagnostic testing of an Open Systems Adapter (OSA)-Express port.

The sense data indicates the results of running diagnostics.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Sense data

LAN port status word 0 displays the hexadecimal values of sense data bytes 0, 1, 2, and 3.

LAN port status word 1 displays the hexadecimal value of sense data bytes 4, 5, 6, and 7.

LAN port status word 2 displays the hexadecimal values of sense data bytes 8, 9, 10, and 11.

LAN port status word 3 displays the hexadecimal values of sense data bytes 12, 13, 14, and 15.

LAN port status word 4 displays the hexadecimal values of sense data bytes 16, 17, 18, and 19.

LAN port status word 5 displays the hexadecimal values of sense data bytes 20, 21, 22, and 23.

LAN port status word 6 displays the hexadecimal values of sense data bytes 24, 25, 26, and 27.

LAN port status word 7 displays the hexadecimal values of sense data bytes 28, 29, 30, and 31.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission mode of local area network (LAN) ports.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical port identifier
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode

Select the transmission mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Full duplex
Enable sending and receiving data transmissions at the same time.

Half duplex
Enable sending and receiving data transmissions, but not at the same time.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission speed and mode of local area network (LAN) ports.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical port identifier
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode/speed

Select the transmission speed and mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Auto Negotiate
Set the port at the current network speed.

Mode/Speed
Set the transmission speed and mode you want for the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission speed and mode of local area network (LAN) ports.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode/speed

Select the transmission speed and mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Auto Sense
Set the port at the current network speed.

Speed/Mode
Set the transmission speed and mode you want for the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Display client connections

Use this window to display Network Interface Card information for the selected Open Systems Adapter (OSA)-Express channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client connections table

Session Index
Displays the session numbers for the selected OSA-Express channel. A valid range for the session numbers is 0 to 120.

Status
Displays one of the following client session connections for the selected OSA-Express channel:

- **Ready** - Indicates the session has been configured and the client can be connected.
- **Active** - Indicates the session has been configured and the client is connected.
- **Not configured** - Indicates the session has not yet been configured.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Connected** - Indicates the session has been configured and the client is connected to it.

- **DHD Pending** - Indicates the client has been disconnected. However, since DHD was enabled, OSA-ICC has not notified the host operating system.

MAC
Displays the media address control (MAC) address of the client that is being connected. A MAC address identifies a port as a destination and source of information it receives and transmits, respectively, on the local area network (LAN).

Client IP
Indicates the client's IP address.

Port
Indicates the number that identifies the port for the client connection.

Socket Number
Displays the TCP socket number that uniquely defines the connection.

LT Index
Displays the index in the LT table. A valid range for the LT index is 0 to 119.

Connect Rule
Indicates one of the following connect rules:

- IP only
- LU only
- IP and LU
- Unknown

Disable Logo
Displays the OSA-ICC logo that appears when the session is first connected.

Additional functions on this window include:

OK
To close the current window, click **OK**.

Help
To display help for the current window, click **Help**.

Panel configuration options

Use this window to determine if you can select a configuration option for the selected Open Systems Adapter (OSA)-Express channel to validate the session configuration or view the validate error.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Configuration file options

Edit OAT entries
To open a window to configure OSA Address Table (OAT) entries for the selected OSA defined OSE channel type.

Edit SNA timers
To open a window to configure SNA timer values for the selected OSA defined OSE channel type.

Validate panel values
To open a window to validate panel values for a session configuration for the selected Open Systems Adapter (OSA)-Express channel.

Display validate panel errors
To open a window to display validate panel errors, if any exist.

Note: After the values have been validated, select the Activate configuration option on the Advanced Facilities window to active them or your current changes are lost.

Additional functions on this window include:

OK
To apply the selected options, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit SNA timers

Use this window select or enter SNA timer values to configure the OSA for the selected OSE defined channel type.

Port Number
Indicate the port number the SNA timers are associated with the selected OSE defined channel type.

Inactivity Timer/Ti (ms)
Use the drop down box to select or type the inactivity timer to be initialized for the selected OSE defined channel type. If the Ti timer is enabled, you can set its timeout value in increments of 0.12 seconds from 0.24 to 90.00 second. An enabled inactivity timer (ti) periodically tests the viability of the network media. The timer setting applies to all the clients on the target LAN, not to individual clients. The timer interval indicates how quickly a failure of the network media can be detected when the connection is quiescent.

Response timer/T1 (ms)
Use the drop down box to select or type the response timer for the selected OSE defined channel type. The T1 timer clocks link events that require responses from clients on the network. T1 can be set to a timeout value from 0.20 up to 51.00 seconds in increments of 0.20 seconds. Set the T1 timer to a value not less than the average round-trip transit time from the OSA to the clients and back.

Acknowledgment timer/T2 (ms)
Use the drop down box to select or type the acknowledgment timer for the selected OSE defined channel type. An OSA starts the T2 timer when it receives an I-format LPDU and stops when it sends an acknowledgment. An acknowledgment is sent either when an outgoing I frame is sent or when N3 number of I-format link protocol data units (LPDUs) has been received. Set a value from 0.08 seconds up to 20.40 seconds in increments of 0.08 seconds.

Maximum Frames Before Transmit Window/N3
Use the drop down box to select or type the maximum frames before transmit window for the selected OSE defined channel type. When determining the maximum I-frames that can be sent before an acknowledgment is sent (N3 count) and the maximum number of outstanding I-format link protocol data units (LPDUs) (TW count), consider the N3 and TW counts that are set at the clients as well.

Maximum Transmit Window/TW
Use the drop down box to select or type the maximum transmit window for the selected OSE defined channel type. The TW count allows the sender to transmit before that sender is forced to halt and wait for an acknowledgment. The TW count can be set as an integer from 1-16.

Additional functions on this window include:

OK
To save the new values, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit/display sessions configuration

Use this window to display or allow you to select a configuration edit session for the selected Open Systems Adapter (OSA)-Express channel. The window displays information that can be configured for the selected OSA-Express channel edit session configuration.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Edit/display sessions configuration table

Session index
Displays the session index number for the selected OSA-Express channel.

State
Displays one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS
Displays the channel subsystem (CSS). A valid range for the CSS is 0 to 3.

MIFID
Displays the logical partition ID. A valid range for the Image ID is 1 to F.

Device Number
Displays a unique number that is assigned for each device that was defined in the IOCDS.

LU Name (3270 OSC OSA channels only)
Indicates what active session you are connecting to. The LU name defines a group pool of devices.

Client IP
Indicate the IP address that a client will use to connect to the session. The client IP address can remain 0.0.0.0 or empty in order to allow any client to connect to a specific session. If a nonzero IP is specified, any client with a nonmatching IP will be rejected.

IP Filter
Displays the IP Filter address that is used for routing to specific subnets.

Session Type (3270 OSC OSA channels only)
Displays one of the following active session types for the selected OSA-Express channel:

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect (DHD) (3270 OSC OSA channels only)
Displays the defer host disconnect (DHD) time for the active session configuration to wait until the session instructs the host it has disconnected. The defer host disconnect can be:

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Response mode (RSP) (3270 OSC OSA channels only)
Displays the response mode (RSP) for the active session configuration. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgment.

Read Timeout (RTO) (3270 OSC OSA channels only)
Displays the read timeout (RT0) for the active session configuration to wait (in seconds) for a response from the client before performing a client disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Additional functions on this window include:

OK
To close the window when you finish reviewing the sessions, click **OK.**

Save
To save edit session data, click **Save**.

Change
To change edit session data, select a line and click **Change**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window.

Edit sessions configuration

Use this window to select a configuration session for the selected Open Systems Adapter (OSA)-Express channel. The window displays information that can be configured for the selected OSA-Express channel session configuration.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Edit sessions configuration table

Session Index
Display the session index number for the selected OSA-Express channel.

State
Display one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS Value
Display the channel subsystem (CSS). A valid range for the CSS is 0 to 3.

MIFID
Display the logical partition ID. A valid range for the Image ID is 1 to F.

Device Number
Display a unique number that is assigned for each device that was defined in the IOCDS.

LU Name
Indicate what active session you are connecting to. The LU name defines a group pool of devices.

Client's IP
Indicate the IP address that a client will use to connect to the session. The client's IP address can remain 0.0.0.0 or empty in order to allow any client to connect to a specific session. If a nonzero IP is specified, any client with a nonmatching IP will be rejected.

IP Filter
Display the IP Filter address that is used for routing to specific subnets.

Session Type
Display one of the following active session types for the selected OSA-Express channel:

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect (DHD)
Display the defer host disconnect (DHD) time for the active session configuration to wait until the session instructs the host it has disconnected. The defer host disconnect can be:

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Response mode (RSP)
Display the response mode (RSP) for the active session configuration. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgment.

Read Timeout (RTO)
Display the read timeout (RT0) for the active session configuration to wait (in seconds) for a response from the client before performing a client disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Additional functions on this window include:

Save
To save session data, click **Save**.

Change
To change session data, select a line and click **Change**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit session configuration

Use this window to change a configuration session for the selected Open Systems Adapter (OSA)-Express channel.

Channel ID
Display a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identify the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Session Index
Display the session number for the selected OSA-Express channel.

Session State
Display one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Active** - Indicates the session has been configured and the client is connected.
- **Connected** - Indicates the session has been configured and the client is connected to it.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS Value
Use the drop down box to select or type the channel subsystem (CSS) value for the session configuration of the selected Open System Adapter (OSA)-Express channel. A valid range for the CSS is 0 to 3.

MIFID
Use the drop down box to select or type the logical partition ID for the session configuration of the selected Open Systems Adapter (OSA)-Express channel.

Device Number
Use the drop down box to select or type the unique number for each device for the session configuration of the selected Open System Adapter (OSA)-Express channel.

LU Name
Enter the session you are connecting to for the selected Open Systems Adapter (OSA)-Express channel. The LU name defines a group pool of devices.

Client's IP address
Enter the client's IP address for the selected OSC channel. This entry field is optional.

IP Filter
Enter the IP filter address that is used for routing to specific subnets.

Session Type
Select one of the following choices to indicate the session type for the selected Open Systems Adapter (OSA)-Express channel.

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect
Select a one of the following to indicate the type of defer host disconnect (DHD) you want the session configuration to wait before instructing the host to disconnect.

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Defer host disconnect time value (seconds)
Enter your own defer host disconnect (DHD) time value in seconds that you want to specify for the session to wait before instructing the host to disconnect.

Response mode
Select a response (RSP) mode choice for the host to wait for the client to respond to the last packet of data. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgement.

Read Timeout
Select a choice to indicate the read timeout (RTO) for a response (in seconds) from the client before instruction the host to perform a disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Read timeout value
Enter your own read timeout (RTO) response (in seconds) value you want to specify for the session to wait before instructing the host to disconnect.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Delete Session
To delete the currently selected sessions configuration, click **Delete Session**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Display/Edit server configuration

Use this window to enter server configuration information for selected channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port 0/1

You can edit the server configuration information for the selected channel. To define a physical port, valid parameter values must be entered as displayed on the ranges adjacent to the parameter field. If a physical port is not defined, the IP address, Gateway, and TCP Port must all be set to 0 and the Prefix must be set to 1.

Note: By default all physical port parameters are set to 0. If the default value of 0 is not present in the IP address, Gateway, and TCP Port and 1 is not present in the in the Prefix physical port fields, that physical port is considered defined.

Server name
Enter the server name that the client is connected to for the selected Open Systems Adapter (OSA)-Express channel.

Enable IPv4
Check this box to enable IPv4

Host IPv4 address
Enter the host IP4v address for the active server configuration

Prefix
Enter the prefix of the IPv4 address for the active server configuration

IPv4 TCP port
Enter the IPv4 TCP port identifier for the active server configuration

IPv4 secure TCP port
Enter the IPv4 secure TCP port identifier for the active server configuration

Enable IPv6
Check this box to enable IPv6

Address type
Use this pull down to select the address for this IPv6 address

Host IPv6 address
Enter the host IPv6 address for the active server configuration

Prefix
Enter the prefix of the IPV6 address

IPv6 TCP port
Enter the IPv6 TCP port identifier for the active server configuration

IPv6 secure TCP port
Enter the IPv6 secure TCP port identifier for the active server configuration.

MTU size
Enter the maximum transfer (MTU) size to be transferred in one frame. A valid range is from 256 to 1492.

TLS version
Use this pull down to select the TLS version

- Select TLS 1.0 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.0, TLS 1.1, and TLS 1.2
- Select TLS 1.1 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.1 and TLS 1.2
- Select TLS 1.2 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.2 .

IPv4 default Gateway
Enter the IPv4 default gateway. The IPv4 default gateway is the network that connects the hosts

IPv6 default Gateway
Enter the IPv6 default gateway. The IPv6 default gateway is the network that connects the hosts.

Additional functions on this window include:

OK
To apply the changes displayed in the fields, click **OK**.

Close
To close the window without saving the current selected changes, click **Close**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Display/Edit server configuration

Use this window to enter server configuration information for selected channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port 0/1

You can edit the server configuration information for the selected channel. To define a physical port, valid parameter values must be entered as displayed on the ranges adjacent to the parameter field. If a physical port is not defined, the IP address, Gateway, and TCP Port must all be set to 0.

Note: By default all physical port parameters are set to 0. If the default value of 0 is not present in the IP address, Gateway, Subnet Mask, and TCP Port physical port fields, that physical port is considered defined.

Server name
Enter the server name that the client is connected to for the selected Open Systems Adapter (OSA)-Express channel.

Host IP address
Enter the host IP address for the active server configuration.

TCP port
Enter the TCP port identifier for the active server configuration.

Secure TCP port
Enter the secure TCP port identifier for the active server configuration.

Subnet Mask
Enter the subnet mask. The subnet mask identifies the TCP/IP protocol that is used for routing to specific subnets.

Default Gateway
Enter the default gateway. The default gateway is the network that connects the hosts.

MTU Size(B)
Enter the maximum transfer unit (MTU) size to be transferred in one frame. A valid range is from 256 to 1492.

Frame types

Select a choice to indicate the Ethernet standards that you want the network to follow. Every host in a network must have the same frame type.

DIX
Select the DIX frame type for the session configuration. It is **strongly recommended** that you use DIX as your frame type.

SNAP
Select the SNAP frame type for the session configuration.

Note: The recommended frame type for OSA-ICC is DIX. Changing the frame type to another mode without checking with your Network Administrator could cause a loss of data.

Additional functions on this window include:

OK
To apply the changes displayed in the fields, click **OK**.

Close
To close the window without saving the current selected changes, click **Close**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Manual configuration options

Use this window to select the manual configuration option for the session configuration of the selected Open Systems Adapter (OSA)-Express channel. You can export a session source file to a media source, then edit the file on your workstation with an editor. After you have completed editing your file, import the session source file back on the Support Element using the import source file choice.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Configuration file options

Import source file
Import a session configuration file that was exported to a diskette for editing.

Note: In order to make the imported edited source file the active configuration, you must *Validate source file* and then *Activate configuration*.

Insert the media source containing the source file into your disk drive, then highlight the file you would like to import and click **OK**.

Export source file
Export a session configuration file to a media source to edit with your workstation editor. You can also use this panel to export your configuration file as a backup.

Insert the media source containing the source file into your disk drive, then type the name to be given to the exported configuration file in the field and click **OK**.

Import source file by FTP
Import a session configuration file from a designated FTP site.

Export source file by FTP
Export a session configuration file to a designated FTP site.

Load default source file
To load the default source file.

Edit source file
Edit the session source configuration file.

Validate source file
Validate the session source configuration file to ensure that the file is valid before activating it. **Attention:** In order to make the validated source file the active configuration, you must activate it. Activating a configuration makes any changes you made effective immediately. This could result in active sessions being dropped.

If the source file you are validating is incorrect, the errors and warnings will be commented in the source file. You must fix any errors before activating your configuration. When the validate is successful, you will receive a message stating that your source file is successful, then click **OK**.

Note: After the source file has been validated, select the Activate configuration option on the Advanced Facilities window to active them or your current changes are lost.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Import Source File

Select **Import Source File** to copy a configuration source file from one medium to the Support Element.

The import function copies a source file from the FTP destination to the Support Element hard disk.

Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import data configuration files from a FTP destination, click **Import**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Source File

Select **Export Source File** to export a configuration source file from the Support Element hard disk to an FTP destination.

The export function copies a source file from the Support Element to an FTP destination.

Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the file path and the file name of the data file that is to be saved.

Additional functions on this window include:

Export
To export configuration data files to an FTP destination, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Debug utilities

Use this window to select a debug option for the selected Open Systems Adapter (OSA)-Express channel. This window identifies the channel ID and LAN port type of the selected OSA-Express channel.

Ping utility
Select the ping utility to ping an active session to verify the status of the connection.

Trace route utility
Select the trace route utility to trace the route of a packet of data to a session.

Drop session
Select drop session to enter the session number to drop for the ping utility to identify.

Logo controls
Select the logo controls to enter the operating system session number to enable or disable a three line logo screen.

Query command
Select the query command to enter a command to the OSC channel for information.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Ping utility

Use this to open a window to ping an active session to verify the status of the connection.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client IP address
Indicate the client's IP address.

Length (in bytes)

Use this entry field to indicate the ping custom length of 8 to 32000 bytes.

Default (256)
Use the length default value. The default length value is 256 bytes.

Custom length
Set your own custom length of 8 to 32000 bytes.

Count

Use this entry field to indicate a custom count for the ping between 1 and 10.

Default (1)
Use the count default value. The default count value is 1.

Custom count
Set a custom count for the ping between 1 and 10.

Timeout (in seconds)

Use this entry field to indicate you own ping custom timeout value.

Default (1)
Use the timeout default value. The default timeout value is 10.

Custom timeout
Set your own custom timeout value between 1 and 30.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Trace route utility

Opens a window to trace the route of a packet of data to a session.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client IP address
Indicate the client's IP address.

MAX TTL

Use to select the trace route maximum time to live (TTL) for the packet that is being sent.

Default(30)
Use the MAX TTL default value. The default MAX TTL value is 30.

Custom MAX TTL
Set a custom MAX TTL.

Attempts

Use to select the attempts value for the trace route.

Default(3)
Use the attempts default value. The default attempts value is 3.

Custom attempts
Set a custom attempts value of between 1 and 20.

Port

Use to select the trace route port value you want set for the trace route.

Default(4096)
Use the port default value. The default port value is 4096.

Custom port
Set a custom port identifier between 2048 and 60000.

Wait time in seconds

Default(5)
Use the wait time default value. The default wait time value is 5 seconds.

Custom wait time
Set a custom wait time value of between 1 and 255.

Extra debug messages

No
Do not display extra debug messages.

Yes
Display the extra debug messages.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Drop session

Use the entry field to identify what session index number to drop.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Session index
Identify what session index number to drop.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To stop the command currently being processed by the selected channel, click **Cancel.**

Help
To display help for the current window, click **Help**.

Logo controls

Use this window to enter the operating system session index for the selected OSA-Express channel when enabling or disabling a three line logo screen for the operating system screen.

Enable Logo
Clear the operating system screen and display a three line logo screen for the operating system session index entered.

Disable Logo
Do not display a three line logo screen for the operating system session index entered.

Additional functions on this window include:

OK
To close the window after making changes, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Query command

Use this window to enter a query command to request information from the channel. The query command can be up to 50 alpha-numeric ASCII characters.

Note: This command should be used only under the guidance of service support.

Additional functions on this window include:

OK
To continue with the query command operation, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Manage security certificate

Use this window to manage Secure Socket Layer (SSL) certificates. Select an action and location to manage the security certificates.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

OSA-ICC certificate scope
Displays the current OSA-ICC certificate scope that is used for this physical channel identifier (PCHID). Click **Change** to select a different certificate scope action for the selected PCHID.

OSA-ICC certificate type
Displays the OSA-ICC certificate type of this physical channel identifier (PCHID)

OSA-ICC certificate expiration
Displays the OSA-ICC certificate expiration of this physical channel identifier (PCHID).

Actions

- Select **Export self-signed certificate** to generate a self-signed certificate and store in the configuration file to export via USB drive or FTP site
- Select **Reload self-signed certificate** to install the self-signed certificate
- Select **Regenerate OSA-ICC key and self-signed certificate** to regenerate the self-signed certificate
- Select **Create certificate signing request** to generate a certificate signing request and store in the configuration file to export via USB drive or FTP site
- Select **Import signed certificate** to import and install a file via USB drive or FTP site
- Select **View certificate** to view the certificate that is currently being used
- Select **Edit certificate** to edit the certificate signing request (CSR) attributes.

Location

- Select **USB drive** to export or import the selected action
- Select **FTP site** to export or import the selected action.

Additional functions on this window include:

Apply
To save the new values, click **Apply**.

Change
To change the OSA-ICC certificate scope, click **Change**.

Close
To close the window without saving the current selected changes, click **Close.**

Help
To display help for the current window, click **Help**.

Edit Certificate

Use this window to provide the necessary information to create a new certificate or to modify the values of the existing certificate.

Common name
Specify the common name for the certificate

Organization
Optionally, specify the name of the corporation, limited partnership, university, or government agency

Organization unit
Optionally, specify the organization name, which differentiates between divisions within an organization (for example, Hardware Development or Human Resources)

Country or region
Optionally, select or specify the two-character ISO format country code for your country (for example, a two-character code of GB for Great Britain or US for the United States).

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the list.

State or province
Optionally, select or specify the state or province name.

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the list

Locality
Optionally, specify the city or locality name

Valid until
Specify the ending date that the certificate can be valid until, beginning from the time the certificate is created or modified

DNS name
Optionally, add DNS names to the list of valid entries for the certificate

IP Address
Optionally, add IPv4 and IPv6 addresses to the list. The IPv4 address must be specified as 4 decimal numbers separated by a period (for example, dd.ddd.ddd.ddd). The IPv6 address can be specified in several different ways with one form being 8 hexadecimal numbers separated by a colon (for example, xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Email address
Optionally, add email addresses to the list.

Additional functions on this window include:

Save
To save the new values, click **Save**.

Next
To proceed to the next window, click **Next**.

Cancel
To close the window without saving the new values, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Certificate Signing Request

Use this window to select an export method for the certificate signing request.

Export to FTP
To export to an FTP location, select **Export to FTP**

Export to USB
To export to a USB media, select **Export to USB**

Note: This option is not available remotely.

Export to file system
To export to a local file system, select **Export to file system**

Note: This option is only available remotely.

Additional functions on this window include:

Export
To continue with the selected export method, click **Export**.

Back
To go back to the previous window, click **Back**.

Help
To display help for the current window, click **Help**.

Change OSA-ICC Certificate Scope

Select the certificate scope action that will apply for the PCHID:

Use the shared certificate for this PCHID
Select **Use the shared certificate for this PCHID** to use the shared certificate for this physical channel identifier (PCHID)

Use an individual certificate for this PCHID
Select **Use an individual certificate for this PCHID** to use an individual certificate for this physical channel identifier (PCHID).

Additional functions on this window include:

OK
To save the new values, click **OK**.

Change Certificate Scope
To change the certificate scope, click **Change Certificate Scope**.

Cancel
To close the window without saving the current selected changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Import Source File

Select **Import Source File** to copy a configuration source file from one medium to the Support Element.

The import function copies a source file from the FTP destination to the Support Element hard disk.

Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import data configuration files to an FTP destination, click **Import**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Source File

Select **Export Source File** to export a configuration source file from the Support Element hard disk to an FTP destination.

The export function copies a source file from the Support Element to an FTP destination.

Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the file path and the file name of the data file that is to be saved.

Additional functions on this window include:

Export
To export configuration data files to an FTP destination, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Alternate Support Element

Accessing the Alternate Support Element task

Notes:

- Each CPC must be a model that has both a primary and alternate Support Element installed.
- The primary Support Element is scheduled for automatic mirroring by default at 10 a.m. with a one-hour window for starting the operation. A record is added to the Support Element's event log to indicate the outcome of the operation.

This task performs any of the following actions for the selected CPC:

- Mirror data from the primary Support Element to the alternate Support Element
- Switch from the primary Support Element to the alternate Support Element
- Query whether a switch between Support Elements can take place.

Accessing the mirroring the primary Support Element data to the alternate Support Element option

Mirroring Support Element data copies the data from a CPC's primary Support Element to its alternate Support Element. By regularly mirroring primary Support Element data, you help ensure the alternate Support Element will function the same as the primary Support Element in case you need to switch the

alternate Support Element to become the primary Support Element (for example, because of a hardware failure on the existing primary Support Element).

Ordinarily, Support Element data is mirrored automatically each day at 10:00 a.m., but you can use this task to mirror Support Element data immediately, at any time, and for any reason. The following are examples of when you would want to mirror Support Element data instead of waiting for the automatic mirroring default times:

- Licensed internal code changes
- Input/output configuration data set (IOCDS) changes
- Hardware configuration definition (HCD) changes
- Dynamic I/O changes
- Dynamic load address and parameter changes
- LPAR data
- Profile changes
- Lockout disruptive tasks
- Scheduled operations
- Creating, changing, or deleting groups
- Automatic activation.

To mirror the primary Support Element data:

1. Select one or more CPCs (servers).
2. Open the **Alternate Support Element** task. The Alternate Support Element window is displayed.
3. Select **Mirror the Primary Support Element data to the Alternate Support Element**.
4. Click **OK** to begin mirroring.

Accessing the switching to the alternate Support Element option

Do this when you need to switch the alternate Support Element to become the primary Support Element. When a manual switchover is started, the system checks that all internal code level information is the same on both Support Elements and that the CPC is activated. If the switch can be made concurrently, the necessary files are passed between the Support Elements, and the new primary Support Element is rebooted. If a disruptive switch is necessary, the CPC will be powered off before completing the switch. The following are several conditions that will prevent a switchover:

- Mirroring task in progress
- Internal code update
- Hard disk restore
- Engineering change
- Concurrent upgrade engineering changes preload condition.

The system automatically attempts a switchover for the following conditions:

- Primary Support Element has a serious hardware problem
- Primary Support Element detects a CPC status check
- Alternate Support Element detects a loss of communications to the primary over both the service network and the customer's LAN.

To switch to the alternate Support Element from the Alternate Support Element window:

1. Select one or more CPCs (servers).
2. Open the **Alternate Support Element** task. The Alternate Support Element window is displayed.
3. Select **Switch the Primary Support Element and the Alternate Support Element**.
4. Click **OK** to switch to the alternate Support Element.

5. A confirmation window is displayed.

Accessing the querying switch capabilities between Support Elements option

The querying switch capability provides a quick check of the communication path between the Support Elements, the status of the Support Elements, and the status of the automatic switch action. You may want to perform this action before attempting to switch to the alternate Support Element.

To query switch capabilities from the Alternate Support Element window:

1. Select one or more CPCs (servers).
2. Open the **Alternate Support Element** task. The Alternate Support Element window is displayed.
3. Select **Query Switch capabilities**.
4. Click **OK** to start the query.
5. A confirmation window is displayed.

Alternate Support Element

Use this window to confirm or cancel your request to mirror Support Element data for the selected central processor complex (CPC), switch the Primary Support Element data to the Alternate Support Element, or query the switch capabilities.

Mirror the Primary Support Element data to the Alternate Support Element

Mirroring Support Element data copies it from a CPC's Primary Support Element to its Alternate Support Element. By regularly mirroring Support Element data, you help ensure the Alternate Support Element will look and work the same as the Primary Support Element, should you ever need to switch to using the Alternate Support Element (due to a Primary Support Element hardware failure, for example).

Ordinarily, Support Element data is mirrored automatically each day. But you can use this window to mirror Support Element data immediately, at any time and for any reason. For example, you may want to mirror Support Element data immediately after installing internal code changes on the Primary Support Element, to ensure the Alternate Support Element is at the same internal code level right away (otherwise, the Alternate Support Element would remain at the previous internal code level until its daily, automatic mirroring occurred).

To begin mirroring Support Element data for the selected CPC, select **Mirror the Primary Support Element data to the Alternate Support Element**.

Note: The Primary Support Element's daily automatic mirroring is scheduled for 10 a.m. with a one hour window for starting the operation. A record is added to the Support Element's event log to indicate the outcome of the operation.

Switch the Primary Support Element and the Alternate Support Element

This action switches the role of the two Support Elements, so that the Primary Support Element becomes an Alternate Support Element and the Alternate Support Element becomes a Primary Support Element.

To make a request to switch from the Primary Support Element to the Alternate Support Element, (or from the Alternate Support Element to the Primary Support Element), select **Switch the Primary Support Element and the Alternate Support Element**. This request automatically determines what type of switch it is, queries whether the switch is concurrent or disruptive, and displays the appropriate confirmation panel showing the switch information.

Query Switch Capabilities

This action provides the current switch status of the Alternate Support Element and whether or not the user interface switch, the user interface switch concurrency, or the automatic switch are enabled or disabled.

To see if different types of Switch requests (User Initiated or Automatic) are enabled or disabled, select **Query Switch Capabilities**. This request also displays the reasons why a Switch request has been disabled. If the User Initiated Switch is enabled, you are informed whether the type of switch is Concurrent or Disruptive. Generally, this option is only used if a switch did **not** occur as expected, or if you have a plan to periodically run this option to ensure that the alternate Support Element has no problems and is enabled for both types of switching.

When you have selected an action, you can proceed with any of the following:

OK
To perform the selected action, click **OK**.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Switch Disabled

The switch disabled status occurs when:

- Support Element is fenced from the previous automatic switchover
- A status change occurred on the Primary Support Element and has not been communicated to the Alternate Support Element

Or, if any of the following is in progress:

- Mirroring
- EC upgrade
- Restore Critical Data
- Install/Activate or Remove/Activate

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

Disruptive Switch

To use Disruptive Switch to switch the Primary Support Element to the Alternate Support Element the code levels of the Primary Support Element and Alternate Support Element must be different.

Switch Disruptive
To switch the Primary Support Element to the Alternate Support Element, click **Switch Disruptive**.

code levels of the Primary Support Element and Alternate Support Element must be different.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Concurrent Switch

You can use Concurrent Switch to switch the Primary Support Element to the Alternate Support Element if the code levels of the Primary Support Element and Alternate Support Element are the same.

Switch Concurrently
To switch the Primary Support Element to the Alternate Support Element, click **Switch Concurrently**.

The code levels of the Primary Support Element and Alternate Support Element must be the same.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Switch Capabilities

This window displays the current switch status of the Alternate Support Element and whether or not the user interface switch, the user interface switch concurrency, or the automatic switch are enabled or disabled.

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

Alternate Support Element Engineering Changes (ECs)

Accessing the Alternate Support Element Engineering Changes (ECs) task

Notes:

- This task is available only on a CPC that has both a primary and an alternate Support Element.
- You cannot perform this task remotely.

This task upgrades the alternate Support Element of the selected CPC. You can perform any of the following options:

Upgrade Alternate SE (Preload)
Upgrade both the operating system and the Support Element function code to the alternate Support Element.

Alternate SE - Retrieve and Activate MCLs from the support system
Retrieve and activate microcode level (internal code change) updates obtained from the support system to the alternate Support Element.

Upgrade Alternate SE (Preload) and then Retrieve and Activate MCLs from the support system
Upgrade the alternate Support Element (SE) and retrieve and activate the alternate Support Element (SE) Microcode Levels (MCLs) from the support system.

Alternate SE - Retrieve and Activate MCLs from removable media
Retrieve and activate microcode level (internal code change) updates obtained from removable media (USB flash memory drive) to the alternate Support Element.

To upgrade the alternate Support Element:

1. Select a CPC (server).
2. Open the **Alternate Support Element Engineering Changes (EC)** task. The Upgrade Engineering Change (EC) - Alternate SE window is displayed.
3. Select the engineering change option you want to perform, then click **OK**. The Apply Changes Confirmation window is displayed.
4. The processor or processors to change are listed. Click **OK** to confirm performing the update.

Upgrade Engineering Change (EC) - Alternate SE

Use this window to apply engineering changes to the alternate Support Element.

Upgrade Alternate SE (Preload)
To upgrade the alternate Support Element (SE) (Preload), select **Upgrade Alternate SE (Preload)**.

Alternate SE - Retrieve and Activate MCLs from the support system
To retrieve and activate the alternate SE Microcode Level (MCL) from the support system, select **Alternate SE - Retrieve and Activate MCLs from the support system**.

Upgrade Alternate SE (Preload) and then Retrieve and Activate MCLs from the support system
To upgrade the alternate Support Element (SE) and retrieve and activate the alternate Support Element (SE) Microcode Levels (MCLs) from the support system, select **Upgrade Alternate SE (Preload) and then Retrieve and Activate MCLs from the support system**.

Alternate SE - Retrieve and Activate MCLs from removable media
To upgrade the alternate Support Element (SE) and retrieve and activate the alternate Support Element (SE) Microcode Levels (MCLs) from removable media (USB flash memory drive), select **Alternate SE - Retrieve and Activate MCLs from removable media**.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

OK
To confirm your request to upgrade the engineering changes, click **OK**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Analyze Console Internal Code

Accessing the Analyze Console Internal Code task

This task enables you to retrieve, delete, or view a console's Licensed Internal Code fix.

To analyze console internal code:

1. Open the **Analyze Console Internal Code** task. The Analyze Internal Code Changes window is displayed.
2. Use the menu bar for the actions you want to perform on the internal code:
   - Selecting **File** allows you to choose to delete a selected code fix or choose to retrieve an MCF from removable media or an FTP site.
   - Selecting **Options** allows you to activate or deactivate an internal code fix.
   - Selecting **View** allows you to review the internal code fix information you are about to activate or lists the code fixes that have already been accepted.
3. When you have completed this task, select **File** from the menu bar, then click **Exit**.

Analyze Console Internal Code

Use this window to perform specific actions on selected internal code. Internal code fixes modify the console's Licensed Internal Code. The actions you can perform on the internal code fixes include:

- Reviewing internal code fix information and content.
- Retrieving and deleting internal code fixes.
- Activating and deactivating internal code fixes.

You can perform actions on internal code fixes only at the direction of your support system.

Select one or more internal code fixes from the list, then select a choice from the menu bar.

Click **File**, then select the following:

- **Delete** to erase one or more selected temporary internal code fixes.

- **Retrieve MCF from Removable Media** to receive internal code fixes from removable media.

  Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.
- **Retrieve MCF from FTP site** to receive internal code fixes from an FTP site.
- **Exit** to end this task and return to the console workplace.

Click **Options**, then select the following:

- Activate Internal Code Fix to prepare one or more internal code fixes to replace corresponding Licensed Internal Code.

  Note: This option is not available when you are accessing this task with a user ID definition that is based on the *Service Representative* task roles.
- Deactivate Internal Code Fix to prepare to remove one or more internal code fixes, to restore the corresponding Licensed Internal Code.

  Notes:

  1. You can activate or deactivate on one or more internal code fixes.
  2. This option is not available when you are accessing this task with a user identification that is based on the *Service Representative* task roles.

You can activate or deactivate on one or more internal code fixes.

Click **View**, then select the following:

- Internal Code Fix Information to display the contents of the file and list the code modules provided in an internal code fix.

  Note: You can only view the information on a single code fix.
- **Accepted Internal Code Fixes** to list internal code fixes that are a permanent part of the Licensed Internal Code on the console. You do not need to select an internal code fix to use this choice. Accepted fixes are no longer available for use with menu choices. An internal code fix is accepted when its internal code change level is accepted.

Click **Help** to display help for the current window.

You can find more detailed help on the following elements of this window:

Change management services

Change management services control the availability of operations used to work on internal code change levels stored on the console hard disk.

Change management services are either enabled or disabled, depending on the status of internal code fixes stored on the console hard disk.

Enabled
: Indicates you can work on internal code change levels stored on the console hard disk. The required operations are available.

Disabled
: Indicates you cannot work on internal code change levels stored on the console hard disk. The required operations are not available.

The services become disabled to prevent the use of an internal code change level that differs, in any way, from the change level provided by the support system.

Internal code change levels may be altered unintentionally by errors that occur while copying them. For example, change levels may not be copied correctly from removable media to the console hard disk.

Internal code change levels can be altered intentionally when you use the **Analyze Internal Code Change** window to activate a temporary internal code fix, or to activate individual fixes from a change level.

Note: If change management services are disabled, contact your support system for instructions before using the **Analyze Console Internal Code** task or the **Change Internal Code** task.

Internal code fixes table

This list displays the internal code fixes stored on the console hard disk. Select one or more fixes to work on, then select a choice from the menu bar.

EC Number
Specifies the Engineering Change (EC) number.

ID
Specifies the internal code fix identification.

Level
Identifies the internal code change level that includes the fix.

Note: Level 000 is not associated with an MCL.

Status
Indicates the outcome of the most recent work performed on the fix.

Date
Displays the date of the most recent change in status.

Time
Displays the time of day on the date of the most recent change in status.

Description
Displays a summary of engineering data or machine dependencies for the fix.

You can find more detailed help on the following:

Internal code fix status

The status of an internal code fix indicates the outcome of the most recent action performed on the fix. The status also indicates the type of action you can perform on the fix now. The status types and their conditions are the following:

Activated
The internal code fix is currently activated. The fix was activated individually using the **Analyze Internal Code Changes** window.

AutoActivated
The internal code fix is currently activated. The fix was activated automatically due to the activation of its internal code change level. The change level was activated by using the **Change Internal Code** task.

Deactivated
The internal code fix is currently deactivated. The internal code fix can be activated or viewed.

Error
An attempt to activate the internal code fix was not successful. The internal code fix is not activated.

Activated pending reboot
A request was made to activate the internal code fix, but the system requires a reboot.

Deactivated pending reboot
A request was made to deactivate the internal code fix, but the system requires a reboot.

Activate Internal Code Fix

To prepare one or more internal code fixes to replace corresponding licensed internal code, select **Activate Internal Code Fix**.

You must select one or more fixes to use with this choice.

The selected fixes are checked for syntax errors. The status of each fix becomes **Activated** or **Activated Pending Reboot** if no syntax errors are found.

If syntax errors are found in a fix, its status becomes **Error**. The fix must be edited to correct the errors before it can be activated.

This choice is available only while internal code fixes from the default directory display. Otherwise, it is unavailable.

Deactivate Internal Code Fix

To prepare to remove one or more internal code fixes and then restore the corresponding licensed internal code, select **Deactivate Internal Code Fix**.

You must select one or more fixes to use with this choice.

Deactivating internal code fixes does not erase them. The internal code fixes are replaced by corresponding licensed internal code. But the fixes remain available on the console hard disk.

The status of each fix becomes **Deactivated** or **Deactivated pending reboot** upon selecting this option.

This choice is available only while internal code fixes from the default directory display. Otherwise, it is unavailable.

Internal Code Fix Information

This window displays the contents of the file (**Details** tab) and lists the code modules (**Modules** tab) provided in an internal code fix.

Click **Cancel** to close the window.

Click **Help** to display help for the current window.

Details

Licensed Internal Code, referred to also as internal code, controls many of the operations available on the console. Internal code changes may provide new internal code or correct or improve existing internal code.

A service representative will provide new internal code changes and manage their initial use.

File name
Displays the name of the internal code fix file. An internal code fix name is made up of the following information:

- A one-character internal code fix type identifier
- A six-character engineering change (EC) name
- A three-character sequence number.

When saved as an internal code fix file, the fix type identifier and the EC name are used for the file name and the sequence number is the file extension.

Level
Identifies the internal code change level that includes the fix.

Author
Displays the name of the person who wrote the internal code fix.

Status
Displays a description of the status of the fix.

Date of last update
Displays the date of the most recent change in status.

Time of last update
Displays the time of day on the date of the most recent change in status.

Description
Displays a summary of engineering data or machine dependencies for the internal code fix.

Modules

Use this window to view the modules table which displays a list of the internal code fix modules.

File Name
The name of the file as it will exist on the console after the fix is activated.

Module Name
The name of the file as it exists in the console.

Size
The number of bytes in the module.

Date
The date the module was created.

Time
The day and time the module was last updated.

Browse MCF Data

To view the contents of the selected MCF (microcode fix) data file, click **Browse MCF Data**.

Browse MCL Data

If an MCF is included in an MCL (microcode library) data file, you can view the contents of the selected MCL data file by clicking **Browse MCL Data**.

Archive Security Logs

Accessing the Archive Security Logs task

Notes:

- When you use a USB flash memory drive it must have a capacity of 1 GB or greater.
- You can perform this task remotely. However, you can only archive security logs to an FTP server.

This task allows you to archive a security log for the console or Central Processor Complex (CPC) to a USB flash memory drive or an FTP server. Up to ten CPC security logs can be archived at one time. When the Archive Security Logs window is displayed, verify that the console or CPC shown in the window list is the one whose security log you want to archive.

To archive a security log:

1. Select the console's or CPC's security logs.
2. Open the **Archive Security Logs** task. The Archive Security Logs window is displayed.
3. Verify the console or CPC(s) shown in the window list is the one whose security log you want to archive.

   Note: Ensure that the USB flash memory drive that you are using for archiving is inserted properly.
4. Click **Archive**, choose the USB flash memory drive or an FTP server to archive to from the Archive to Removable Media or FTP Server window, then click **OK** to start the procedure.

Archive Security Logs

Use this window to confirm or cancel your request to archive the console's security log or the security logs for the selected Central Processor Complex's (CPCs).

Archiving the security log is a means of long-term storage of security events.

Archiving saves the security log's event data in another file on a USB flash memory drive, then erases enough events from the log to reduce its size to 20 percent of its maximum capacity.

Consider archiving a security log *before* its current size reaches 100 percent of its maximum capacity. Otherwise, if you allow the security log to reach its maximum capacity, the oldest one-third of its events will be erased automatically to allow logging new events.

Note: When you use the **View Security Logs** task to view the console's security log, its current size is displayed (as a percentage of its maximum capacity) near the bottom of the **View Security Logs** window.

Archive
To archive the console's or Central Processor Complex's (CPCs) security logs, click **Archive**. The “Archive to Removable Media or FTP Server” on page 427 window is displayed. From this window, you can choose a USB flash memory drive or an FTP server you want to send the data to. If you’re accessing this task remotely, the “Archive to FTP Server” on page 428 window is displayed. You can only archive to an FTP server remotely.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Cancel
To close this window without archiving the security logs and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Archive to Removable Media or FTP Server

Use this window to archive a security log to a USB flash memory drive or to an FTP server.

Note: If you are accessing this task remotely, you only have the option to archive a security log to an FTP server.

Hardware Management Console USB flash memory drive
To archive a security log to a Hardware Management Console USB flash memory drive, select **Hardware Management Console USB flash memory drive**. A table is displayed which includes the available USB flash memory drives. To make sure you have the available USB flash memory drive, click **Refresh**.

Note: If you’re using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP Server
To archive a security log to an FTP server, select **FTP Server**. The following input areas are displayed.

Host name:
Specify the host name address or destination. This is a required field.

User name:
Specify the user name for the target FTP destination. This is a required field.

Password:
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol:

Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)
- **SFTP** (SSH File Transfer Protocol)

File path
If you select an FTP server the security log is to be archived to, you must provide the path name in the input area.

Note: The file path has a maximum length of 2048 characters.

OK
To continue with your selection, click **OK**.

Cancel
To exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Archive to FTP Server

Use this window to archive a security log to an FTP server.

Host name:
Specify the host name address or destination. This is a required field.

User name:
Specify the user name for the target FTP destination. This is a required field.

Password:
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol:

Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)
- **SFTP** (SSH File Transfer Protocol)

File path
Provide the path name in the input area.

If you don't provide a file path for an FTP selection, then the default is to the home directory of the FTP server.

Note: The file path has a maximum length of 2048 characters.

OK
To continue with your selection, click **OK**.

Cancel
To exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Audit and Log Management

Accessing the Audit and Log Management task

Use this task to choose the audit data types to be generated, viewed, and offloaded to a remote workstation or removable media.

To generate audit report data:

1. Open the **Audit and Log Management** task. The Audit and Log Management window is displayed.
2. Select the report type to be generated.
3. Select the audit data type of report you want to generate from the audit data types list.

Note: The audit data types list displays only the data types that the user has authority to view.

4. Optionally, select **Limit event based audit data to a specific range of dates and times** to limit the report content for the selected event based audit data types to a time and date range.
5. Optionally, select the range of dates and times for the event based audit data types using the **View Calendar** and **View Time** icons to the right of the entry fields.
6. Click **OK** to generate the selected reports.

Audit and Log Management

Use this window to choose the audit data types to be generated, viewed, and offloaded to a remote workstation or removable media.

To generate an audit report:

- Select the report type to be generated
- Select the audit data type of report you want to generate from the **Audit data types** list

  Note: The audit data types list only displays the data types that the user has authority to view.
- Optionally select **Limit event based audit data to a specific range or dates and times** to limit the report content for the selected event based audit data types to a time and date range
- Optionally select the range of dates and times for the event based audit data types using the icons to the right of the entry fields
- Click **OK** to generate the report.

Additional functions on this window include:

OK
To proceed with your selections, click **OK**.

Cancel
To close this window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Report type

Select the format type of report to be generated. The supported types of reports are:

HTML
HyperText Markup Language is used to generate an easily viewable report.

XML
eXtensible Markup Language is used to generate a report that is easily parsed by programs for backend processing.

Note: You can view the XML schema file from Resource Link. This file defines the form of the XML output for audit, event, and security logs.

Range for event based audit data types

Use this section to limit the selected event based audit data type log to a specific range of dates and times. Use the **View Calendar** and **View Time** icons to the right of the entry fields to indicate the date and time for the selected event based audit data types to be included in the generated report.

Limit event based audit data to a specific range of dates and times
To limit the report content for the selected event based audit data types to a specific date and time range, select **Limit event based audit data to a specific range of dates and times**.

Starting date
Specify the starting date for the range used to limit the content of selected event based audit data types contained in the report. Use the icon to the right of the entry fields to indicate the starting date for the selected event based audit data types to be generated.

Starting time
Specify the starting time for the range used to limit the content of selected event based audit data types contained in the report. Use the icon to the right of the entry fields to indicate the starting time for the selected event based audit data types to be generated.

Ending date
Specify the ending date for the range used to limit the content of selected event based audit data types contained in the report. Use the icon to the right of the entry fields to indicate the ending date for the selected event based audit data types to be generated.

Ending time
Specify the ending time for the range used to limit the content of selected event based audit data types contained in the report. Use the icon to the right of the entry fields to indicate the ending time for the selected event based audit data types to be generated.

Audit data types

Select the audit data types that you want included in the audit report from the list. When you have completed selecting the preferred audit data types, click **OK** to generate the audit report. The Audit and Log Report window displays the audit report.

Note: The audit data types list only displays the data types that the user has authority to view. For example, the "Users" data type under "User profiles" is only shown to users who are authorized to the **Manage Users** task portion of the **User Management** task.

Audit and Log Report

Use this window to view a generated audit report and offload the generated report to a remote workstation or removable media.

Additional functions on this window include:

Save...

You can save the generated audit report:

Remotely
A browser window displays to specify the location for the audit report to be saved. To save the audit report content, click **Save...**.

Locally
A window displays to specify the name of the file and removable media selection for saving the audit report. To save the audit report content, click **Save...**.

Close
To close this window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Authorize Internal Code Changes

Accessing the Authorize Internal Code Changes task

This task gives you the option to allow or to not allow the Hardware Management Console and all of its managed systems to install and activate licensed internal code changes.

To authorize internal code changes:

1. Open the **Authorize Internal Code Changes** task. The Authorize Internal Code Changes window is displayed.

2. To authorize internal code changes make sure **Do not allow installation and activation of internal code changes** is ***not*** selected (a check mark does not appear).
3. Click **Save** if a change was made and begin the operation, or **Cancel** to close the task without proceeding with the operation.

Authorize Internal Code Changes

Use this window to verify or change the setting that allows using this console to perform installation and activation of internal code changes and other **subsequent operations**.

The operations can be used to work with internal code changes on this console and all of its managed systems.

When to change the setting

Normally, the operations are **allowed**.

- Change the setting to not allow the operations when you do not want internal code to be changed. This can be for any reason.
- Change the setting to not allow the operations when you perceive a problem after changes are activated. This prevents installing and activating the same changes on other systems, and reduces the risk of causing the same problem on them.
- Change the setting to allow the operations when you want to install and activate changes that correct a previously detected problem.

Note: The console automatically changes the setting to not allow the operations if it detects errors after activating new internal code changes.

Do not allow installation and activation of internal code changes
To change the setting that allows using this console to perform installation and activation of internal code changes and other **subsequent operations**, select **Do not allow installation and activation of internal code changes**.

A check mark displays to indicate the operations are **not allowed**.

Subsequent Operations

A set of tasks that can be used to work with internal code changes and managed systems only after the changes are installed or activated.

Subsequent operations include:

- Accepting changes that are installed and activated.
- Removing changes that are installed but not activated.
- Deleting changes that are removed, or retrieved but not installed.
- Backing up critical hard disk data.

The internal code change setting for a console controls whether performing the operations is allowed.

The option displays the current setting:

Select the option
A check mark is displayed and indicates the operations are **not allowed**.

Not allowed
An internal code change setting that does not allow using a console to perform installation and activation of internal code changes and other **subsequent operations**.

This is not the normal setting.

Normally, the operations are **allowed**.

The normal setting might be changed to not allow the operations:

- Manually, by a user who wants to prevent changing internal code for any reason.
- Automatically, by the console when it detects an error after activating new internal code changes.
- Manually, by a user who perceives a problem after activating new internal code changes.

Do not select the option
A check mark is not displayed and indicates the operations are **allowed**.

Allowed
An internal code change setting that allows using a console to perform installation and activation of internal code changes and other **subsequent operations**.

This setting allows scheduling the operations to perform them automatically and on a regular basis. It also allows manually performing the operations using console tasks.

This is the normal setting.

Select or clear the option to change the setting, then click **Save**, to save the new setting.

Save
To save a new setting or to keep the existing setting and begin the operation, click **Save**.

The **Authorize Internal Code Changes Progress** window is displayed, click **OK** to exit this window.

Reset
To restore the setting to its original choice, click **Reset**.

Cancel
To exit the window without applying any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Automatic Activation

Accessing the Automatic Activation task

This task controls whether the selected CPC is activated automatically when power is restored following a utility power failure. Follow your local procedures for recovering from a power outage that is the result of a utility power failure. You may, however, be able to speed recovery from such power outages by enabling *Automatic Activation* for the selected CPC.

- When automatic activation is *enabled* and a utility power failure occurs, the CPC is activated automatically when the power is restored. The CPC is activated using the same reset profile used most recently to activate the CPC before the power outage.
- When automatic activation is *disabled* (default setting) and a utility power failure occurs, the CPC power remains off when the power is restored. You can activate the CPC manually at any time once the utility power is restored. If the system had been IMLed without using **Activate**, then the CPC is not automatically activated when power is restored, even if automatic activation is enabled.

To enable or disable automatic activation:

1. Select one or more CPCs (servers).
2. Open the **Automatic Activation** task. The Automatic Activation window is displayed.
3. Click **Enable** or **Disable** depending on your preference.
4. Click **Save** to save the setting and close the window.

Automatic Activation

Use this window to enable or disable automatic activation for the selected Central Processor Complex (CPC).

Automatic activation is a CPC setting that controls whether the selected CPC is activated automatically when power is restored following a utility failure.

You should customize the selected CPC's automatic activation setting, in advance, to suit your local procedures for recovering from a power outage that is the result of a utility power failure.

Activation table
Displays whether automatic activation is enabled or disabled and allows you to change the setting.

Object Name
Displays the name of the CPC.

Setting
Indicates whether automatic activation for the CPC is currently enabled or disabled.

- Enable Automatic Activation:

  To enable automatic activation for the selected CPC, select **Enabled**. When automatic activation is *enabled*, and a utility power failure occurs, the selected CPC is activated automatically when utility power is restored. The selected CPC is activated using the same reset profile used most recently to activate the CPC before the power outage.

- Disable Automatic Activation:

  To disable automatic activation for the selected CPC, select **Disabled**. When automatic activation is *disabled*, and a utility power failure occurs, the selected CPC power remains off when utility power is restored. You can manually activate the CPC at any time after utility power is restored.

Save
To save new settings, click **Save**.

Reset
To return to the settings from the last save, click **Reset**.

Cancel
To return to the settings from the last save and exit the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Enable Automatic Activation

To enable automatic activation for the selected Central Processor Complex (CPC) to automatically activate the last used reset profile:

1. Select the CPC. The selected CPC becomes highlighted and the setting for the selected is displayed.
2. Select **Enabled**. The automatic activation setting displays Enabled.
3. To save the setting, click **Save**. A message is displayed confirming that the setting is saved.
4. Click **OK**. The Automatic Activation window is displayed.
5. To return to the previous window without saving any more new settings, click **Cancel**.

Disable Automatic Activation

To disable automatic activation from the last used reset profile for the selected Central Processor Complex (CPC):

1. Select the CPC. The CPC becomes highlighted and the setting for the selected CPC is displayed.
2. Select **Disabled**. The automatic activation setting displays Disabled.
3. To save the setting, click **Save**. A message is displayed confirming that the setting is saved.
4. Click **OK**. The Automatic Activation window is displayed.
5. To return to the previous window without saving any more new settings, click **Cancel**.

Backup Critical Console Data

Accessing the Backup Critical Console Data task

Notes:

- The USB flash memory drive used for the **Backup Critical Console Data** task must be formatted with a volume label of **ACTBKP**.
- This task backs up only the critical data associated with Hardware Management Console Application (HWMCA).
- To back up data stored on each Support Element, see the **Backup Critical Data** task.
- To back up data to an FTP server, you must define your external server using the **Configure Backup Settings** task.

This task backs up the data that is stored on your Hardware Management Console hard disk and is critical to support Hardware Management Console operations. You should back up the Hardware Management Console data after changes have been made to the Hardware Management Console or to the information associated with the processor cluster.

Information associated with processor cluster changes is usually information that you are able to modify or add to the Hardware Management Console hard disk. Association of an activation profile to an object, the definition of a group, hardware configuration data, and receiving internal code changes are examples of modifying and adding information, respectively.

Use this task after customizing your processor cluster in any way. A backup copy of hard disk information may be restored to your Hardware Management Console following the repair or replacement of the fixed disk.

To back up console data:

1. Open the **Backup Critical Console Data** task. The Backup Settings window is displayed.
2. Choose the destination in which to back up your files:
   - USB
   - FTP server
   - USB or FTP server
3. To proceed with your selection, click **OK**.
4. The Backup Critical Console Data Progress window is displayed.
5. When backup is complete, click **OK**.

Backup Settings

Use this window to select your back up settings in which to back up critical data for this console. The backup critical data operation copies critical files from the console to a USB flash memory drive, to an FTP server, or to both.

Select your backup destination
Select one of the choices provided in the drop-down.

USB
To choose to have your files backed up to a USB flash memory drive, select **USB** and insert a formatted USB flash memory drive into the drive.

The USB flash memory drive for the **Backup Critical Console Data** task must be formatted with a value label of **ACTBKP**, using the **Format Media** task.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP server
To choose to have your files backed up to an FTP server, choose **FTP server**. Set up a connection to the FTP server from the **Configure Backup Settings** task.

Note: If you have not set up a connection to the FTP server, then a message appears to configure your FTP server. You might also receive a message indicating the transfer rate of the data is not acceptable, you can choose whether or not to continue or cancel this task.

USB and FTP server
To choose to have your files backed up to both a USB flash memory drive and an FTP server, select **USB and FTP server**.

Note: If you have not set up a connection to the FTP server, then a message appears to configure your FTP server. You might also receive a message indicating the transfer rate of the data is not acceptable, you can choose whether or not to continue or cancel this task.

OK
To back up the hard disk information for this console depending on your selection of the backup destination, click **OK**.

Cancel
To cancel your request to back up critical data, click **Cancel**.

Help
To display help for the current window, click **Help**.

Backup Critical Data

Accessing the Backup Critical Data task

Note: You must define your external server by using the **Configure Backup Settings** task to back up data to an FTP server.

This task transfers critical CPC data that is stored on its Support Element to the Hardware Management Console and copies it to the hard disk on the SEs only or to the hard disk on the SEs and to the FTP server. CPC data should be backed up when configuration or CPC licensed internal code changes have been made or as a routine preventive maintenance procedure.

To back up critical CPC data stored on its Support Element:

1. Select one or more CPCs.
2. Open the **Backup Critical Data** task. The Backup Critical Data Confirmation window is displayed.
3. Select the appropriate backup destination.
4. To begin the backup, click **OK**.
5. The Backup SE Critical Data Progress window is displayed.
6. When back up is complete, click **OK**.

Backup Critical Data Confirmation

Use this window to confirm or cancel your request to back up Central Processor Complex (CPC) hard disk information to the hard disk on the SEs only or to the hard disk on the SEs and to the FTP server.

Notes:

- Although it is allowable to back up selected CPCs, it is recommended that all CPCs are backed up at the same time. This can be done by targeting a group for CPCs.
- The backup critical data operation copies critical files from the CPCs hard disks to the hard disk on the SEs only or to the hard disk on the SEs and to the FTP server.

Table of selected CPCs
This is a list of the CPCs that are selected for back up.

Name
Specifies the name of the CPC.

Backup Destination
Select the location in which the hard disk information will be stored.

Primary and Alternate SE
To choose to back up files to the hard disk on the Support Elements, select **Primary and Alternate SE**.

Primary SE, Alternate SE, and FTP Server
To choose to back up files to the hard disk on the Support Elements and to an FTP server, select **Primary SE, Alternate SE, and FTP Server**. Set up a connection to the FTP server from the **Configure Backup Settings** task.

Note: If you have not set up a connection to the FTP server, then a message appears to configure your FTP server. You might also receive a message indicating the transfer rate of the data is not acceptable. You can choose whether or not to continue or cancel this task.

OK
To proceed with the back up, click **OK**.

Cancel
To cancel your request to back up selected CPCs and nodes and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Block Automatic Licensed Internal Code Change Installation

Accessing the Block Automatic Licensed Internal Code Change Installation task

This task, used by an access administrator or a user ID that is assigned access administrator roles, allows you to prevent automatically installed licensed internal code change from being installed outside of an explicitly initiated licensed internal code change installation operation.

Note: In most cases, this setting should not be changed. If this task is set to block automatic licensed internal code change installation, it prevents your system from automatically retrieving critical service or customer alerts, in addition to future enhanced driver maintenance sync port updates.

To block automatic licensed internal code change installation:

1. Open the **Block Automatic Licensed Internal Code Change Installation** task. The Block Automatic Licensed Internal Code Change Installation window is displayed.
2. Select **Block Automatic Licensed Internal Code Change Installation**, then click **Save** to complete the task.

Block Automatic Licensed Internal Code Change Installation

Use this window to prevent automatically installed licensed internal code changes from being installed outside of an explicitly initiated licensed internal code change installation operation.

When to change the setting

In most cases, this setting should not be changed. Blocking automatic licensed internal code change installation prevents your system from automatically retrieving Critical Service/Customer alerts, in addition to future Enhanced Driver Maintenance sync point updates.

To block automatically installed licensed internal code changes from being installed outside of an explicitly initiated licensed internal code change installation operation, select **Block automatic Licensed Internal Code Change installation**, then click **Save** to save the new setting.

Note: The setting applies only to licensed internal code changes for the current console.

Block automatic Licensed Internal Code Change installation
Changes the setting that blocks automatic licensed internal code change installation on this console.

The option displays the current setting if you:

Select the option
A check mark is displayed and indicates that automatic licensed internal code change installation is currently blocked.

Do not select the option
A check mark is NOT displayed and indicates that automatic licensed internal code change installation is currently blocked.

Save
To set the saved-state values to the changed setting choice and begin the operation, click **Save**.

Note: A message is displayed confirming your selection to block your system from automatically installing Critical Service/Customer alerts and future Enhanced Driver Maintenance sync point updates. Click **Yes** to continue or **No** to return to the previous window.

Cancel
To close this window and exit the task without applying any changes, click **Cancel**.

Note: If you click **Cancel** and made a change to this window without saving first, a message is displayed indicating a change has been made. Click **Yes** to exit the task without making changes, or click **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Browse Directories and Files

Browse Directories and Files

Use this window to view selected directories and files.

File name
Specifies the file name of the security log you want to open.

Show Files
To view a list of files, click **Show Files**.

Directories
Shows the tree structure of the directories where the archived security logs reside. You can click on a directory to get a list of log files in that directory to choose from.

Select
Indicates how many files you have selected that you want to open. However, only one file can be opened at a time.

OK
To confirm your file selection, click **OK**. You can only open one file at a time.

Cancel
To exit this window without making a file selection, click **Cancel**.

Help
To display help for the current window, click **Help**.

Certificate Management

Accessing the Certificate Management task

All remote browser access to Version 2.9.0 or later of the Hardware Management Console must use Secure Sockets Layer (SSL) encryption. With SSL encryption required for all remote access to the Hardware Management Console, a certificate is required to provide the keys for this encryption. Version

2.9.0 or later of the Hardware Management Console provides a self-signed certificate that allows this encryption to occur.

This task manages the certificate(s) used on your Hardware Management Console. It provides the capability of getting information on the certificate(s) used on the console. This task allows you to create a new certificate for the console, change the property values of the certificate, and work with existing and archived certificates, signing certificates, or cipher suites.

Note: For any newly created, self-signed, or CA-signed certificates, the supported certificate key length is 2048 bits.

To manage your certificates:

1. Open the **Certificate Management** task. The Certificate Management window is displayed.
2. Use the menu bar from the Certificate Management window for the actions you want to take with the certificates:
   - To create a new certificate for the console, click **Create**, then select **New Certificate**. Determine whether your certificate will be self-signed or signed by a Certificate Authority, then click **OK**.
   - To modify the property values of the self-signed certificate, click **Selected**, then select **Modify**. Make the appropriate changes, then click **OK**.
   - To work with existing and archived certificates, signing certificates, or cipher suites, click **Advanced**. Then you can choose the following options:
     - Delete and archive certificate
     - Work with archived certificate
     - Import server certificate
     - Export server certificate
     - Configure SSL cipher suites
     - Manage trusted signing certificates
     - View issuer certificate.
3. Click **Apply** for all changes to take effect.

Certificate Management

Use this task to provide the capability of getting information on the certificate(s) used on the console. Use the window's menu bar to perform the following functions on the certificates:

- Click **Create**, New Certificate to create a new certificate for the console.
- Click **Selected**, **Modify** to change the property values of the certificate.
- Click **Advanced** to work with existing and archived certificates, signing certificates, or cipher suites:
  - Click **Delete and Archive Certificate** to delete/archive the current certificate.
  - Click Work with Archived Certificate to work with a previously archived certificate.
  - Click **Import Server Certificate** to import and install a certificate signed by a Certificate Authority.

    Note: The certificate file must contain only a CA-signed X.509 certificate and may be supplied in the binary Distinguished Encoding Rules (DER) or printable (Base64 encoded ASCII) formats. The signed certificate must be based on a Certificate Signing Request (CSR) that was exported from this HMC. If the certificate is provided in Base64 encoding, it must be bounded at the beginning by `----BEGIN CERTIFICATE----`, and must be bounded at the end by `----END CERTIFICATE----`. Attempting to import a certificate that cannot be read by the HMC will result in message ACT05178. The HMC does not support PKCS formats (e.g. PKCS#7 and PKCS#12) and will fail to import files in PKCS format, even if they are DER or Base64 encoded ASCII files.
  - Click **Export Server Certificate** to export the server certificate being used by this console.
  - Click Configure SSL Cipher Suites to define the SSL cipher suites that are allowed to be used.
  - Click Manage Trusted Signing Certificates to allow for the import of trusted signing certificates.

– Click **View Issuer Certificate** to view a Certificate Authority's certificate used to sign the certificate in use by the console, if any.

Note: For any newly created, self-signed, or CA-signed certificates, the supported certificate key length is 2048 bits.

Certificate Properties and Values
This table displays the properties and values of the certificate that you created for your console. You can modify the values by selecting the property, then click **Selected**, **Modify** to change the value.

Note: The only values that can be selected for modifying are **Valid Until**, **Subject**, and **Subject Alternative Names**.

Apply
To save changes made to the certificate, click **Apply**.

Note: If the installation is successful the console is restarted.

Cancel

To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Certificate Signing

Use this window to decide if you want the new certificate to be self-signed or signed by a Certificate Authority (such as Verisign or Entrust or a Certificate Authority within your own enterprise).

Note: The self-signed certificate or the Certificate Signing Request (CSR) will use SHA-256 as the certificate signing algorithm.

Self-signed
If you do not choose to use a Certificate Authority (CA) to sign the certificate, select **Self-signed**.

Signed by a Certificate Authority
To use a Certificate Authority (CA) (such as Verisign or Entrust or a Certificate Authority within your own enterprise) to sign the certificate for the Hardware Management Console, select **Signed by a Certificate Authority**. A Certificate Signing Request (CSR) is generated.

OK
To have the new certificate self-signed or signed by a Certificate Authority, click **OK**.

Cancel
To close this window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

New or Modify Certificate

Use this window to provide the necessary information to create a new certificate that is enabled for the console or to modify the values of the **Subject** property from an existing certificate.

Common name
Specify the common name for the certificate. Generally this name matches the “Console name” appended with a period character (that is, '.') appended with the “Domain name”. This is where the “Console name” and “Domain name” are specified within the **Customize Network Settings** task. For example, if the “Console name” is “HMC” and the “Domain name” is “ibm.com”, the common name is specified as “HMC.ibm.com”. If a certificate is being created, this field is pre-filled with the values, if any, currently specified for the “Console name” and “Domain name” and can be overridden. The specified common name must be 1 - 64 characters in length.

Organization
Optionally, specify the name of the corporation, limited partnership, university, or government agency. The specified organization name must be 1 - 64 characters in length.

If a *self-signed certificate* is being created or modified, the organization name can be any name recognizable to the console users.

If a *certificate signed by a certifying authority* is being created, the organization name must be registered with some authority at the national, state, or city level and must be the legal name that your organization is registered with.

Organization unit
Optionally, specify the organization name, which differentiates between divisions within an organization. For example, 'Hardware Development' or 'Human Resources'. The specified organization unit name must be 1 - 64 characters in length.

Country or region
Optionally, select or specify the two-character ISO format country code for your country. For example, a two-character code of 'GB' for Great Britain or 'US' for the United States. For convenience, the list of current two-character country codes is available for selection. If specified, the two-character specified country code must consist of alphabetic characters, numeric characters, or the following special characters:

- apostrophe (')
- left and right parentheses ( )
- plus sign (+)
- comma (,)
- dash (-)
- period (.)
- slash (/)
- colon (:)
- equals sign (=)
- question mark (?)

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the list. If you do not need to include a country or region code in the certificate, then select **No value** from the drop-down.

Note: This field defaults to the country or region that you configured in the **Customize Customer Information** task, otherwise, it defaults to "US".

State or province
Optionally, select or specify the state or province name where the organization that owns the console operates. For convenience, the list of states or provinces might be available for selection, depending on the value that is selected within the **Country or region** field. Otherwise, "No value" is displayed. Also, if a certificate is being created, the first value in the alphabetical list is selected by default. The specified state or province name must be 1 - 128 characters in length.

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the list. If you do not need to include a state or province in the certificate, then select **No value** from the drop-down.

If a *self-signed certificate* is being created or modified, the state or province name can be any name recognizable to the console users.

If a *certificate signed by a certifying authority* is being created and the organization that owns the console operates in a state in the United States or a province in Canada, the state or province must be specified and cannot be abbreviated.

Note: Organizations outside the United States or Canada can leave this field empty only if a Locality is specified.

Locality
Optionally, specify the city or locality name where the organization that owns the console operates. The specified city or locality name must be 1 - 128 characters in length.

If a *self-signed certificate* is being created or modified, the state or province name can be any name recognizable to the console users.

If a *certificate signed by a certifying authority* is being created, the name must not be abbreviated.

Note: Organizations outside the United States or Canada can leave this field empty but only if a State or Province is specified.

Number of days until expiration
Specify the number of days that the certificate can be valid for, beginning from the time the certificate is created or modified. If a certificate is being created, the field is pre-filled with a value of 3653 (approximately 10 years). The value that is specified must be 1 - 3653 days, inclusive.

Email address
Optionally, specify the email address of the contact person or persons for this console. The specified email address must be 1 - 128 characters in length and consist of US ASCII characters.

OK
To create and enable a new certificate or modify an existing certificate on the console, click **OK**.

Cancel
To exit this window without creating a new certificate or modifying an existing certificate and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Modify DNS and IP Address

Use this window to modify the values of the **Subject Alternative Names** property of an existing certificate on the console.

DNS entry
Specify a DNS entry to add to the list of valid entries for the console.

You can also specify this name, for the host name part of the URL, used to access the console through a web browser.

DNS list
Displays a list of the valid DNS entries for the console. You can add to or remove from the list.

Add
To add a DNS entry, specify the DNS name in the field provided, then click **Add**.

Remove
To remove a DNS entry from the list, select the name to be deleted, then click **Remove**.

IP Address
Specify an IPv4 or IPv6 address in the field provided to add to the list of valid addresses for the console. The IPv4 address must be specified as 4 decimal numbers separated by a period (e.g. dd.ddd.ddd.ddd). The IPv6 address can be specified in several different ways with one form being 8 hexadecimal numbers separated by a colon (e.g. xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).

You can also specify this IP address, for the host name part of the URL, used to access the console through a web browser.

IP Address List
Displays a list of valid IPv4 and IPv6 addresses for the console. You can add to or remove from the list.

Add
To add an IPv4 or IPv6 address, specify the address in the field provided, then click **Add**.

Remove
To remove an IPv4 or IPv6 address from the list, select the address to be deleted, then click **Remove**.

OK
To save all the changes and close this window, click **OK**.

Cancel
To close this window without saving the changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Modify Expiration

This window is used to change the expiration of the certificate.

Number of days
Specify the number of days that the certificate should be valid for, beginning from the time the certificate is modified.

OK
To save the new expiration, click **OK**.

Note: The certificate is not modified until you click **Apply** from the main (**Certificate Management**) window.

Cancel
To exit this window without changing the expiration, click **Cancel**.

Help
To display help for the current window, click **Help**.

Issuer Certificate

Use this window to view the Certificate Authority's (such as Verisign or Entrust) certificate used to sign the certificate in use by the console, if any.

Issuer Certificate Properties and Values
This table displays the properties and values of the Certificate Authority's certificate used to sign the certificate in use by the console, if any.

Close
To return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Archived Certificate

Use this window to work with an archived certificate.

A certificate becomes archived when you previously requested to delete the certificate.

Click **Actions** on the menu bar:

- To import and install the archived certificate you are viewing, click **Install**.
- To view an archived Certificate Authority's certificate used to sign an archived certificate, click **View Archived Issuer Certificate**.

Archived Certificate Properties and Values
This table displays the properties and values of the archived certificate that was previously created for your console.

Close
To return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Archived Issuer Certificate

Use this window to view the issuer certificate that was used to sign the archived certificate that you are currently viewing, if any. If you click **Actions**, **View Archived Issuer Certificate** from the menu bar while viewing an archived issuer certificate you will be viewing the archived issuer certificate that was used to sign the archived issuer certificate that you are viewing.

Archived Issuer Certificate Properties and Values
This table displays the properties and values of the issuer certificate.

Close
To return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

File Selection

This window displays the certificates and issuer certificates that you can import and install on the console.

Note: If the installation is successful the console is restarted.

Files
Select the certificate or issuer certificate(s) that you want to import and install on the console.

OK
To proceed with your selection, click **OK**.

Cancel
To return to the previous window without making a selection, click **Cancel**.

Help
To display help for the current window, click **Help**.

Export Server Certificate

Use this window to select where the **server certificate** will be written.

Export to Hardware Management Console USB Device
To export data to the Hardware Management Console USB flash memory drive, select **Export to Hardware Management Console USB Device**. Insert a USB flash memory drive into a USB port, then click **OK**. The server certificate is written to the top-level directory of the media in the device.

To update the device list, click **Refresh**.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Export to FTP Server
To export data to an FTP server, select **Export to FTP server**. Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

File path
Specify the FTP server directory where files are to be saved to or read from.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the Manage SSH Keys task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

Export to Remote File System
To export data to a remote file system, click **Export to Remote File System**, then click **OK**. The Save File window is displayed where you can navigate to the appropriate directory and save the server certificate.

Note: This option is only available if you are accessing the Hardware Management Console remotely.

OK
To continue the task, click **OK**.

Cancel
To exit this window without making any changes and to return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Import Server Certificate

Use this window to select where the signed server certificate and optional signing certificate(s) will be imported.

Note: The certificate file provided must be Distinguished Encoding Rules (DER) encoded and may be supplied in binary or printable (Base64) encoding. If the certificate is provided in Base64 encoding, it must be bounded at the beginning by `----BEGIN CERTIFICATE----`, and must be bounded at the end by `----END CERTIFICATE----`.

Import from Hardware Management Console USB Device
To import data from the Hardware Management Console USB flash memory drive, select **Import from Hardware Management Console USB Device**. Insert a USB flash memory drive into a USB port, then click **OK**. The server certificate must exist in the top-level directory of the media in the device.

To update the device list, click **Refresh**.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Import from FTP Server
To import data from an FTP server, select **Import from FTP server**. Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

File path
Specify the FTP server directory where files are to be saved to or read from.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the Manage SSH Keys task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

Import from Remote File System
To import data from a remote file system, click **Import from Remote File System**, then click **OK**. The Upload File window is displayed where you can navigate to the appropriate directory and select the name of the server certificate.

Note: This option is only available if you are accessing the Hardware Management Console remotely.

OK
To continue the task, click **OK**.

Cancel
To exit this window without making any changes and to return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save File

Use this window to select the **Certificate Signing Request** link that is used to save the Certificate Signing Request as a file on the system running the browser.

OK
After the file has been saved, click **OK** to return to the **Certificate Management** task.

Cancel
To return to the previous window without saving the file, click **Cancel**.

Help
To display help for the current window, click **Help**.

Upload File

Use this window to specify the name of the server certificate file or signing certificate files, if any, to import to the console. The file(s) specified must exist on the system running the browser. You can click **Browse...** to locate the file(s) you need to import.

Note: The certificate file must contain only a CA-signed X.509 certificate and may be supplied in the binary Distinguished Encoding Rules (DER) or printable (Base64 encoded ASCII) formats. The signed certificate must be based on a Certificate Signing Request (CSR) that was exported from this HMC. If the certificate is provided in Base64 encoding, it must be bounded at the beginning by `----BEGIN CERTIFICATE----`, and must be bounded at the end by `----END CERTIFICATE----`. Attempting to import a certificate that cannot be read by the HMC will result in message ACT05178. The HMC does not

support PKCS formats (e.g. PKCS#7 and PKCS#12) and will fail to import files in PKCS format, even if they are DER or Base64 encoded ASCII files.

OK
To perform the import of the specified file(s) to the console, click **OK**.

Cancel
To return to the previous window without importing the specified file(s), click **Cancel**.

Help
To display help for the current window, click **Help**.

Manage Trusted Signing Certificates

Use this window to allow for the import of trusted signing certificates. Currently, the only practical uses of importing these certificates are:

- When the HMC is connecting to a syslog server that has been configured using the **Manage Syslog Servers** task to make SSL connections. (See the "Manage Syslog Servers" on page 1001 task for more inforamation.)
- When LDAP authentication is used to log on to the console. (See the "User Management" on page 1389 task for more information.)
- When the console's 3270 session is forced through a TLS tunnel (see the "Configure 3270 Emulators" on page 524 task for more information) or the 3270 server negotiates for the 3270 session to use a TLS tunnel.
- When a proxy server, that is used for RSF connections, performs an SSL inspection by terminating SSL connections at the proxy instead of IBM.
- When IBM Multi-Factor Authentication for z/OS is used to log on to the console. (See the "User Management" on page 1389 task for more information.)
- When a console task that supports connecting to an FTP server is used and the FTPS protocol is selected.

Trusted signing certificates are used:

- When an application on a different system sends this console a certificate or chain of certificates.
- If the console is to trust the certificate or chain of certificates, the issuer/signer of the certificate or the issuer/signer of the root certificate in the chain must be equal to the subject of one of the trusted signing certificates. Also, the public key of the trusted signing certificate must be associated with the private key used to sign the certificate or root certificate.

Manage Trusted Signing Certificates table
This table lists the trusted signing certificates. Make a selection from the menu bar then perform one of the following functions on the certificates:

- Click **Import** then select one of the following options:
  - From Remote Server to import the trusted signing certificate from a remote server.
  - **From Removable Media** to import the trusted signing certificate from removable media on the console.
  - **From Local File System** to import the trusted signing certificate from the file system on the system running the browser. This option is only available when you are accessing the console remotely.

  Note: The trusted signing certificates imported from removable media or from a remote browser must be Distinguished Encoding Rules (DER) encoded and might be supplied in binary or printable (Base64) encoding. If the certificate is provided in Base64 encoding, it must be bounded at the beginning by `----BEGIN CERTIFICATE----`, and must be bounded at the end by `----END CERTIFICATE----`.
- Click **Selected** then **Delete** to remove the selected trusted signing certificate.

Close
To return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Import Remote Certificate

Use this window to specify a host name (or IP address) and port to which an SSL connection should be established. The root certificate presented to this console by the target server will be trusted only for this SSL connection and will be presented as a certificate that can be imported as a trusted signing certificate (from this point on it will be trusted for all future SSL connections between this console and other machines).

IP/Host
Specify the IPv4 or IPv6 address or host name of the remote server.

Port
Specify the port number of the remote server.

OK
To import the certificate from the remote server with the specified information, click **OK**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Configure SSL Cipher Suites

Use this window to specify which SSL cipher suites are allowed to be used for SSL connections to this console. The SSL connections for which this set applies are those from remote web browsers or web services API programs connecting to the HMC API HTTP server. Also affected, are connections to the Java Message Service (JMS) message broker from Web Services API clients; including the use of Streaming Text Oriented Messaging Protocol (STOMP) and OpenWire protocols.

The toolbar at the top of the table contains icons used to select or arrange the columns in the table.

You can work with the table by using the table icons or **---Select Action---** drop-down list from the table tool bar. Filter the data you would like to appear in the table by manipulating the information in the table. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions:

Select All
The **Select All** icon allows you to select all the objects in the table.

Deselect All
The Deselect All icon allows you to deselect all the objects in the table.

Configure Columns
The **Configure Columns** icon allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns.

Cipher Suites
Specify the cipher suites that are to be allowed for SSL connections to this console.

OK
To save the selected cipher suites as those to be used for SSL connection to this console, click **OK**.

Default
To update the selected set of cipher suites with the default set, click **Default**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Console Internal Code

Accessing the Change Console Internal Code task

This task enables you to specify what you want to do with the internal code changes provided by the support system. This function is used when working with the Licensed Internal Code supplied with the Hardware Management Console. For information on changes to an object's internal code, see the **Change Internal Code** task.

A service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on your Hardware Management Console hard disk, it is recommended that you manage these changes only under the supervision of a service representative or with the assistance of your support system. Licensed internal code controls many of the operations available on the Hardware Management Console. Internal code changes may provide new operations, or correct or improve existing operations.

To change the internal code on the Hardware Management Console:

1. Open the **Change Console Internal Code** task. The Change Console Internal Code window is displayed.
2. Select one of the following options for managing the internal code, then click **OK**.

   Note: Verify that the term **Enabled** is displayed in the **Change Management Services** field. Change management services must be enabled for you to use options that manage the internal code changes stored on the Hardware Management Console hard disk.

   - Accept installed changes that were activated
   - Check dependencies
   - Install and activate changes that were retrieved. You can apply this to all applicable internal code changes, a subset of its applicable internal code changes, or specify a bundle level number for internal code changes.
   - Browse system and internal code information
   - Remove and activate changes
   - Retrieve internal code changes
     - If you select the **Retrieve code changes from the support system to removable media** option, you will need to specify an support system user ID and password to continue.
     - If you select the **Retrieve changes from FTP site to the Hardware Management Console** option, you will need to provide FTP site access information and you have the option to enable a secure data transfer.
   - Delete retrieved changes that were not installed

   If you select the **Retrieve internal code changes** option and then select **Retrieve code changes from the support system to removable media** option, you will need to specify a support system user ID and password to continue.

Change Console Internal Code

Use the **Change Console Internal Code** task to work with internal code changes for the console.

Licensed internal code, referred to also as internal code, controls many of the operations available on the console. Internal code changes may provide new internal code, or correct or improve existing internal code.

Note: A service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on the console, it is recommended that you manage these changes only under the supervision of a service representative or with the assistance of the support system.

Working with internal code changes

Use the **Change Console Internal Code** task to start any of the following actions for working with the internal code changes.

It is recommended to take the following actions while following the internal code change process:

- Accept previous internal code changes to make them permanent internal code.
- Retrieve new internal code changes from a source to the console.
- Install and activate new internal code changes to make them operational.

Or use the following actions for undoing internal code changes:

- Remove internal code changes to resolve problems.
- Delete internal code changes to attempt error recovery.

Change Management Services

The status of change management services determines whether you can change internal code at this time, and controls the availability of applicable options for changing internal code.

The field displays **Enabled** to indicate you can change internal code at this time.

Change Console Internal Code options

Select the option that describes the task you want to perform, then click **OK** to start the task.

Accept installed changes that were activated
To make operational internal code changes permanent, select **Accept installed changes that were activated**.

Check dependencies
To check whether internal code changes meet all the dependencies that must be met to use them with operations that change the internal code of the console, select **Check dependencies**.

Install and activate changes that were retrieved
To make retrieved internal code changes operational, select **Install and activate changes that were retrieved**.

Browse system and internal code information
To display information about the console and its internal code changes, select **Browse system and internal code information**.

Remove and activate changes
To undo the installation of installed internal code changes and to make their previous change levels operational, select **Remove and activate changes**.

Retrieve internal code changes
To copy internal code changes from a source to the console and to retrieve internal code changes from the support system to media, select **Retrieve internal code changes**.

Delete retrieved changes that were not installed
To erase retrieved internal code changes that are not yet installed or to erase removed internal code changes, select **Delete retrieved changes that were not installed**.

OK
To start the task that you have selected, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Change Management Services

This field indicates the status of change management services on the console. The status of the services determines whether you can change internal code at this time, and controls the availability of applicable options for changing internal code.

Status indicators

Enabled
Indicates you can change internal code at this time. The applicable options for changing internal code are available.

Disabled
Indicates you cannot change internal code at this time. All options for changing internal code are unavailable.

Note: Options that do not change internal code remain available. For example, the **Retrieve internal code changes** option remains available while change management services are disabled.

When change management services are disabled

Change management services cannot be enabled or disabled directly. Instead, the console sets the status of change management services following any operation that involves internal code changes.

The console disables change management services to prevent you from using internal code changes that differ, in any way, from the changes provided to you.

Internal code changes may be altered unintentionally by errors that occur while retrieving them. For example, the changes may not be copied correctly from the source to the Support Element.

Note: If change management services are disabled following an unsuccessful attempt to retrieve internal code changes, try to retrieve the changes again. If the error occurs again, and change management services remain disabled, report the error to your service representative.

Internal code changes may be altered intentionally by your service representative. For example, your service representative may apply a temporary internal code change to modify internal code changes stored on the console.

Note: If change management services are disabled, yet no errors have occurred, the disabled condition may be due to the use of a temporary internal code change. Your service representative must deactivate the temporary internal code change to enable change management services.

Accept installed changes that were activated

To make operational internal code changes permanent, select **Accept installed changes that were activated**.

Then click **OK** to start the task.

Consequences of using this option

Operational internal code changes include all installed changes that are currently activated.

Accepting operational internal code changes permanently changes the internal code of the console. Accepting the changes makes them internal code.

Accepting internal code changes cannot be undone. That is, accepted changes cannot be removed or deleted, and the internal code they changed cannot be restored.

Options for accepted changes

All options for changing internal code are no longer applicable to accepted internal code changes.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are installed and currently activated.

Otherwise, the option is unavailable.

Check dependencies

To check whether internal code changes meet all the dependencies that must be met to use them with operations that change the internal code of the console, select **Check dependencies**.

Then click **OK** to start the task.

Note: Ordinarily, only a service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the console's internal code. If you are not following a service procedure, it is recommended that you check dependencies only with assistance from product support, provided through your service representative or support system.

About internal code change dependencies

Internal code is organized into units called *Engineering Changes (ECs)*, which are also referred to as *streams*.

Internal code changes may provide new internal code, or correct or improve existing internal code, for particular streams. If internal code changes for multiple streams are needed, together, to complete an addition, correction, or improvement of the console's internal code, then the internal code changes have *dependencies*. For example, if Engineering Change (EC) E12345, change level 001, must be installed and activated before EC E54321 level 005 can be installed and activated, then EC E54321 level 005 has a dependency on EC E12345 level 001.

The dependencies of internal code changes are designated by when the changes are created. After internal code changes are retrieved to the console, their dependencies, if any, are checked automatically whenever you start an operation that will change the console's internal code. Such an operation will be attempted only if all dependencies of the internal code changes are met.

Manually checking dependencies

This option provides a means for manually checking the dependencies of internal code changes. Manually checking dependencies is useful:

- Before you perform an operation for changing the console's internal code.

  By manually checking the dependencies of internal code changes you intend to select while performing the operation, you may get a detailed list of the dependencies that would not be met, but which you must meet before or while actually attempting the operation.

  Note: This is especially important if you intend to use specific internal code changes, rather than all changes, while performing the operation. Using specific changes increases the possibility of **not** specifying one or more dependencies of the specific changes.
- After automatic dependency checking notifies you, upon attempting an operation, that one or more dependencies are not met.

  By manually checking the dependencies of internal code changes you selected while attempting the operation, you get a detailed list of the dependencies that were not met, but which you must meet before or while attempting the operation again.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are eligible for being either accepted, installed, or removed.

Otherwise, the option is unavailable.

Install and activate changes that were retrieved

To make retrieved internal code changes operational, select **Install and activate changes that were retrieved**.

Then click **OK** to start the task.

Consequences of using this option

Installing retrieved internal code changes makes them eligible for being activated. Activating installed changes makes them operational.

But installing and activating internal code changes does **not** permanently change the internal code of the console. Instead, installing changes makes them only temporarily eligible for being activated. Then activating the installed changes now, and any subsequent activation of the console, makes the changes operational instead of the internal code they changed.

Installed changes can be removed, if necessary, to restore the internal code they changed.

Options for installed and activated changes

After you install and activate internal code changes, the following options for changing internal code are applicable to them:

- Accept installed changes that were activated

  Use this option to make operational internal code changes permanent.
- Remove and activate changes

  Use this option to undo the installation of installed internal code changes and to make their previous change levels operational.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are retrieved or removed.

Otherwise, the option is unavailable.

Browse system and internal code information

To display information about the console and its internal code changes, select **Browse system and internal code information**.

Then click **OK** to start the task.

About the information

Information about the console identifies its machine type, model number, and serial number.

Information about the internal code changes is a record of tasks performed on the changes. For each internal code change, the information identifies:

- Its Engineering Change (EC) number.
- The change level most recently retrieved.
- The change level most recently installed.
- The change level most recently activated.
- The change level most recently accepted.

- The lowest change level that can be activated after removing installed change levels.
- Additional details include the date and time each task was most recently performed.

Using the information

The information may assist you with planning and managing internal code changes. For example, review the information to either:

- Determine whether the console is operating with your latest available change levels.
- Determine which tasks you must perform next to make the console operate with your latest available change levels.

Remove and activate changes

To undo the installation of installed internal code changes and to make their previous change levels operational, select **Remove and activate changes**.

Then click **OK** to start the task.

Consequences of using this option

Removing installed internal code changes makes them ineligible for being activated, and makes their previous change levels eligible instead. Activating the previous change levels makes them operational.

But removing internal code changes and activating previous change levels does **not** permanently change the internal code of the console. Instead, removing changes restores the internal code they changed. Then activating without the removed changes now, and any subsequent activation of the console, makes the restored internal code operational.

Removed changes are not erased. They remain stored on the console and can be installed again at any time.

Options for removed changes

After you remove internal code changes, the following options for changing internal code are applicable to them:

- Install and activate changes that were retrieved

  Use this option to make removed internal code changes operational again.
- Delete retrieved changes that were not installed

  Use this option to erase removed internal code changes if an error occurred while installing or activating them.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are installed.

Otherwise, the option is unavailable.

Retrieve internal code changes

To copy internal code changes from a source to the console and to retrieve internal code changes from the support system to media, select **Retrieve internal code changes**.

Then click **OK** to start the task.

Consequences of using this option

Retrieving internal code changes makes them available for being installed and activated.

But retrieving internal code changes does **not** change the internal code of the console. It only copies them from their source to the console.

Options for retrieved changes

After you retrieve internal code changes, the following options for changing internal code are applicable to them:

- Install and activate changes that were retrieved

  Use this option to make retrieved internal code changes operational.
- Delete retrieved changes that were not installed

  Use this option to erase retrieved internal code changes if an error occurred while retrieving them.

Delete retrieved changes that were not installed

To erase retrieved internal code changes that are not yet installed and to erase removed internal code changes, select **Delete retrieved changes that were not installed**.

Then click **OK** to start the task.

Delete retrieved internal code changes if an error occurred while retrieving them. Remove then delete installed internal code changes if an error occurred while installing or activating them.

Consequences of using this option

Deleting internal code changes allows retrieving the changes over again if errors occurred during previous attempts to retrieve, install, or activate the changes.

Deleting internal code changes does **not** change the internal code of the console; it erases only retrieved and removed internal code changes from the console.

Options for deleted changes

All options for changing internal code are no longer applicable to deleted internal code changes. But if the source of the internal code changes is still available, the following option for changing internal code is applicable to them:

- Retrieve internal code changes

  Use this option to copy internal code changes again from the source to the console.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are retrieved or removed.

Otherwise, the option is unavailable.

Activate Internal Code Change Confirmation

Use this window to activate the internal code changes that are currently installed on the console.

Yes
To activate the internal code changes that are currently installed on the console, click **Yes**.

No
If you do not want to activate the internal code changes that are currently installed on the console, click **No**.

Help
To display help for the current window, click **Help**.

Specify Internal Code Changes

Use this window to identify the specific internal code changes you want the task you selected to apply to.

Identify the changes by their Engineering Change (EC) numbers and change levels.

Note: You will need the assistance of your service representative or your support system to identify a specific internal code change by its EC number and change level.

Engineering Change table
Complete one row of fields for each internal code change you want to apply the task to, then click **OK** to continue the task.

Note: Fields are initialized with default entries for EC numbers and change levels derived from previous entries, if any. If you do not want to use the default entries, click **Clear** to discard them. All entry fields will be cleared to allow you to specify other EC numbers and change levels.

EC Number
Specify the EC number of the internal code change you want the task you selected to apply to.

Then use the applicable fields in the same row to identify the change levels of the internal code change you want the task to apply to.

Starting Change Level and Ending Change Level
Enter the numbers of the first and last change levels you want to retrieve from the support system to a removable media. Or enter the starting change level, then enter **ALL** for the ending change level to retrieve all change levels.

The task will retrieve the specified range of change levels of the internal code changes identified by the adjacent EC number.

OK
To continue the selected action and apply it to the specific internal code changes identified by the EC numbers and change levels, click **OK**.

Clear
To remove all entry fields on the window by discarding the EC numbers and change levels specified the last time the window was used, click **Clear**.

Cancel

To close the window and return to the window from which you selected the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Specify Internal Code Changes

Use this window to identify the specific internal code changes you want the task you selected to apply to.

Identify the changes by their Engineering Change (EC) numbers and change levels.

Note: You will need the assistance of your service representative or your support system to identify a specific internal code change by its EC number and change level.

Select the type of operation
If you chose to **Remove and activate changes** or **Install and activate changes that were retrieved** then you can choose the type of operation you prefer by selecting **Do the changes concurrently** or **Do the changes disruptively**.

Engineering Change table
Complete one row of fields for each internal code change you want to apply the task to, then click **OK** to continue the task.

Note: Fields are initialized with default entries for EC numbers and change levels derived from previous entries, if any. If you do not want to use the default entries, click **Clear** to discard them. All entry fields will be cleared to allow entering other EC numbers and change levels.

EC Number
Enter the EC number of the internal code change you want the task you selected to apply to.

Then use the applicable field in the same row to identify the change levels of the internal code change you want the task to apply to.

Change Level
Specify the number of the last change level you want the task you selected to apply to, or enter **ALL** to apply the selected task to all applicable change levels.

The task will be applied to applicable change levels of the internal code change, identified by the adjacent EC number, from the current applicable change level to the change level you specify.

The applicable change levels and their range depends on the action you selected:

Accept
Applies to installed and activated change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Accept
Applies to installed and activated change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Install
Applies to retrieved change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Remove
Applies to installed change levels in the range from the highest change level down to and including the change level you specify.

Delete
Applies to retrieved and removed change levels in the range from the highest change level down to and including the change level you specify.

Install
Applies to retrieved change levels in the range from the lowest change level up to and including the change level you specify.

Remove
Applies to installed change levels in the range from the highest change level down to and including the change level you specify.

Retrieve
Applies to change levels available from the source in the range from the lowest change level up to and including the change level you specify.

Note: You will need the assistance of your service representative or your support system to identify a specific internal code change by its EC number and change level.

Include internal code changes which will inhibit the Concurrent Upgrade Engineering Changes (EC) task from being used to apply the next Licensed Internal Code EC level
This option is only available if you chose to **Install and activate changes that were retrieved** and if there are retrieved changes that would break the **Concurrent Upgrade Engineering Changes** task's maximum change level requirements if the changes were installed.

OK
To continue the selected task and apply it to the specific internal code changes identified by the EC numbers and change levels, click **OK**.

Clear
To remove all entry fields on the window by discarding the EC numbers and change levels specified the last time the window was used, click **Clear**.

Cancel

To close the window and return to the window from which you selected the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Internal Code Changes

Use this window to indicate whether you want the task you selected to apply to all or a subset of its applicable internal code changes.

Ordinarily, you should use all applicable internal code changes each time you use any task that changes the internal code. But you can use subsets of changes instead, if it meets your particular circumstances or needs for changing the internal code. For example, you may want to use specific changes:

- To install only some changes, but not other changes, to preserve internal code you do not want to change.
- To remove only some changes if they caused problems or did not operate satisfactorily, while letting other changes remain installed.

Important: It is recommended that you use specific internal code changes only under the supervision of a service representative or with the assistance of the support system.

All internal code changes
To apply the selected task to all its applicable internal code changes, select **All internal code changes**.

Specific internal code changes
To apply the selected task to a subset of its applicable internal code changes, select **Specific internal code changes**.

Then, on the subsequent window, identify the changes by their Engineering Change (EC) numbers and change levels.

Note: You will need the assistance of your service representative or your support system to identify specific changes.

If this option is not available when you are using the **Retrieve Internal Code** task, then one or more of the following conditions were met:

- More than one object was selected.
- The object selected was not a System z10 and later.
- The **Retrieve code changes from all Hardware Management Consoles also** was selected (a check mark appears).

Bundle of internal code changes
To apply a specified bundle level number for internal code changes, select **Bundle of internal code changes**.

OK
To continue the selected task and apply it to the internal code changes described by your selection, click **OK**.

Cancel
To close the window and return to the window from which you selected the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Check Dependencies Failed

This window indicates one or more dependencies were not met for using the selected operation and internal code changes to change the internal code of the console. The window also lists messages that describe each dependency that was not met. Each message includes:

- A description of the dependency.
- The operation you must perform to meet the dependency.

- The Engineering Change (EC) number and change level of each internal code change you can or must use with the operation to meet the dependency.

Upon returning to the service procedure you are following, you can proceed with its instructions and refer to its recovery actions for meeting failed dependencies described by the messages.

Important: Ordinarily, only a service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the console's internal code. If you are not following a service procedure, it is recommended that you check dependencies only with assistance from product support, provided through your service representative or support system.

Engineering Change table
These entries indicate that one or more dependencies were not met for using the selected operation and internal code changes to change the internal code of the console.

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Check Dependencies

Use this window to check whether internal code changes meet all the dependencies that must be met to use them with operations that change the internal code of the console.

Note: Ordinarily, only a service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the console's internal code. If you are not following a service procedure, it is recommended that you check dependencies only with assistance from product support, provided through your service representative or support system.

Internal code is organized into units call *Engineering Changes (ECs)*, which are referred to also as *streams*.

Internal code changes may provide new internal code, or correct or improve existing internal code, for particular streams. If internal code changes for multiple streams are needed, together, to complete an addition, correction, or improvement of the console's internal code, then the internal code changes have *dependencies*. For example, if Engineering Change (EC) E12345, change level 001, must be installed and activated before EC E54321 level 005 can be installed and activated, then EC E54321 level 005 has a dependency on EC E12345 level 001.

The dependencies of internal code changes are designated by when the changes are created. After internal code changes are retrieved to the console, their dependencies, if any, are checked automatically whenever you start an operation that will change the console's internal code. Such an operation will be attempted only if all dependencies of the internal code changes are met.

This option provides a means for manually checking the dependencies of internal code changes. Manually checking dependencies is useful:

- Before you perform an operation for changing the console's internal code.

  By manually checking the dependencies of internal code changes you intend to select while performing the operation, you may get a detailed list of the dependencies that would not be met, but which you must meet before or while actually attempting the operation.

  Note: This is especially important if you intend to use specific internal code changes, rather than all changes, while performing the operation. Using specific changes increases the possibility of not specifying one or more dependencies of the specific changes.
- After automatic dependency checking notifies you, upon attempting an operation, that one or more dependencies are not met.

  By manually checking the dependencies of internal code changes you selected while attempting the operation, you get a detailed list of the dependencies that were not met, but which you must meet before or while attempting the operation again.

Dependency checking options

To check dependencies of internal code changes manually, select the option that describes the operation and internal code changes for which you want dependencies checked, then click **OK**.

Install and activate of all changes
To check the dependencies that must be met to install and activate all internal code changes, select **Install and activate of all changes**.

Remove and activate of all changes
To check the dependencies that must be met to remove and activate all internal code changes, select **Remove and activate of all changes**.

Install and activate of specific changes
To check the dependencies that must be met to install and activate specific internal code changes, select **Install and activate of specific changes**.

Remove and activate of specific changes
To check the dependencies that must be met to remove and activate specific internal code changes, select **Remove and activate of specific changes**.

Accept specific changes
To check the dependencies that must be met to accept specific internal code changes, select **Accept specific changes**.

OK
To start the dependency checking described by your selection, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Install and activate of all changes

To check the dependencies that must be met to install and activate all internal code changes, select **Install and activate of all changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by installing and activating all internal code changes. But you can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes that are eligible for being installed and activated. That is, dependencies will be checked only for internal code changes that were retrieved to the console, but are not currently installed.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually installing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually installing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Availability of this option

This option is available while internal code changes are eligible for being installed. That is, this option is available while any changes are retrieved.

Otherwise, the option is unavailable.

Remove and activate of all changes

To check the dependencies that must be met to remove and activate all internal code changes, select **Remove and activate of all changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by removing and activating all internal code changes. But you can use this choice to manually perform the same dependency checking now, without removing and activating the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes that are eligible for being removed and activated. That is, dependencies will be checked only for internal code changes that are currently installed.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually removing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually removing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Availability of this option

This option is available while internal code changes are eligible for being removed. That is, this option is available while any changes are retrieved.

Otherwise, the option is unavailable.

Install and activate of specific changes

To check the dependencies that must be met to install and activate specific internal code changes, select **Install and activate of specific changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by installing and activating specific internal code changes. But you can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being installed and activated. That is, dependencies will be checked only for specified internal code changes that were retrieved to the console, but are not currently installed.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually installing and activating the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually installing and activating the specific internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being installed and activated, but it is recommended that you install and activate all retrieved internal code changes instead. Using specific changes risks installing and activating an untested combination of changes.

Availability of this option

This option is available while any internal code changes are eligible for being installed. That is, this option is available while any changes are retrieved.

Otherwise, the option is unavailable.

Remove and activate of specific changes

To check the dependencies that must be met to remove and activate specific internal code changes, select **Remove and activate of specific changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by removing and activating specific internal code changes. But you can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being removed and activated. That is, dependencies will be checked only for specified internal code changes that are currently installed.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually removing and activating the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually removing and activating the specific internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being removed and activated, but it is recommended that you remove and activate all installed internal code changes instead. Using specific changes risks removing and activating an untested combination of changes.

Availability of this option

This option is available while any internal code changes are eligible for being removed. That is, this option is available while any changes are installed.

Otherwise, the option is unavailable.

Accept specific changes

To check the dependencies that must be met to accept specific internal code changes, select **Accept specific changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by accepting specific internal code changes. But you can use this choice to manually perform the same dependency checking now, without accepting the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being accepted. That is, dependencies will be checked only for specified internal code changes that are currently installed and activated.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually accepting the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually accepting the specific internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being accepted, but it is recommended that you accept all installed and activated internal code changes instead. Using specific changes risks accepting an untested combination of changes.

Availability of this option

This option is available while any internal code changes are eligible for being accepted. That is, this option is available while any changes are installed and activated.

Otherwise, the option is unavailable.

Retrieve Internal Code Changes

Use this window to copy internal code changes from their source to the console and to copy the internal code changes from the support system to a removable media.

Retrieve Internal Code Changes options

Select the option that describes the action you want to perform, then click **OK** to start the action.

Retrieve code changes from removable media to the console
: To copy internal code change from removable media to the console, select **Retrieve code changes from removable media to the console**.

Retrieve code changes from the support system to the console
: To copy internal code changes from the support system to the console, select **Retrieve code changes from the support system to the console**.

Retrieve code changes from FTP site to the console
To copy internal code changes from a designated FTP site to the console, select **Retrieve code changes from FTP site to the console**.

Retrieve code changes from the support system to removable media
To copy internal code changes from the support system to removable media to make it a source of internal code changes, select **Retrieve code changes from the support system to removable media**. Prepare media for use with this option by using the **Format Media** task.

OK
To start the task that you selected, click **OK**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Retrieve code changes from removable media to the console

To copy internal code changes from removable media, select **Retrieve code changes from removable media to the console**.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Use this option when you have removable media that has internal code changes stored on it. For example, use this option when either:

- The support system has delivered the internal code changes to you on removable media.
- You used another console to copy internal code changes from the support system to removable media.

Retrieve code changes from the support system to the console

To copy internal code changes from the support system to the console, select **Retrieve code changes from the support system to the console**.

Use this option when:

- This console is configured and enabled for communicating with the support system.
- And after you are notified that new internal code changes are available from the support system.

Retrieve code changes from FTP site to the console

To copy internal code changes from an FTP site to the console, select **Retrieve code changes from FTP site to the console**.

This option allows you to enter the FTP site address and account access information.

Retrieve code changes from support system to removable media

To copy internal code changes from the support system to removable media, select **Retrieve code changes from support system to removable media**.

You can then use the removable media as an alternative source for retrieving internal code changes to another console.

Note: It is recommended that you use this option only under the supervision of a service representative or with the assistance of the support system.

To continue with this option, click **OK**. The **Support System Access Information** window is displayed. Specify a support system user ID and password to proceed.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Use this option when:

- This console is configured and enabled for communicating with the support system.
- And after you have been notified that new internal code changes are available from the support system.
- And if you need to distribute internal code changes to other consoles that cannot use the support system as a source.

FTP Server Information / Configure Backup Settings

Use this window to configure FTP settings when you use an external server to back up your files or when you are transferring data for the following tasks:

- Analyze Console Internal Code
- Change Console Internal Code
- Retrieve Internal Code (targeting an object)
- Backup Critical Data
- Save Upgrade Data

Host name
Specify the host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To apply this information, click **OK**.

Clear
To remove all information from the input fields, click **Clear**.

Cancel
To close the window without providing information, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Accept

Use this window to confirm or cancel your request to accept operational internal code changes.

Accepting operational internal code changes makes them permanent internal code.

At this point in the task, **operational internal code changes** are:

- All changes you installed that are currently activated.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Attention: Accepting internal code changes permanently changes the internal code of the console. The process cannot be undone. That is, accepted internal code changes cannot be removed to restore their previous change levels.

Internal code change process

The window displays the summary of the internal code change process that are recommended. Accepting internal code changes is the second step (step **B**) of the process. Review the process before continuing.

Note: You should cancel your request to accept internal code changes in these cases:

- If you have not completed the third or fourth steps (steps **C** or **D**) of the process for **previous** internal code changes. That is:
  - If you have not yet retrieved all **previous** internal code changes provided to you by the support system.
  - Or if you did not install and activate the previously retrieved internal code changes after checking their dependencies.
- Or if you have not completed the first step (step **A**) of the internal code change process upon receiving new internal code changes. That is, if you have not yet performed a backup of critical data of the console.

You should confirm your request to accept internal code changes only after completing the recommended steps described above.

Accept
To confirm your request to accept operational internal code changes, click **Accept**.

Cancel
To cancel your request and close the window without accepting the operational changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Retrieve from a source to console

Use this window to confirm or cancel your request to retrieve internal code changes from their source to the console.

Retrieving internal code changes makes them available for being installed and activated.

At this point in the task, **internal code changes** are:

- All changes available from the source you selected.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Internal code change process

The window displays a summary of the internal code change process. Retrieving internal code changes is the third step (step **C**) of the process. Review the process before continuing.

Note: You should cancel your request to retrieve internal code changes in these cases:

- If you have not completed the last step (step **D**) of the process for **previous** internal code changes. That is, if you have not yet installed and activated all **previously** retrieved internal code changes.
- If you did not perform the first or second steps (steps **A** or **B**) of the process upon receiving the new internal code changes. That is:
  - If you have not yet performed a backup of critical data of the console.
  - Or if you have not yet accepted all **previously** installed and activated internal code changes.

You should confirm your request to retrieve new internal code changes only after completing the recommended steps described above.

Retrieve
To confirm your request to retrieve internal code changes from their source to the console, click **Retrieve**.

Cancel
To cancel your request and close the window without retrieving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Retrieve from a support system to console

Use this window to confirm or cancel your request to retrieve internal code changes from their source to the console.

Retrieving internal code changes makes them available for being installed and activated.

At this point in the task, **internal code changes** are:

- All changes available from the source you selected.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Internal code change process

The window displays a summary of the recommended internal code change process. Retrieving internal code changes is the third step (step **C**) of the process. Review the process before continuing.

Note: You should cancel your request to retrieve internal code changes in these cases:

- If you have not completed the last step (step **D**) of the process for **previous** internal code changes. That is, if you have not yet installed and activated all **previously** retrieved internal code changes.
- If you did not perform the first or second steps (steps **A** or **B**) of the process upon receiving the new internal code changes. That is:
  - If you have not yet performed a backup of critical data of the console.
  - Or if you have not yet accepted all **previously** installed and activated internal code changes.

You should confirm your request to retrieve new internal code changes only after completing the recommended steps described above.

Retrieve
To confirm your request to retrieve internal code changes from their source to the console, click **Retrieve**.

Cancel
To cancel your request and close the window without retrieving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Retrieve from the support system to source

Use this window to confirm or cancel your request to retrieve internal code changes to a source.

Retrieving internal code changes makes them available for being installed and activated.

At this point in the task, **internal code changes** are:

- All changes available from the source you selected.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Retrieve
To confirm your request to retrieve internal code changes from the support system to a source, click **Retrieve**.

Cancel
To cancel your request, and close the window without retrieving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Install and Activate

Use this window to confirm or cancel your request to install and activate the retrieved internal code changes.

Installing and activating the retrieved changes makes them operational.

At this point in the task, **retrieved internal code changes** are:

- All changes you retrieved from their source to the console. That is, all changes that are eligible for being installed.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Internal code change process

The window displays a summary of the internal code recommended change process. Installing and activating internal code changes is the last step (step **D**) of the process. Review the process before continuing.

Important: You should cancel your request to install and activate internal code changes if you did not perform the preceding steps (steps **A** through **C**) of the process upon receiving the new internal code changes. That is:

- If you have not yet performed a backup of critical data of the console.
- Or if you have not yet accepted all **previously** installed and activated internal code changes.
- Or if you have not yet retrieved the new internal code changes provided to you by the support system.

You should confirm your request to install and activate new internal code changes only after completing the recommended steps described above.

Install and Activate
To confirm your request to install and activate the retrieved internal code changes, click **Install and Activate**.

Cancel
To cancel your request, and close the window without installing or activating the retrieved changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Remove and Activate

Use this window to confirm or cancel your request to remove the installed internal code changes and to activate their previous change levels.

Removing the installed changes and activating their previous change levels makes the previous levels operational. Any subsequent initialization of the console also will make the previous change levels operational.

At this point in the task, **installed internal code changes** are:

- All changes you installed, but have not yet accepted or removed. That is, all changes that are activated or eligible for being activated.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Remove and Activate
To confirm your request to remove and activate the installed internal code changes, click **Remove and Activate**.

Cancel
To cancel your request, and close the window without removing the installed changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Delete

Use this window to confirm or cancel your request to delete:

- Retrieved internal code changes.
- Removed internal code changes.

At this point in the task:

- **Retrieved internal code changes** are all changes you retrieved from their source to the console, but have not yet installed.
- And **removed internal code changes** are all retrieved changes you installed, but then removed to undo their installation.
- But both are limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Important: Deleting internal code changes erases them from the console. The process cannot be undone. However, deleted internal code changes can be retrieved again from their source to the console.

Delete
To confirm your request and delete the internal code changes, click **Delete**.

Cancel
To cancel your request, and close the window without deleting the internal code changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Specify Bundle to Install

Use this window to provide a bundle level number that you want installed.

Bundle Level
Specify the bundle level number in the input area.

OK
To proceed with installing the specified bundle level number, click **OK**.

Cancel

To return to the previous window without providing a bundle level number, click **Cancel**.

Help

To display help for the current window, click **Help**.

Change Internal Code

Accessing the Change Internal Code task

Note: Change Internal Code is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task enables you to modify system internal code which may provide new operations, or correct or improve existing operations. Also, any Support Element at Version 2.10.0 or later must use this task for all change internal code functions.

You can modify the internal code of:

- All defined systems
- All systems in a user-defined group
- Selected individual system or systems.

You can:

- Accept installed changes that were activated
- Install and activate changes that were retrieved. You can apply this to all applicable internal code changes, a subset of its applicable internal code changes, or specify a bundle level number for internal code changes.
- Browse system and internal code information
- Remove and activate changes
- Delete all retrieved changes that were not installed.

A service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on your hard disk, it is recommended that you manage these changes only under the supervision of a service representative or with the assistance of your support system.

Certain licensed internal code changes may require the MRU to shut down during the activation of the change. This is normal for these changes. This could cause a slight degradation in system performance during the time the MRU is shut down. After activation is complete, the MRU will be turned on again, and normal performance will be resumed.

To change the system internal code:

1. Select one or more systems (servers).
2. Open the **Change Internal Code** task. The Change Internal Code window is displayed.
3. Click the option you want to perform and then click **OK**.
4. Follow the instructions on the subsequent windows to complete the task.

Change Internal Code

Use this window to start tasks for working with internal code changes for the selected systems.

Licensed internal code, referred to also as internal code, controls many of the operations available on its system. Internal code changes may provide new internal code, or correct or improve existing internal code.

Important: A service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on Support Elements, it is recommended that you manage these

changes only under the supervision of a service representative or with the assistance of the support system.

Change Internal Code Options

Select the option that describes the task you want to perform, then click **OK** to start the task.

Accept installed changes that were activated
To make operational internal code changes permanent, select **Accept installed changes that were activated.**

Install and activate changes that were retrieved
To make retrieved internal code changes operational, select **Install and activate changes that were retrieved**.

Browse system and internal code information
To display information about each selected system and its internal code changes, select **Browse system and internal code information**.

Remove and activate changes
To undo the installation of installed internal code changes and to make their previous change levels operational, select **Remove and activate changes**.

Delete all retrieved changes that were not installed
To erase retrieved internal code changes that are not yet installed or to erase removed internal code changes, select **Delete all retrieved changes that were not installed**.

OK
To start the task that you have selected, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Tasks

Use this window to start the following tasks for changing internal code. For an example, with step-by-step instructions, select one of the following tasks.

- Accepting internal code changes to make them permanent internal code.
- Installing and activating internal code changes to make them operational.
- Removing internal code changes to resolve problems.
- Deleting internal code changes to attempt error recovery.

Note: The options for changing internal code from a Hardware Management Console apply to **all** applicable internal code changes available on the Support Elements. To work with specific internal code changes:

1. You must work with one system at a time, and change its internal code by using its Support Element console, either directly or by using **Single Object Operations** for the system from a Hardware Management Console.
2. You will need the assistance of your service representative or your support system to identify specific changes by their Engineering Change (EC) numbers and change levels.

You can find more detailed help on the following elements of this window:

Accept installed changes that were activated

To make operational internal code changes permanent, select **Accept installed changes that were activated**.

To start the task, click **OK**.

Consequences of using this option

Operational internal code changes include all installed changes that are currently activated.

Accepting operational internal code changes permanently changes the internal code of each selected system. Accepting the changes makes them internal code.

Accepting internal code changes cannot be undone. That is, accepted changes cannot be removed or deleted, and the internal code they changed cannot be restored.

Options for accepted changes

All options for changing internal code are no longer applicable to accepted internal code changes.

Install and activate changes that were retrieved

To make retrieved internal code changes operational, select **Install and activate changes that were retrieved**.

To start the task, click **OK**.

Note: If the retrieved internal code changes include both concurrent and disruptive changes, then a subsequent window will provide you with options for indicating which changes you want to install.

Consequences of using this option

Installing retrieved internal code changes makes them eligible for being activated. Activating installed changes makes them operational.

But installing and activating internal code changes does **not** permanently change the internal code of the selected systems. Instead, installing changes makes them only temporarily eligible for being activated. Then activating the installed changes now, and any subsequent activation of the selected systems, makes the changes operational instead of the internal code they changed.

Installed changes can be removed, if necessary, to restore the internal code they changed.

Options for installed and activated changes

After you install and activate internal code changes, the following options for changing internal code are applicable to them:

- Accept installed changes that were activated

  Use this option to make operational internal code changes permanent.
- Remove and activate changes

  Use this option to undo the installation of installed internal code changes and to make their previous change levels operational.

Browse system and internal code information

To display information about each selected system and its internal code changes, select **Browse system and internal code information**.

To start the task, click **OK**.

Machine information

Information about a system identifies its machine type, model number, serial number, and communication status.

Internal Code Change Information

Information about the internal code changes is a record of tasks performed on the changes. For each internal code change, the information identifies:

- Its Engineering Change (EC) number.
- The change level most recently retrieved.
- The highest retrieved change level that can be installed and activated concurrently.
- The change level most recently installed.
- The change level most recently activated.
- The change level most recently accepted.
- The lowest installed change level that can be removed such that the remaining installed change levels can be activated concurrently.
- The lowest change level that can be activated after removing installed change levels.
- Additional details include the date and time each task was most recently performed.

Using the information

The information may assist you with planning and managing internal code changes. For example, review the information to either:

- Determine whether a system is operating with your latest available change levels.
- Determine which tasks you must perform next to make a system operate with your latest available change levels.

Remove and activate changes

To undo the installation of installed internal code changes and to make their previous change levels operational, select **Remove and activate changes**.

To start the task, click **OK**.

Note: If the installed internal code changes include both concurrent and disruptive changes, then a subsequent window will provide you with options for indicating which changes you want to remove.

Consequences of using this option

Removing installed internal code changes makes them ineligible for being activated, and makes their previous change levels eligible instead. Activating the previous change levels makes them operational.

But removing internal code changes and activating previous change levels does **not** permanently change the internal code of the selected systems. Instead, removing changes restores the internal code they changed. Then activating without the removed changes now, and any subsequent activation of the selected systems, makes the restored internal code operational.

Removed changes are not erased. They remain stored on the systems and can be installed again at any time.

Options for removed changes

After you remove internal code changes, the following options for changing internal code are applicable to them:

- Install and activate changes that were retrieved

  Use this option to make removed internal code changes operational again.
- Delete all retrieved changes that were not installed

  Use this option to erase removed internal code changes if an error occurred while installing or activating them.

Delete retrieved changes that were not installed

To erase retrieved internal code changes that are not yet installed or to erase removed internal code changes, select **Delete retrieved changes that were not installed**.

To start the task, click **OK**.

Delete retrieved internal code changes if an error occurred while retrieving them. Remove then delete installed internal code changes if an error occurred while installing or activating them.

Consequences of using this option

Deleting internal code changes allows retrieving the changes over again if errors occurred during previous attempts to retrieve, install, or activate the changes.

But deleting internal code changes does **not** change the internal code of the selected systems. It erases only retrieved and removed internal code changes from the systems.

Options for deleted changes

All options for changing internal code are no longer applicable to deleted internal code changes.

Changing internal code instructions

Prerequisites: To change internal code:

1. You must be logged on a Hardware Management Console in at least the advanced operator user mode.

After you satisfy the prerequisites, follow these instructions to start a task for changing internal code:

From the **Hardware Management Console Workplace**:

1. Locate the task:
   a. Open the **Task List** view.

      This opens the **Task List Work Area**.
   b. Open **Change Management** tasks.

      This opens the **Change Management** task list on the right side of the workplace. The list contains the task you will start: **Change Internal Code**.
2. Locate the target systems:
   a. Open the **Groups** view.

      This opens the **Groups Work Area**.
   b. Select a group of systems if you want to change the internal code of all systems in the group.

      Otherwise, to change the internal code of one or more particular systems:

      1) Open the **system** group or any other group that contains the systems you want to work with.

         This opens the group's work area. The area contains the target systems.
      2) Select each system for which you want to change internal code.
3. To start the task after selecting the target group or target systems, double-click on **Change Internal Code**.

   This opens the **Change Internal Code** window. It provides controls for changing internal code.
4. After you start the task, request help for the controls or the window for additional information about using them to change internal code.

You can find more information on the following change internal code instructions:

Accepting internal code changes

Accept operational internal code changes to make them permanent. That is, accept operational internal code changes to make them internal code.

Operational internal code changes include all installed changes that are currently activated.

Important: Refer to the instructions in the following example for general guidance. Then, while performing the task, request help for any window while it displays for more information about using it to complete the task.

Example

The following example shows the steps for accepting all installed internal code changes that are currently activated.

From the **Hardware Management Console Workplace:**

1. Select the target systems or system group, and start the task: **Change Internal Code**.

   This opens the **Change Internal Code** window.

   From the **Change Internal Code** window:
2. Select **Accept installed changes that were activated**, then click **OK**.

   This opens the **Confirm the Action** window.

   From the **Confirm the Action** window:
3. Click **Accept** to begin the process.
4. Wait until a message indicates the process is complete, then click **OK** to close the message.

   This completes the task.

Installing and activating internal code changes

Install and activate retrieved internal code changes to make them operational.

Important: Instructions for installing and activating internal code changes will vary with the set of changes you want to install, whether you want to activate them immediately, and how you want to activate them. Each example below provides instructions for a particular situation. Your situation may be different; refer to the instructions for general guidance. Then, while performing the task, request help for any window while it displays for more information about using it to complete the task.

Example 1

The following example shows the steps for:

- Installing all retrieved internal code changes.
- Activating the changes **immediately** and **concurrently**.

From the **Hardware Management Console Workplace**:

1. Select the target systems or system group, and start the task: **Change Internal Code**.

   This opens the **Change Internal Code** window.

   From the **Change Internal Code** window:
2. Select **Install and activate changes that were retrieved**, then click **OK**.

   This opens the **Request Selection** window.

   From the **Request Selection** window:
3. Select **Do all concurrent changes only**, then click **Install and Activate**.

   This opens the **Confirm the Action** window.

From the **Confirm the Action** window:

4. Click **Install and Activate Concurrently** to begin the process.

   This opens the **Change Internal Code Progress** window.

   From the **Change Internal Code Progress** window:

5. Wait until the window indicates the process is complete, then click **OK** to close the window.

   This completes the task.

Example 2

The following example shows the steps for:

- Installing all retrieved internal code changes.
- Activating the change **immediately** and **disruptively**.

From the **Hardware Management Console Workplace**:

1. Select the target systems or system group, and start the task: **Change Internal Code**.

   This opens the **Change Internal Code** window.

   From the **Change Internal Code** window:

2. Select **Install and activate changes that were retrieved**, then click **OK**.

   This opens the **Request Selection** window.

   From the **Request Selection** window:

3. Select **Do all changes even if they are disruptive**, then click **Install and Activate**.

   This opens the **Confirm this Disruptive Action** window.

   From the **Confirm this Disruptive Action** window:

4. Click **Install and Activate Disruptively** to begin the process.

   This opens the **Change Internal Code Progress** window.

   From the **Change Internal Code Progress** window:

5. Wait until the window indicates the process is complete, then click **OK** to close the window.

   This completes the task.

Removing internal code changes and activating previous change levels

Remove installed internal code changes and activate their previous change levels to make the previous levels operational.

Remove internal code changes only if it is necessary to resolve a problem that occurred after installing and activating the changes.

Important: Instructions for removing internal code changes and activating their previous change levels will vary with the set of changes you want to remove, whether you want to activate the previous levels immediately, and how you want to activate them. Each example below provides instructions for a particular situation. Your situation may be different; refer to the instructions for general guidance. Then, while performing the task, request help for any window while it displays for more information about using it to complete the task.

Example 1

The following example shows the steps for:

- Removing all installed internal code changes.
- Activating their previous change levels **immediately** and **concurrently**.

From the **Hardware Management Console Workplace**:

1. Select the target systems or system group, and start the task: **Change Internal Code**.

   This opens the **Change Internal Code** window.

   From the **Change Internal Code** window:
2. Select **Remove and activate changes**, then click **OK**.

   This opens the **Request Selection** window.

   From the **Request Selection** window:
3. Select **Do all concurrent changes only**, then click **Remove and Activate**.

   This opens the **Confirm the Action** window.

   From the **Confirm the Action** window:
4. Click **Remove and Activate Concurrently** to begin the process.

   This opens the **Change Internal Code Progress** window.

   From the **Change Internal Code Progress** window:
5. Wait until the window indicates the process is complete, then click **OK** to close the window.

   This completes the task.

Example 2

The following example shows the steps for:

- Removing all installed internal code changes.
- Activating its previous change level **immediately** and **disruptively**.

From the **Hardware Management Console Workplace**:

1. Select the target systems or system group, and start the task: **Change Internal Code**.

   This opens the **Change Internal Code** window.

   From the **Change Internal Code** window:
2. Select **Remove and activate changes**, then click **OK**.

   This opens the **Request Selection** window.

   From the **Request Selection** window:
3. Select **Do all changes even if they are disruptive**, then click **Remove and Activate**.

   This opens the **Confirm this Disruptive Action** window.

   From the **Confirm this Disruptive Action** window:
4. Click **Remove and Activate Disruptively** to begin the process.

   This opens the **Change Internal Code Progress** window.

   From the **Change Internal Code Progress** window:
5. Wait until the window indicates the process is complete, then click **OK** to close the window.

   This completes the task.

Deleting internal code changes

Delete internal code changes to allow retrieving the changes over again if errors occurred during previous attempts to retrieve, install, or activate the changes.

Delete retrieved internal code changes if an error occurred while retrieving them. Remove then delete installed internal code changes if an error occurred while installing or activating them.

Deleting internal code changes erases retrieved internal code changes and removed internal code changes from the Support Elements of the selected systems.

Important: Refer to the instructions in the following example for general guidance. Then, while performing the task, request help for any window while it displays for more information about using it to complete the task.

Example

The following example shows the steps for deleting all internal code changes that are currently retrieved or removed.

From the **Hardware Management Console Workplace**:

1. Select the target systems or system group, and start the task: **Change Internal Code**.

   This opens the **Change Internal Code** window.

   From the **Change Internal Code** window:
2. Select **Delete all retrieved changes that were not installed**, then click **OK**.

   This opens the **Confirm the Action** window.

   From the **Confirm the Action** window:
3. Click **Delete** to begin the process.
4. Wait until a message indicates the process is complete, then click **OK** to close the message.

   This completes the task.

Applicable internal code changes

The following list shows the options you can select for changing internal code, and describes in general the set of internal code changes each option applies to. That is, the list defines what **all internal code changes** means with respect to each option.

Accept installed changes that were activated
This option applies to all installed changes that are currently activated.

Install and activate changes that were retrieved
This option applies to all changes that are eligible for being installed:

- All retrieved changes.
- All removed changes.

Browse system and internal code information
This task always applies to all changes.

Remove and activate changes
This option applies to all installed changes.

Delete all retrieved changes that were not installed
This option applies to all changes that are eligible for being installed:

- All retrieved changes.
- All removed changes.

Confirm the Action: Accept

Use this window to confirm or cancel your request to accept operational internal code changes.

Accepting operational internal code changes makes them permanent internal code.

At this point in the task, **operational internal code changes** are all changes you installed that are currently activated.

Attention: Accepting internal code changes permanently changes the internal code of the selected systems. The process cannot be undone. That is, accepted internal code changes cannot be removed to restore their previous change levels.

Accept
To confirm your request to accept operational internal code changes, click **Accept**.

Object List
To display and review the systems you selected to start this task, click **Object List**.

Cancel
To cancel your request, and close the window without accepting the operational changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Internal code change process

This window displays a summary of the internal code change process that is recommended. Accepting internal code changes is the second step (step **B**) of the process. Review the process before continuing.

Note: You should cancel your request to accept internal code changes in the following cases:

- If you have not completed the third or fourth steps (steps **C** or **D**) of the process for **previous** internal code changes.
  - If you have not yet retrieved all **previous** internal code changes provided to you by the support system.
  - Or if you have not yet installed and activated all **previous** retrieved internal code changes
- Or if you have not completed the first step (step **A**) of the internal code change process upon receiving new internal code changes. That is, if you have not yet performed a backup of critical data of the selected systems.

You should confirm your request to accept internal code changes only after completing the recommended steps described above.

Task

Use this window to complete the following task. For an example, with step-by-step instructions, select the following task.

- Accept internal code changes to make them permanent internal code.

Request Selection: Install and Activate

This window indicates whether the internal code changes retrieved for each selected system include concurrent or disruptive changes. The type of included changes determine whether installing and activating all changes will disrupt operating system activity on the systems.

Request Options
To qualify your request, make a selection that describes the internal code changes you want to install and activate. To continue the task, click **Install and Activate**.

Install and Activate
To continue installing and activating the changes as qualified by the option you selected, click **Install and Activate**.

Cancel
To cancel your request, and close the window without installing and activating any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

System Name and Concurrency Status selection

Review the concurrency status of the internal code changes retrieved for each system to determine whether installing and activating all changes will disrupt operating system activity on the systems.

System Name
Displays the name of each system for which internal code changes will be installed and activated.

Concurrency Status
Indicates whether the internal code changes retrieved for the system include concurrent or disruptive changes.

Note: If the concurrency status is: **Some changes are concurrent but not all.**, indicating changes for the system include both concurrent and disruptive changes, click **Details...** to display the individual concurrency status of each internal code change. The individual concurrency status of each change indicates whether its change levels are concurrent or disruptive. If you intend to install and activate only concurrent changes, the individual concurrency status determines which change levels will be installed and activated.

You can find more help information on the following:

Concurrency status: install and activate

This list column indicates whether the internal code changes retrieved for the system include concurrent or disruptive changes. The type of included changes determine whether installing and activating all changes will disrupt operating system activity on the system.

Concurrency statuses

No applicable changes. Considered concurrent.
Indicates there are no retrieved changes for the system.

Installing and activating all changes will not disrupt operating system activity on the system.

All changes are concurrent.
Indicates all changes for the system are concurrent changes.

Installing and activating all changes will not disrupt operating system activity on the system.

Some changes are concurrent but not all.
Indicates changes for the system include both concurrent and disruptive changes.

Installing and activating all changes will disrupt operating system activity on the system.

Note: Click **Details...** to display the individual concurrency status of each internal code change. The individual concurrency status of each change indicates whether its change levels are concurrent or disruptive. If you intend to install and activate only concurrent changes, the individual concurrency status determines which change levels will be installed and activated.

All changes are disruptive.
Indicates all changes for the system are disruptive changes.

Installing and activating all changes will disrupt operating system activity on the system.

Unable to query. Considered disruptive.
Indicates the concurrency status of changes for the system cannot be determined, but are assumed to include disruptive changes.

Installing and activating all changes may disrupt operating system activity on the system.

Concurrent and disruptive internal code changes: install and activate

A set of retrieved internal code changes may include both concurrent and disruptive internal code changes.

Concurrent internal code changes can be activated without disrupting operating system activity on the selected systems.

In contrast, activating **disruptive** internal code changes will disrupt operating system activity on the systems.

To install and activate retrieved changes that include both concurrent and disruptive changes, you will be given the options of either:

- Installing and activating all the internal code changes.

  This will disrupt operating system activity on the systems, but all retrieved changes will be installed and activated.
- Or installing and activating only the concurrent internal code change levels up to the lowest disruptive change level of each internal code change.

  This will not disrupt operating system activity on the systems, but one or more retrieved internal code changes will not have all their change levels installed.

Details...

To receive more information on the system you have selected, click **Details...**.

Do all concurrent changes only

To install and activate a limited set of concurrent internal code changes for each system, without disrupting its operating system activity, select **Do all concurrent changes only**.

Note: The concurrent changes installed and activated for each system will be limited to those that can be activated without first installing and activating a disruptive change. That is, for each internal code change, only concurrent change levels up to the lowest disruptive change level will be installed and activated.

Do all changes even if they are disruptive

To install and activate all internal code changes for each system, regardless of whether its operating system activity is disrupted, select **Do all changes even if they are disruptive**.

Include internal code changes which will inhibit the Concurrent Upgrade Engineering Changes (EC) task from being used to apply the next Licensed Internal Code EC level

This option is only available if you chose to **Install and activate changes that were retrieved** and if there are retrieved changes that would break the **Concurrent Upgrade Engineering Changes** task's maximum change level requirements if the changes were installed.

Confirm the Action: Install and Activate Concurrently

Use this window to confirm or cancel your request to install and activate the retrieved internal code changes for the selected systems.

Installing and activating the retrieved changes makes them operational.

At this point in the task, **retrieved internal code changes** are:

- All changes you retrieved from their source to the Support Elements of the systems. That is, all changes that are eligible for being installed.
- But limited to the type of changes you selected for the task on a previous window: concurrent changes **only**.

Concurrent internal code changes

Activating concurrent internal code changes does not require activating the systems on which the changes are installed. For this reason, activating the internal code changes is considered a concurrent operation. That is, it occurs while the systems and their operating systems continue to operate.

You can confirm your request to install and activate concurrent internal code changes without affecting the operating system activity of the selected systems.

Install and Activate Concurrently
To confirm your request to install and activate the retrieved internal code changes, click **Install and Activate Concurrently**.

Object List
To display and review the systems you selected to start this task, click **Object List**.

Cancel
To cancel your request, and close the window without installing or activating the retrieved changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm this Disruptive Action: Install and Activate

Use this window to confirm or cancel your request to install and activate the retrieved internal code changes for the selected systems.

Installing and activating the retrieved changes makes them operational.

At this point in the task, **retrieved internal code changes** are:

- All changes you retrieved from their source to the Support Elements of the systems. That is, all changes that are eligible for being installed.
- And qualified by the type of changes you selected for the task on a previous window: concurrent **and** disruptive changes.

Disruptive internal code changes

Activating disruptive internal code changes requires activating the systems on which the changes are installed. Since activating a system ends its operating system activity, activating the internal code changes is considered a disruptive operation.

You should confirm your request to install and activate disruptive internal code changes only if ending operating system activity on the selected systems are acceptable at this time.

Install and Activate Disruptively
To confirm your request to install and activate the retrieved internal code changes, click **Remove and Activate Disruptively**.

Object List
To display and review the systems you selected to start this task, click **Object List**.

Cancel
To cancel your request, and close the window without installing or activating the retrieved changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Engineering Change Concurrency Status

This window displays the individual concurrency status of each internal code change for a selected system. The individual concurrency status of each change indicates whether its change levels are concurrent or disruptive. If you intend to install and activate only concurrent changes, the individual concurrency status determines which change levels will be installed and activated.

System name
Displays the name of the selected system, for which the internal code changes will be installed and activated.

EC Number
Displays the Engineering Change (EC) number of each internal code change.

Concurrency Status
Indicates whether the change levels of the internal code change are concurrent or disruptive. The concurrency statuses include the following:

No applicable changes. Considered concurrent.
Indicates there are no retrieved changes for the system.

Installing and activating all changes will not disrupt operating system activity on the system.

All changes are concurrent.
Indicates all change levels are concurrent.

Installing and activating only concurrent changes will install and activate all change levels.

Changes are concurrent up to level *nn*.
Indicates only some change levels can be installed and activated concurrently.

Installing and activating only concurrent changes will install and activate all change levels from the current installed level up to and including level *nn*.

All changes are disruptive.
Indicates all change levels are disruptive.

Installing and activating only concurrent changes is not an option.

OK
To close the window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Request Selection: Remove and Activate

This window indicates whether the internal code changes installed for each selected system include concurrent or disruptive changes. The type of included changes determine whether removing and activating all changes will disrupt operating system activity on the systems.

Use this window to qualify or cancel your request to remove and activate the changes.

Request Options
To qualify your request, make a selection that describes the internal code changes you want to remove and activate. To continue the task, click **Remove and Activate**.

Remove and Activate
To continue removing and activating the changes as qualified by the option you selected, click **Remove and Activate**.

Cancel
To cancel your request, and close the window without removing and activating any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

System Name and Concurrency Status selection

Review the concurrency status of the internal code changes installed for each system to determine whether removing and activating all changes will disrupt operating system activity on the systems.

System Name
Displays the name of each system for which internal code changes will be removed and activated.

Concurrency Status
Indicates whether the internal code changes installed for the system include concurrent or disruptive changes.

Note: If the concurrency status is: **Some changes are concurrent but not all.**, indicating changes for the system include both concurrent and disruptive changes, click **Details...** to display the individual concurrency status of each internal code change. The individual concurrency status of each change indicates whether its change levels are concurrent or disruptive. If you intend to remove and activate only concurrent changes, the individual concurrency status determines which change levels will be removed and activated.

You can find more help information on the following:

Concurrency status: remove and activate

This list column indicates whether the internal code changes installed for the system include concurrent or disruptive changes. The type of included changes determine whether removing and activating all changes will disrupt operating system activity on the system.

Concurrency statuses

No applicable changes. Considered concurrent.
Indicates there are no installed changes for the system.

Removing and activating all changes will not disrupt operating system activity on the system.

All changes are concurrent.
Indicates all changes for the system are concurrent changes.

Removing and activating all changes will not disrupt operating system activity on the system.

Some changes are concurrent but not all.
Indicates changes for the system include both concurrent and disruptive changes.

Removing and activating all changes will disrupt operating system activity on the system.

Note: Click **Details...** to display the individual concurrency status of each internal code change. The individual concurrency status of each change indicates whether its change levels are concurrent or disruptive. If you intend to remove and activate only concurrent changes, the individual concurrency status determines which change levels will be removed and activated.

All changes are disruptive.
Indicates all changes for the system are disruptive changes.

Removing and activating all changes will disrupt operating system activity on the system.

Unable to query. Considered disruptive.
Indicates the concurrency status of changes for the system cannot be determined, but are assumed to include disruptive changes.

Removing and activating all changes may disrupt operating system activity on the system.

Concurrent and disruptive internal code changes: remove and activate

A set of installed internal code changes may include both concurrent and disruptive internal code changes.

Concurrent internal code changes can be activated without disrupting operating system activity on the selected systems.

In contrast, activating **disruptive** internal code changes will disrupt operating system activity on the systems.

To remove installed changes that include both concurrent and disruptive changes, and to activate their previous change levels, you will be given the options of either:

- Removing all the internal code changes, and activating the previous change levels.

This will disrupt operating system activity on the systems, but all installed changes will be removed.

- Or removing only the concurrent internal code change levels down to the highest disruptive change level of each internal code change, and activating the previous change levels.

  This will not disrupt operating system activity on the systems, but one or more installed internal code changes will not have all their change levels removed.

Details...

To receive more information on the system you have selected, click **Details...**.

Do all concurrent changes only

To remove and activate a limited set of concurrent internal code changes for each system, without disrupting its operating system activity, select **Do all concurrent changes only**.

Note: The concurrent changes removed and activated for each system will be limited to those that can be activated without first removing and activating a disruptive change. That is, for each internal code change, only concurrent change levels down to the highest disruptive change level will be removed and activated.

Do all changes even if they are disruptive

To remove and activate all internal code changes for each system, regardless of whether its operating system activity is disrupted, select **Do all changes even if they are disruptive**.

Confirm the Action: Remove and Activate Concurrently

Use this window to confirm or cancel your request to remove the installed internal code changes and to activate their previous change levels for the selected systems.

Removing the installed changes and activating their previous change levels makes the previous levels operational.

At this point in the task, **installed internal code changes** are:

- All changes you installed, but have not yet accepted or removed. That is, all changes that are activated or eligible for being activated.
- And qualified by the type of changes you selected for the task on a previous window: concurrent changes **only**.

Concurrent internal code changes

Activating concurrent internal code changes does not require activating the systems on which the changes are installed. For this reason, activating the internal code changes is considered a concurrent operation. That is, it occurs while the systems and their operating systems continue to operate.

You can confirm your request to remove and activate concurrent internal code changes without affecting the operating system activity of the selected systems.

Remove and Activate Concurrently
To confirm your request to remove and activate the installed internal code changes, click **Remove and Activate Concurrently**.

Object List
To display and review the systems you selected to start this task, click **Object List**.

Cancel
To cancel your request, and close the window without removing the installed changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm this Disruptive Action: Remove and Activate

Use this window to confirm or cancel your request to remove the installed internal code changes and to activate their previous change levels for the selected systems.

Removing the installed changes and activating their previous change levels makes the previous levels operational.

At this point in the task, **installed internal code changes** are:

- All changes you installed, but have not yet accepted or removed. That is, all changes that are activated or eligible for being activated.
- And qualified by the type of changes you selected for the task on a previous window: concurrent **and** disruptive changes.

Disruptive internal code changes

Activating disruptive internal code changes requires activating the systems on which the changes are installed. Since activating a system ends its operating system activity, activating the internal code changes is considered a disruptive operation.

You should confirm your request to remove and activate disruptive internal code changes only if ending operating system activity on the selected systems is acceptable at this time.

Remove and Activate Disruptively
To confirm your request to remove and activate the installed internal code changes, click **Remove and Activate Disruptively**.

Object List
To display and review the systems you selected to start this task, click **Object List**.

Cancel
To cancel your request, and close the window without removing the installed changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Delete

Use this window to confirm or cancel your request to delete:

- Retrieved internal code changes from the selected systems.
- Removed internal code changes from the selected systems.

At this point in the task:

- **Retrieved internal code changes** are all changes you retrieved from their source to the Support Elements of the systems, but have not yet installed.
- And **removed internal code changes** are all retrieved changes you installed, but then removed to undo their installation.

Attention: Deleting internal code changes erases them from the Support Elements of the systems. The process cannot be undone. However, deleted internal code changes can be retrieved again from their source to the Support Elements.

Selected systems
This window displays the selected systems for which you requested to delete all internal code changes that were previously retrieved.

Delete
To confirm your request and delete the internal code changes, click **Delete**.

Cancel
To cancel your request, and close the window without deleting the internal code changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Task

Use this window to complete the following task. For an example, with step-by-step instructions, select the following task.

- Deleting internal code changes to attempt error recovery.

Change LPAR Controls

Accessing the Change LPAR Controls task

Note: This task is not available when one or more managed systems have DPM enabled.

This task allows you to review or change logical processor assignments of logical partitions and the CPC's settings for processor running time if the selected CPC is operating in logically partitioned (LPAR) mode.

The settings that determine how processor resources are assigned to, used by, and managed for logical partitions that can be activated on the central processor complex (CPC) are referred to here as *control setting*s. More specifically, control settings determine:

- Whether logical partitions are assigned dedicated or shared processor resources.
- How each logical partition activated with shared processor resources shares them with other logical partitions activated with shared processor resources.
- How the CPC manages logical partitions' use of shared processor resources.

Both the CPC and its logical partitions have control settings. A logical partition's control settings apply only to the logical partition. The CPC's control settings apply to all of its logical partitions. The control settings are:

Logical processor assignment
These logical partition settings control how many logical processors are assigned to the logical partition, how they are assigned as either dedicated or shared processor resources, the processing weights of logical partitions, and absolute capping. The settings control how a partition is workload managed and whether software pricing is to change based on the number of defined capacity.

Processor running time
These CPC settings control how its logical partitions' processor running time is determined. The processor running time, referred to also as a timeslice, is the amount of continuous time allowed for each logical partition's logical processors to perform jobs on shared central processors.

The initial control settings of the CPC and each logical partition are established by the activation profiles used to activate them. Normally after the CPC is activated, changing its control settings requires opening and customizing a reset profile and then using the profile to activate the CPC again. Likewise, after the CPC is activated in LPAR mode, changing the control settings of its logical partition requires opening and customizing their image profile and then using the profile to activate the logical partition. Through this task you can change some of the control settings *dynamically* (new settings take affect without customizing profiles or activating objects).

To change control settings of the CPC and the logical partitions that can be activated on it:

1. Select a CPC (server).
2. Open the **Change LPAR Controls** task. The Change Logical Partition Controls window is displayed.
3. Depending on the physical processors installed in your system (CPs, ICFs, IFLs, and zIIPs), select the processor assignment tab to display the processor assignment window. Each processor assignment window lists the logical partitions that can be activated on the CPC and displays check boxes, entry fields, and other controls that indicate their current control settings.

From this window you have the option to export the data table to a Comma Separated Values (csv) file for audit purposes as well as performing further analysis. If you are accessing the Hardware Management Console remotely you can click **Export** to perform this function.

4. Select the **Processor Running Time** tab to change the control settings of the logical partitions, then proceed to indicate what you want to do with the new settings.

Change Logical Partition Controls

Note: This task is not available when one or more managed systems have DPM enabled.

Use this window to review or change logical processor assignments of logical partitions and the system settings for processor running time:

- Displays the last rest profile attempted for the most recent activation of the system.

  Note: If the field is blank, then the system was brought to its current state and status by operations other than activation.
- Displays the identifier of the Input/output Configuration Data Set (IOCDS) used during the most recent power-on reset and the processor controls for logical partitions defined by this IOCDS.
- "Logical processor assignment tabs" on page 488 identify the number of logical processors and type of physical processors assigned to logical partitions, and set processing weights for logical partitions that share central or internal coupling facility processors (and whether they are capped).
- Settings for the "Processor Running Time tab" on page 489 control how the system manages logical partition use of the logical processors assignment.

The processor controls of the system and logical partitions are established by the activation profiles used to activate them. Ordinarily, after the system is activated, changing its processor controls requires opening and customizing a reset profile, and then using the profile to activate the system again. Likewise, when the system is activated, changing the processor controls of its logical partitions requires opening and customizing their image profiles, and then using the profiles to activate the logical partitions.

This window allows changing some processor controls *dynamically* (new settings take effect without customizing profiles or activating objects). You can dynamically change:

- The processing weights of logical partitions that share processors (and whether they are capped).
- Allow a partition to be workload managed and set a minimum and maximum weight value.
- Allow software pricing to change based on the number of Workload Units (WLUs).
- The CPC's settings for processor running time.
- The absolute capping of logical partitions that share processors.

Additional functions on this window include:

Save to Profiles
If you want the new settings to take effect whenever the selected system and its logical partitions are activated with the modified profiles, click **Save to Profiles**. Saving new settings modifies the following activation profiles:

- A logical partition's control settings are saved in its image profiles. The settings take affect whenever the logical partition is activated with its image profile.
- The system's settings for processor running time are saved in the reset profile identified by the Last reset profile attempted filed. The settings take affect whenever the system is activated with that reset profile.

Note: Saving processor controls to activation profiles saves *all* processor controls currently displayed, regardless of when the settings were set.

Change Running System
If you change the logical partition group controls, click **Change Running System** if you want the new settings to take effect immediately. The selected system and its active logical partitions are referred to here as the *running system*. Using new settings to change the running system:

- Makes the processing weight, capped setting, and absolute capping currently displayed for each active logical partition (that shares central processors) take affect.
- Makes the settings currently displayed for system processor running time take affect.

The new settings remain in effect for the system and active logical partitions until you either dynamically change their processor controls again or activate them (which makes the processor controls in their activation profiles take affect).

Note: The running system includes active logical partitions only (as indicated by the **Active** column). Changes made to processor controls of inactive logical partitions do*not* take affect upon changing the running system. Consider saving the changes to profiles instead, to make them take affect when the logical partitions are activated.

Save and Change

If you change the logical partition group controls, click **Save and Change** if you want the new settings to take effect immediately *and* whenever the selected system and its logical partitions are activated with the modified profiles. **Save and Change** performs the combined operations of **Save to Profiles** and **Change Running System**.

Saving new settings modifies the following activation profiles:

- A logical partition's control settings are saved in its image profile. The settings take affect whenever the logical partition is activated with its image profile.
- The system's settings for group capacity value is saved in the group profile. The settings take affect immediately if any logical partitions assigned to the group are currently active or whenever any logical partition assigned to the group is activated.

Export

Note: This option is only available when you are accessing the Hardware Management Console remotely.

To transfer the change LPAR controls data table to a Comma Separated Value (CSV) file, click **Export**. This copies the data that is currently displayed in the window and puts it into a CSV file that you can use later for audit purposes or for further analysis.

From here, you can select to open the file for immediate viewing or you can save it to your workstation. If you selected **Open**, your file is displayed immediately. If you selected **Save the file** a **Save As** window allows you to browse your workstation and select the location you want to store the exported file.

Reset
To discard the information shown and display the information most recently used, click **Reset**.

Cancel
To close this window without saving changes and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Logical processor assignment tabs

Depending on what physical processors are installed in your system, select the logical processor assignment tab from the window to change the settings of one or more processor controls for the logical processor assignments for:

- Logical partitions with Central Processors (CPs)
- Logical partitions with Internal Coupling Facility (ICF) processors
- Logical partitions with IBM zEnterprise® Application Assist Processor (zAAP) processors (Version 2.12.1 and earlier)
- Logical partitions with Integrated Facility for Linux (IFL) processors

- Logical partitions with z Integrated Information Processors (zIIPs)

Review the information displayed for each possible logical partition processor assignment. The table for each logical processor assignment displays processor controls for the logical partitions and processor running time. You can change the settings of one or more processor controls, then make a selection to indicate when you want the new settings to take effect.

Logical Partition
Displays the name of each logical partition defined by the IOCDS.

Active
Indicates whether each logical partition is activated.

Defined Capacity
Use this column to change the number of Workload Units (WLUs) that are assigned for each logical partition.

Note: Defined capacity can only be changed for central processors.

Workload Manager (WLM) managed
Use this column to allow the partition to be managed by Workload Manager (WLM).

Current Weight
Displays the current processing weight setting in each logical partition's logical processor assignment.

Initial Weight
Use the entry fields in this column to change the initial processing weight of logical partitions that share processors of each logical partition's logical processor assignment.

Minimum Weight
Use the entry fields in this column to change the minimum processing weights of logical partitions. When **WLM Managed** is enabled, a logical partition's minimum weights places a lower limit on the amount of shared processor resources.

Maximum Weight
Use the entry fields in this column to change the maximum processing weights of logical partitions. When **WLM Managed** is enabled, a logical partition's maximum weights places an upper limit on the amount of shared processor resources.

Current Capping
Displays the current capping setting in each logical partition's logical processor assignment.

Initial Capping
Use the entry fields in this column to change whether the processing weights of logical partitions that share central or internal coupling facility processors are capped.

“Absolute Capping” on page 492
Displays the current absolute capping setting in each logical partition's logical processor assignment. Select the current absolute capping to change the setting.

Number of Dedicated Processors
Displays the number of dedicated processors in each logical partition's logical processor assignment.

Number of Not dedicated Processors
Displays the number of non-dedicated processors in each logical partition's logical processor assignment.

Processor Running Time tab

Select the **Processor Running Time** tab to display a window allowing you to change the settings on how the selected Central Processor Complex (CPC) manages logical partition use of shared processor resources.

Processor running time is the amount of continuous time allowed for logical processors to perform jobs on shared processors. The amount of continuous time is referred to also as a *timeslice*.

Shared processors are used by all logical partitions activated without dedicated processor resources. So the processor running time, or timeslice, is assigned to all logical partitions activated without dedicated processor resources.

The processor running time can be calculated dynamically by the CPC, or set to a constant amount. The initial method for calculating the running time is set by the activation profile used to activate the CPC.

Use the settings to change the CPC's processor running time settings. Then make a selection to indicate when you want the new settings to take effect.

Note: When the window is displayed, the CPC's *current* settings for processor running time appears. Since the window allows changing the settings at any time, the CPC's current settings may not be the same as its *initial* settings. The initial settings were established by the reset profile used to activate the CPC.

You can find more detailed help on the following elements of this window:

Dynamically determined by the system

To have the CPC calculate the running time whenever the number of active logical processors changes, select **Dynamically determined by the system**.

Determined by the user

To set a constant running time, select **Determined by the user** to indicate whether logical partitions lose their share of running time when they enter a wait state.

Note: When processor running time is dynamically determined, it reduces the possibilities for suboptimal use of processor resources.

Running time

If you selected **Determined by the user** to set a constant running time, specify the constant running time you want to set.

Do not end the timeslice if a partition enters a wait state

If you selected **Determined by the user** to set a constant running time, select **Do not end the timeslice if a partition enters a wait state** to indicate whether logical partitions lose their share of running time when they enter a wait state.

Note: This selection is available on the Hardware Management Console Version 2.13.1 and earlier.

A logical partition enters a wait state when processing cannot continue due to an error or because its processors are waiting for instructions.

If **Do not end the timeslice if a partition enters a wait state** is not selected this indicates logical partitions lose their share of running time when they enter a wait state. That is, idle processor resources can be used by another logical partition immediately. The share of running time ends for the logical partition that enters the wait state, and a new timeslice begins for another logical partition.

Note: This option is applicable only when **Determined by the user** is selected. Otherwise, it is unavailable.

Workload Manager (WLM) managed

Workload Manager allows the processing weights to be redistributed according to where WLM believes the CPU resources are needed to satisfy customer workload goals. This function works for uncapped shared logical processors only. The weight will be allowed to vary in a range between the minimum weight and maximum weight.

Notes:

- Only **General** mode logical partitions can be enabled for WLM management.
- Enablement of WLM managed in a logical partition is not allowed if **Initial Capping** is selected, and conversely initial capping cannot be selected if WLM managed is selected. However, it is valid for both not to be selected.
- Enablement of WLM in a logical partition and a fully dedicated logical partition are mutually exclusive.

Initial Weight

Use this field to change the initial processing weights of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays:

- The initial processing weight assigned to each active logical partition.
- The initial weight set in the image profile of each inactive logical partition.

The processing weight can be from 1 to 999. To change a logical partition's setting, enter a new initial processing weight in its field, then use the processor controls to indicate when you want the new settings to take effect.

A logical partition's *initial processing weight* is its relative amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time. That percentage is calculated by dividing the logical partition's processing weight by the total processing weight of all active logical partitions.

An initial processing weight is a target, not a limit. It represents the share of resources guaranteed to a logical partition when all processor resources are in use. Otherwise, when excess processor resources are available, the logical partition can use them if necessary. When a logical partition is not using its share of processor resources, other active logical partitions can use them.

While excess processor resources are available, initial processing weights have no effect on how those resources are used. Instead initial processing weights take effect only when the number of logical processors requiring a timeslice is greater than the number of available physical processors.

Notes:

- A field is available for a logical partition only when its logical processor assignment includes at least one non-dedicated processor (as indicated in the **Number of Not dedicated Processors** column. Otherwise, if its logical processor assignment includes only dedicated processors, this field is grayed-out.
- If the logical partition contains any non-dedicated processors that are reserved, they will not appear in the column **Number of Not dedicated Processors**. However, the **Initial Weight** and **Initial Capping** fields can be changed.
- An *initial* processing weight was assigned to each active logical partition by its image profile during activation. Since, the window allows changing the initial processing weight at any time, a logical partition's current setting may not be the same as its initial setting.
- The initial weight displayed for an inactive logical partition does not apply if its image profile does not exist.

Minimum Weight

Use this field to change the initial processing weights of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays only when WLM Managed is enabled.

The minimum weight must be less than or equal to the initial processing weight.

When Workload Manager is enabled, a logical partition's *minimum weight* places a lower limit on the amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

Note: A *minimum* processing weight was assigned to each active logical partition by its image profile during activation. Since the window allows changing the minimum processing weight at any time, a logical partition's current setting may not be the same as its initial setting. The initial settings were established by the reset profile used to activate the CPC.

- The minimum processing weight displayed for an inactive logical partition is not applicable if its image profile does not exist.

Maximum Weight

Use this field to change the initial processing weights of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays only when WLM Managed is enabled.

The maximum weight must be greater than or equal to the initial weight.

When Workload Manager is enabled, a logical partition's *maximum weight* places a upper limit on the amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

Note: A *maximum* weight was assigned to each active logical partition by its image profile during activation. Since the window allows changing the maximum weight at any time, a logical partition's current setting may not be the same as its initial setting. The initial settings were established by the reset profile used to activate the CPC.

- The maximum processing weight displayed for an inactive logical partition is not applicable if its image profile does not exist.

Initial Capping

Use this field to change the initial processing weights of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays:

- Whether the initial processing weight of each active logical partition currently is capped.
- Whether the initial processing weight set in the image profile of each inactive logical partition is capped.

A check indicates the logical partition's initial processing weight is capped.

A logical partition's *initial weight* is its relative amount of shared processor resources. The *Initial Capping* setting indicates whether the logical partition is prevented from using processor resources in excess of its processing weight.

- When the initial processing weight is *not* capped, it is a target, not a limit. It represents the share of resources guaranteed to a logical partition when all processor resources are in use. Otherwise, when excess processor resources are available, the logical partition can use them if necessary.
- When the initial processing weight is capped, it is a limit. It represents the logical partition's maximum share of resources, regardless of the availability of excess processor resources.

Notes:

- A field is available for a logical partition only when its logical processor assignment includes at least one non-dedicated processor (as indicated in the **Number of Not dedicated Processors** column. Otherwise, if its logical processor assignment includes only dedicated processors, the field is grayed-out.
- If the logical partition contains any non-dedicated processors that are reserved, they will not appear in the column **Number of Not dedicated Processors**. However, the **Initial Weight** and **Initial Capping** fields can be changed.
- An *initial* capped setting was assigned to each active logical partition by its image profile during activation. Since, the window allows changing the setting at any time, a logical partition's current setting may not be the same as its initial setting.
- **Initial Capping** cannot be selected if WLM managed is already selected, as they are mutually exclusive. Conversely, WLM managed cannot be selected if initial capping is selected. However, it is valid for both not to be selected.

Absolute Capping

Use this field to change the absolute capping of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays:

- The absolute capping assigned to each active logical partition.
- The absolute capping set in the image profile of each inactive logical partition.

The absolute capping can be None or a number of processors value from 0.01 to 255.0. To change a logical partition's setting, select the current absolute capping setting in its field, then use the Change LPAR Controls window to specify the absolute capping for the selected logical partition to indicate when you want the new settings to take effect.

While excess processor resources are available, absolute capping has no effect on how those resources are used.

Notes:

- A field is available for a logical partition only when its logical processor assignment includes at least one non-dedicated processor (as indicated in the **Number of Not dedicated Processors** column. Otherwise, if its logical processor assignment includes only dedicated processors, this field is grayed-out.
- If the logical partition contains any non-dedicated processors that are reserved, they will not appear in the column **Number of Not dedicated Processors**.
- The absolute capping displayed for an inactive logical partition does not apply if its image profile does not exist.

Edit Absolute Capping

Use this window to specify the absolute capping of the selected logical partitions that share processors.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR Cryptographic Controls

Accessing the Change LPAR Cryptographic Controls task

The settings that determine how the activated logical partition uses the Crypto Express feature assigned to are referred here as cryptographic controls.

Logical partition's initial cryptographic controls are established by the activation profile used to activate the logical partition. See the **Customize/Delete Activation Profiles** task for more information about customizing activation profiles for establishing a logical partition's initial cryptographic controls:

You can use the Support Element workplace to start the task to select cryptographic control settings to be changed dynamically on the system, in the image profile, or both.

To dynamically change logical partition cryptographic controls:

1. Open the **Change LPAR Cryptographic Controls** task.
2. Use the Change LPAR Cryptographic Controls window to change the crypto configuration for a logical partition then proceed to indicate what you want to do with the new settings.

3. Use the cryptographic controls to dynamically:
   - Add unassigned crypto(s) domain(s) to a logical partition for the first time.
   - Edit assigned crypto(s) and domain(s) types to a logical partition already using cryptos and domains.
   - Remove crypto(s) and domain(s) from a logical partition.

Change LPAR Cryptographic Controls

Use this window to customize information that controls how the logical partition activated by the profile uses the coprocessors and accelerators assigned to it. The settings are referred to here as *cryptographic controls* and apply to the logical partition only if it is customized for using coprocessors and accelerators. This window allows you to:

- Add unassigned crypto(s) and domain(s) to a logical partition for the first time
- Edit assigned crypto(s) and domain(s) types to a logical partition already using cryptos and domains.
- Remove crypto(s) and domain(s) from a logical partition.

The assigned cryptographic domain index table displays the control domain and control and usage domain indexes which can be modified in the logical partition.

Control Domain
A logical partition's *control domains* are those cryptographic domains for which remote secure administration functions can be established and administered from this logical partition.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Control and Usage Domain
A logical partition's *control and usage domains* are domains in the cryptos that can be used for cryptographic functions. The usage domains cannot be removed if they are online.

A logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

The assigned cryptos index table displays the cryptographic candidate list and cryptographic online list settings which can be modified in the logical partition.

Cryptographic Candidate List
The candidate list identifies which cryptos will be assigned to the logical partition. Cryptos cannot be removed if they are online.

Cryptographic Online List (from profile)
The online list identifies which cryptos will be brought online at the next activation. Changes to the online list do not affect the running system. You must activate the partition to bring the coprocessor or accelerators online.

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Edit
Allows you to “Edit Domains” on page 798 or “Edit Cryptos” on page 799 for the selected activation profile.

Remove
Allows you to remove selected control and usage domain settings or selected crypto candidate and online settings for the selected activation profile.

Add
Allows you to “Add Domains” on page 799 or “Add Cryptos” on page 799 for unassigned domains or unassigned crypto candidates for the selected activation profile.

The icons perform the following functions in the Assigned domains or crypto tables:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Save and Change

If you want the new settings to take effect immediately *and* whenever the logical partition is activated with the modified profile click “Save and Change” on page 496.

Save to Profiles
If you want the new settings to take effect whenever the logical partition is activated with the modified profile, click “Save to Profiles” on page 495.

Change Running System
If you want the new settings to take effect in the active logical partition immediately, click “Change Running System” on page 496.

Reset
To return the values back to their original values, click **Reset**.

Cancel
To close this window and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save to Profiles

Saving new settings modifies the following activation profiles:

- Saves a logical partition's cryptographic control settings in its image profile. The settings take effect whenever the logical partition is activated with its image profile.

- Saves a logical partition's cryptographic control settings for both active and inactive logical partitions. The partition status (active/inactive) is indicated in the window title, along with the logical partition name.

Change Running System

Changes the cryptographic settings in the logical partition without reactivating the partition. The new settings remain in effect for the logical partition until you either dynamically change the settings again or reactivate the partition.

Note: Change Running System can be selected for an active logical partition only. For an inactive partition, the Change Running System button will be disabled.

Save and Change

Saving new settings modifies the following activation profiles:

- Saves a logical partition's cryptographic control settings in its image profile. The settings take effect whenever the logical partition is activated with its image profile.
- Changes the cryptographic settings in the logical partition without reactivating the partition. The new settings remain in effect for the logical partition until you either dynamically change the settings again or reactivate the partition.

Note: Save and Change can be selected for an active logical partition only. For an inactive partition, the Save and Change button will be disabled.

To perform both **Save to Profiles** and **Change Running System** at the same time, click **Save and Change**. For more information about the operations, select:

- Save to Profiles
- Change Running System

Usage Domain Zeroize

When removing one or more cryptos and/or usage domains from an active logical partition, the Usage Domain Zeroize window will be displayed. This window may contain one or both of the following:

- The crypto and usage domain combinations which can zeroized.
- The crypto and usage domain combinations which already have zeroize pending.

Zeroize of the usage domain indexes will clear the cryptographic keys from the cryptographic number in the selected partition. The cryptographic keys will have to be reentered to re-enable cryptographic operations in this partition.

Click **Options** on the menu bar to *select all the rows*, *deselect all the rows*, or *exit* the window, returning to the Change LPAR Cryptographic Controls window.

Additional functions on this window include:

OK

To close this window and continue with the crypto operation, click **OK**.

Cancel

To close this window and return to the Change LPAR Crypto Controls window, click **Cancel**.

Help

To display help for the current window, click **Help**.

Usage domain zeroize and usage domain zeroize pending tables

The **usage domain zeroize** table will contain one row for each cryptographic number and usage domain combination which can zeroized. By default, all combinations are selected for zeroize. Any or all rows can be deselected so that the zeroize is not performed for those combinations.

The **usage domain zeroize pending** table will contain one row for each cryptographic number and usage domain combination that already has zeroize pending. If a zeroize is pending, these combinations cannot be selected for zeroize.

Cryptographic Number
Displays the cryptographic number which will be zeroized

Usage Domain Index
Displays the usage domain index which will be zeroized

The Usage Domain Zeroize window may contain one or both of these tables.

Change LPAR Group Controls

Accessing the Change LPAR Group Controls task

Note: This task is not available when one or more managed systems have DPM enabled.

This task allows you to view or change a group assignment for logical partitions. It displays the group name, member partitions, and group capacity value that can be customized in determining the allocation and management of processor resources assigned to the group. It also allows changing a group assignment dynamically for active logical partitions.

To change LPAR group controls:

1. Select a CPC (server).
2. Open the **Change LPAR Group Controls** task. The Change LPAR Group Controls window is displayed.
3. You can click **Edit** on the menu bar to change the group capacity value and the group members.
4. Once you have made your changes to those windows you can either:
   - Click **Save to Profile**s if you want the new settings to take effect whenever the selected CPC and its logical partitions are activated with the modified profiles,
   - Click **Change Running System** if you want the new settings to take effect immediately, or
   - Click **Save and Change** if you want the new settings to take effect immediately and whenever the selected CPC and its logical partitions are activated with the modified profiles.

Change Logical Partition Group Controls

Note: This task is not available when one or more managed systems have DPM enabled.

Use this window to view or change a group assignment for logical partitions. This window displays the group name, member partitions, group capacity value, and absolute capping setting that can be customized in determining the allocation and management of processor resources assigned to the group.

This window allows changing a group assignment dynamically for active logical partitions.

Click **Edit** on the menu bar to select the following:

- Edit Group Capacity to change the group capacity value for a defined logical partition group.
- Edit Group Members to assign partitions to a group.
- “Edit Absolute Capping” on page 499 to change the absolute capping value for a processor type in a defined logical partition group.

The table list the group assignments for the logical partitions that can be customized:

Group Name
Displays the group name for the logical partition(s)

Member Partitions
Displays the name(s) of the logical partitions assigned to the group

Group Capacity Value
Displays the number of Workload Units (WLU) that are assigned to the logical partitions group.

Absolute Capping
Displays the current absolute capping setting for each logical partition's logical processor assigned to the group.

Additional functions on this window include:

Save to Profiles
If you want the new settings to take effect whenever the selected system and its logical partitions are activated with the modified profiles, click **Save to Profiles**.

A logical partition's group name is saved in the image profile and the group capacity value is saved in the group profile. The settings take effect whenever any logical partition assigned to the group is activated with its image profile.

Note: Saving processor controls to activation profiles saves *all* processor controls currently displayed, regardless of when the settings were set.

Change Running system
If you change the logical partition group controls, click **Change Running System** if you want the new settings to take effect immediately. The selected system and its active logical partitions are referred to here as the *running system*. Using new settings to change the running system makes the new group name and group capacity setting currently displayed for each active logical partition (that shares central processors) take effect.

The new settings remain in effect for the system and active logical partitions until you either dynamically change their processor controls again or activate them (which makes the processor controls in their activation profiles take effect).

Note: The running system includes active logical partitions only (as indicated by the **Partition Active** column). A group becomes part of the running system when any member partition assigned to the group is activated. The group capacity value can be changed for the running system as long as the group has one active partition. Changes made to group controls of inactive logical partitions do *not* take effect upon changing the running system. Consider saving the changes to profiles instead, to make them take effect when the logical partitions are activated.

Save and Change

If you change the logical partition group controls, click **Save and Change** if you want the new settings to take effect immediately *and* whenever the selected Central Processor Complex (CPC) and its logical partitions are activated with the modified profiles. **Save and Change** performs the combined operations of **Save to Profiles** and **Change Running System**.

Saving new settings modifies the following activation profiles:

- A logical partition's group name is saved in its image profile. The settings take effect whenever the logical partition is activated with its image profile.
- The group capacity value is saved in the group profile. The settings take effect immediately if any logical partitions assigned to the group are currently active or whenever any logical partition assigned to the group is activated.

Reset
To discard the information shown and display the information most recently used, click **Reset**.

Cancel
To close this window without saving changes and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Group Capacity

Use this window to specify a group capacity value for all logical partitions belonging to this group.

Additional functions on this window include:

OK
To apply the group capacity value and return to the previous window, click **OK**.

Cancel
To close the window without saving changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Group Members

Use this window to assign logical partition(s) to a group or to remove logical partition(s) from a group.

Partition Name
Displays the name of the partition

Partition Active
Indicates whether the partition is active

Current Group
Displays the current name of the group

New Group
Enter the name of the new group to which the partition(s) will be assigned or enter "NONE" to remove a partition from a group

You can find more detailed help on the following elements of this window:

OK
To apply the new changes to a group and return to the previous window after assigning partitions to a group, click **OK**.

Cancel
To close the window without saving changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Absolute Capping

Use this field to change the absolute capping of logical partitions in a group that share processors. The absolute capping can be None or a number of processors value from 0.01 to 255.0. To change an absolute capping for a processor type for a group, select the current absolute capping setting in its field and click the hyperlink to display the next Edit Absolute Capping window. Specify the absolute capping for the selected processor type to indicate the new setting.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Refer to the following for additional information on the Edit Absolute Capping table functions:

Edit Absolute Capping

Use this window to specify the absolute capping of the selected processor type belonging to this group.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

OK
To save the new values and return to the Change LPAR Group Controls window, click **OK**.

Cancel
To close the window without saving the changes you made and return to the Change LPAR Group Controls window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR I/O Priority Queuing

Accessing the Change LPAR I/O Priority Queuing task

This task allows you to review or change the minimum or maximum I/O priority queuing value assignments of logical partitions. These values are passed on to the I/O subsystem for use when queuing decisions with multiple requests. You can dynamically (new settings take effect without customizing profiles or activating objects) change the minimum and maximum values.

To change LPAR I/O priority queuing:

1. Select one or more CPCs (servers).
2. Open the **LPAR I/O Priority Queuing** task. The Change Logical Partition Input/Output (I/O) Priority Queuing window is displayed.
3. The window lists the I/O priority queuing values for logical partitions defined by this IOCDS.
4. Use the window to dynamically change the minimum and maximum values.

   Note: If global I/O priority queuing is **Enabled**, changes made for the minimum or maximum values will take effect immediately. If the global value is **Disabled**, changes will be saved by the system, but will not take effect until the global value is changed to **Enabled**.
5. Make a selection to indicate what you want to do with the new setting.

Change Logical Partition Input/Output (I/O) Priority Queuing

Use this window to review or change the minimum and maximum Input/Output (I/O) priority queuing values of logical partitions *dynamically*. (New settings take effect without customizing profiles or activating objects.)

The I/O priority queuing values of the logical partitions are established by the activation profiles used to activate them. Ordinarily, after a CPC is activated in LPAR mode, changing the I/O priority queuing values of its logical partitions requires opening and customizing its image profiles and then using the profiles to activate the logical partitions.

A range of priorities for a logical partition are supported. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

1. Review the information displayed in the window's fields.
2. You can change the settings of one or more priority queuing values by typing values into the table:
   - *Minimum input/output (I/O) priority queuing values* specify a minimum priority to associate with an Input/Output (I/O) request at Start Subchannel time for the logical partition.
   - *Maximum input/output (I/O) priority queuing values* specify a maximum priority to associate with an Input/Output (I/O) request at Start Subchannel time for the logical partition.
3. To indicate when you want the new settings to take effect, click **Save to Profiles**, **Change Running System**, or **Save and Change**.

The following functions are available from this window:

Input/output configuration data set (IOCDS)
Displays the identifier of the IOCDS used during the most recent power on.

Global input/output (I/O) priority queuing
Indicates whether the global input/output (I/O) priority queuing is enabled or disabled.

Note: If global input/output (I/O) priority queuing is enabled, changes made for the minimum or maximum values take effect immediately. If the global value is disabled, changes are saved by the system, but do not take effect until the global value is changed to enabled.

Maximum global input/output (I/O) priority queuing value
Indicates the maximum value allowed in the current system for Input/Output (I/O) priority queuing. This is the highest value to which any of the partition's minimum or maximum Input/Output (I/O) priority queuing value can be set. Changes made on the panel are passed to the I/O subsystem if I/O priority queuing is enabled for use when making queuing decisions with multiple requests.

Note: The Input/Output (I/O) priority queuing values for the partition can be equal to or less than the global maximum Input/Output (I/O) priority queuing value, ensuring that the rules stated for minimum and maximum are met as well.

Logical partition table

This table lists the following information:

Logical Partition
This column displays the name of each logical partition defined by the IOCDS.

Active
This column indicates whether each logical partition is activated.

A logical partition becomes *active* when it is activated. Conversely, a logical partition is not active, or is *inactive*, before it is activated and after it is deactivated.

- **Yes** - Indicates the logical partition currently is activated.

  Note: An active logical partition is not necessarily operating.
- **No** - Indicates the logical partition currently is not activated.

Minimum Input/Output (I/O) Priority
Use this column to change the minimum priority associated with an Input/Output (I/O) request at Start Subchannel time for the logical partition. This minimum value is passed to the I/O subsystem if I/O priority queuing is enabled for use when making queuing decisions with multiple requests.

Note:

- The minimum value must be less than or equal to the maximum value.
- The minimum value must be less than or equal to the **maximum global Input/Output (I/O) priority queuing value**.
- The I/O priority values can overlap with the I/O priority values for other active logical partitions.
- The minimum value also serves as the default I/O priority value for the logical partition. If the software in the logical partition does not understand I/O priority queuing, the minimum value is assigned to all I/O requests in the logical partition. In this case, for clarity, the maximum value should be set equal to the minimum value, although this is not a requirement.
- The logical partition default value for the minimum priority is zero.
- Setting both the minimum and maximum values to zero for a logical partition has a disabling effect on I/O priority queuing for that logical partition. Use caution in doing this because the logical partition would then have the lowest priority possible.

Maximum Input/Output (I/O) Priority
Use this column to change the maximum priority associated with an Input/Output (I/O) request at Start Subchannel time for the logical partition. This maximum value is passed to the I/O subsystem if I/O priority queuing is enabled for use when making queuing decisions with multiple requests.

Note:

- The maximum value must be greater than or equal to the minimum value.

- The maximum value must be less than or equal to the **maximum global Input/Output (I/O) priority queuing value**.
- The I/O priority values can overlap with the I/O priority values for other active logical partitions.
- The logical partition default value for the maximum priority is zero.
- Setting both the minimum and maximum values to zero for a logical partition has a disabling effect on I/O priority queuing for that logical partition. Use caution in doing this because the logical partition would then have the lowest priority possible.

Save to Profiles
If you change the settings of one or more priority queuing values and you want the new settings to take effect whenever the Central Processor Complex (CPC) and logical partitions are activated with the modified profiles, click **Save to Profiles**.

Saving new settings changes the image profile. A logical partition's minimum and maximum Input/Output (I/O) priority queuing settings are saved in its image profile. The settings take effect whenever the logical partition is activated with its image profile.

Note: Be aware that saving priority queuing values to activation profiles saves *all* priority queuing values currently displayed, regardless of when the settings were set. For example, if you used the **Change Logical Partition Input/Output (I/O) Priority Queuing** window previously to change some of the running system's I/O priority queuing settings, those changes are saved in the profiles along with any changes you made presently.

Change Running System
If you change the settings of one or more priority queuing values and you want the new settings to take effect immediately, click **Change Running System**.

The Central Processor Complex (CPC) and its active logical partitions are referred to here as the *running system*. Using new settings to change the running system makes the minimum and maximum Input/Output (I/O) priority queuing setting currently displayed for each active logical partition (that shares central processors) take effect.

The new settings remain in effect for the CPC and active logical partitions until you either dynamically change their priority queuing values again or activate them (which makes the priority queuing values in their activation profiles take effect).

Note: The running system includes active logical partitions only (as indicated by the **Active** list column). Changes made to priority queuing values of inactive logical partitions do *not* take effect upon changing the running system. Instead, consider saving the changes to profiles to make them take effect when the logical partitions are activated.

Reset
To discard changes you made to the settings of priority queuing values and display again the current settings, click **Reset**.

Cancel
To close this window without saving the changes you made and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR Security

Accessing the Change LPAR Security task

The settings that determine the extent of interaction between logical partitions that can be activated on the central processor complex (CPC) are referred to here as *security settings*.

A logical partition's security settings are:

Performance data control
This setting controls whether a logical partition has global access to performance data.

Input/output configuration control
This setting controls whether a logical partition can change the input/output (I/O) configuration of the CPC on which it is activated.

Cross partition authority
This setting controls whether a logical partition can issue a subset of control program instructions to other logical partitions activated on the same CPC

Logical partition isolation
This setting controls whether a logical partition has exclusive use of its reconfigurable channel paths.

Basic counter set authorization control
The basic set authorization control can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

Problem state counter set authorization control
The problem state set authorization control can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

Crypto activity counter set authorization control
The crypto activity counter set authorization control can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

Extended counter set authorization control
The counters of the extended counter set authorization control are model dependent.

Basic sampling authorization control
The basic sampling authorization control allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

Dynamic sampling authorization control
The dynamic sampling authorization control allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

Permit AES key import functions
The permit Advanced Encryption Standard (AES) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

Permit DEA key import functions
The permit Data Encryption Algorithm (DEA) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

Permit ECC key import functions
The permit Elliptical Curve Cryptography (ECC) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

A logical partition's initial security settings are established by the activation profile used to activate the logical partition. See the **Customize/Activation Profiles** task for more information about customizing activation profiles for establishing a logical partition's initial security settings:

To review or change logical partition security settings:

1. Open the **Change LPAR Security** task.

   The Change Logical Partition Security window displays. The window lists the logical partitions that can be activated on the CPC and displays check boxes that indicate their current security settings:

   - Performance data control
   - Input/output configuration control
   - Cross partition security
   - Logical partition isolation
   - Basic counter set authorization control
   - Problem state counter set authorization control

- Crypto activity counter set authorization control
- Extended counter set authorization control
- Basic sampling authorization control
- Dynamic sampling authorization control
- Permit AES key import functions
- Permit DEA key import functions.

2. Use the check boxes to change the logical partitions' security settings, then use the controls to indicate what you want to do with the new settings.

   Use the online Help for more information about changing logical partition security.

   Notes:

   - *Dynamic I/O configuration*: Although more than one logical partition can run an application that supports dynamic I/O configuration, you should allow using only one logical partition to dynamically change the I/O configuration. The I/O configuration control setting of the logical partition you choose must display a check mark. The I/O configuration control setting of all other logical partitions should be blank.
   - *Automatic reconfiguration facility (ARF)*: To use a logical partition for running an application that supports the ARF, its cross partition authority setting must display a check mark.

Change Logical Partition Security

Use this window to review or change the security settings of logical partitions *without* opening their image profiles or activating them. The settings determine the extent of interaction between logical partitions that can be activated on the Central Processor Complex (CPC). The settings are referred to here as *security settings*.

A logical partition's operational capabilities and characteristics, which include its security settings, are established by the activation profile used to activate it. Ordinarily, after the CPC is activated in Logically Partitioned (LPAR) mode, changing the operational capabilities and characteristics of its logical partitions requires opening and customizing their image profiles, and then using the profiles to activate the logical partitions.

The window lists the security settings for logical partitions defined by the Input/Output Configuration Data Set (IOCDS) used during the most recent power-on reset of the CPC.

Reset
To discard changes you made to any security settings, and display the initial security settings for each logical partition, click **Reset**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following element of this window:

Input/Output Configuration Data Set (IOCDS)

Displays the identifier of the IOCDS used during the most recent power-on reset.

Change Logical Partition Security List

Use this window to customize security options for the activated logical partitions.

Logical Partition
Displays the name of each logical partition defined by the IOCDS.

Active
Indicates whether each logical partition is activated.

Performance Data Control
Use each check box in this list column to control whether a logical partition has global access to performance data.

Input/Output Configuration Control
Use each check box in this list column to control whether a logical partition can change the Input/Output (I/O) configuration of the CPC on which it is activated.

This control allows the OSA Support Facility to control OSA configuration for other LPs and allows access to certain STP data.

Cross Partition Authority
Use each check box in this list column to control whether a logical partition can issue a subset of control program instructions to other logical partitions activated on the same CPC.

BCPii Permissions
Select the hyperlink to change the BCPii command permissions for the running system, selected logical partitions, or both.

Logical Partition Isolation
Use each check box in this list column to control whether a logical partition has exclusive use of its reconfigurable channel paths.

Basic Counter
Use the check box in this list column to control whether authorization is allowed to use the basic counter set. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

Problem State Counter
Use the check box in this list column to control whether authorization is allowed to use the problem-state counter set. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

Crypto Activity Counter
Use the check box in this list column to control whether authorization is allowed to use the crypto-activity counter set. The set can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

Extended Counter
Use the check box in this list column to control whether authorization is allowed to use the extended counter set. The counters of this set are model dependent. This set can be used to count the crypto activities of a coprocessor.

Basic Sampling
Use the check box in this list column to control whether authorization is allowed to use the basic-sampling function which provides a set of architected sample data. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

Diagnostic Sampling
Use the check box in this list column to control whether authorization is allowed to use the diagnostic-sampling function which provides a set of architected sample data. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

AES Key
Use the check box in this list column to enable or disable the Advanced Encryption Standard (AES) key import functions for the installed CP Assist for Cryptographic Functions (CPACF) feature.

DEA Key
Use the check box in this list column to enable or disable the Data Encryption Algorithm (DEA) key import functions for the installed CP Assist for Cryptographic Functions (CPACF) feature.

ECC Key
Use the check box in this list column to enable or disable the Elliptical Curve Cryptography (ECC) key import functions for the installed CP Assist for Cryptographic Functions (CPACF) feature.

Note: When the window displays, the check boxes for each logical partition indicate its *current* security settings. Since the window allows changing the security settings at any time, a logical partition's current settings may not be the same as its *initial* settings. The initial settings were established by the activation profile used to activate the logical partition.

Add partition

Use this window to specify the partitions from which the target partition can receive BCPii commands.

Enter system and partition manually
System: Enter the system name for the logical partition from which the target partition can receive BCPii commands.

Netid: Enter the Netid name for the selected system.

Partition: Enter the logical partition name from which the target partition can receive BCPii commands.

Select a system and partition
System: Select from the drop-down menu the system for the logical partition from which the target partition can receive BCPii commands.

Netid: The Netid displays for the selected system.

Partition: Select from the drop-down menu the active logical partition from which the target partition can receive BCPii commands.

Additional functions on this window include:

Add
To add the system and partition, click **Add**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Configure BCPii Permissions

Use this section to enable or disable the Base Control Program internal interface (BCPii) permissions for the selected logical partition.

Enable the partition to send commands
To enable the selected partition to send BCPii commands, select **Enable the partition to send commands**. When selected, the active logical partition can send BCPii commands to other active logical partitions.

Enable the partition to receive commands from other partitions
To enable the selected partition to receive BCPii commands from other partitions, select **Enable the partition to receive commands from other partitions**. When selected, the active logical partition can receive BCPii commands from other active logical partitions.

All partitions
Select this option if you want the selected logical partition to receive BCPii commands from all the active logical partitions.

“Add partition” on page 506 (Selected partitions)
Select this option if you want to remove or add selected logical partitions to receive BCPii commands from the logical partition.

Add
To add a system and logical partition to receive BCPii commands from the logical partition, click **Add**.

Remove
To remove a selected logical partition to receive BCPii commands from the logical partition, click **Remove**.

Additional functions on this window include:

OK
To return to the previous window with updated changes, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save and Change

If you change the security settings for the activated logical partitions, click **Save and Change** if you want the new settings to take effect immediately *and* whenever the selected Central Processor Complex (CPC) and its logical partitions are activated with the modified profiles.

Note: Saving new settings modifies the following activation profiles:

- A logical partition's security settings are saved in its image profile. The settings take effect whenever the logical partition is activated with its image profile.

Clicking **Save and Change** performs at once the two operations performed by selecting **Save to Profiles** and **Change Running System**. For more information about the operations, select:

- Save to Profiles
- Change Running System

Change Running System

If you change the security settings for the activated logical partitions, click **Change Running System** if you want the new settings to take effect immediately.

The selected Central Processor Complex (CPC) and its active logical partitions are referred to here as the *running system*. Using new settings to change the running system make the security settings currently displayed for CPC's processor running time take effect.

The new settings remain in effect for the CPC and active logical partitions until you either dynamically change their security settings again or activate them (which makes the security settings in their activation profiles take effect).

Note: The running system includes active logical partitions only (as indicated by the **Active** column). Changes made to security settings of inactive logical partitions do *not* take effect upon changing the running system. Consider saving the changes to profiles instead, to make them take effect when the logical partitions are activated.

Save to Profiles

If you change the security settings for the activated logical partitions, click **Save to Profiles** if you want the new settings to take effect whenever the selected Central Processor Complex (CPC) and its logical partitions are activated with the modified profiles.

Saving new settings modifies the following activation profiles:

- A logical partition's security settings are saved in its image profile. The settings take effect whenever the logical partition is activated with its image profile.

Note: Saving security settings to activation profiles saves *all* security settings currently displayed, regardless of when the settings were set. For example, if you used the Change Logical Partition Security window previously to change some of the running system's security settings, those changes are saved in the profiles along with any changes you made presently.

Configure BCPii Permissions

Use this section to enable or disable the Base Control Program internal interface (BCPii) permissions for the selected logical partition.

Enable the partition to send commands
To enable the selected partition to send BCPii commands, select **Enable the partition to send commands**. When selected, the active logical partition can send BCPii commands to other active logical partitions.

Enable the partition to receive commands from other partitions
To enable the selected partition to receive BCPii commands from other partitions, select **Enable the partition to receive commands from other partitions**. When selected, the active logical partition can receive BCPii commands from other active logical partitions.

All partitions
Select this option if you want the selected logical partition to receive BCPii commands from all the active logical partitions.

"Add partition" on page 506 (Selected partitions)
Select this option if you want to remove or add selected logical partitions to receive BCPii commands from the logical partition.

Add
To add a system and logical partition to receive BCPii commands from the logical partition, click **Add**.

Remove
To remove a selected logical partition to receive BCPii commands from the logical partition, click **Remove**.

Additional functions on this window include:

OK
To return to the previous window with updated changes, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add partition

Use this window to specify the partitions from which the target partition can receive BCPii commands.

Enter system and partition manually
System: Enter the system name for the logical partition from which the target partition can receive BCPii commands.

Netid: Enter the Netid name for the selected system.

Partition: Enter the logical partition name from which the target partition can receive BCPii commands.

Select a system and partition
System: Select from the drop-down menu the system for the logical partition from which the target partition can receive BCPii commands.

Netid: The Netid displays for the selected system.

Partition: Select from the drop-down menu the active logical partition from which the target partition can receive BCPii commands.

Additional functions on this window include:

Add
To add the system and partition, click **Add**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Password

Accessing the Change Password task

Note: If you are logged onto the Hardware Management Console using an LDAP user ID, this task is not available.

This task allows you to change your password.

To change your password:

1. Open the **Change Password** task. The Change Password window is displayed.
2. Enter your current password and your new password twice, the second time to confirm it.
3. Click **DONE** to change your password.

Change Password

Use this task to change your password when logging on the console.

A password verifies your user identification (user ID) and your authority to log on the console.

Complete the entry fields, then click **DONE** to change your password and then log on to the console.

Current password
Specify your current password.

New password
Specify a new password for logging on the console.

Confirm new password
Specify the new password again to verify its spelling in this field.

Note: The new password is not displayed as you type it; black dots are displayed instead.

DONE
To change your password to log onto the console, click **DONE**.

CANCEL
To close the window, and return to the window from which you selected the task, click **CANCEL**.

Channel Details

Channel Details

This window displays the current instance information and acceptable status settings for a selected channel path identifier (CHPID) of an image or the physical channel identifier (PCHID) for a selected channel of the CPC.

- **Instance Information** includes the current status of the channel path, and other information about the channel path's operating conditions and characteristics.
- **Acceptable Status** settings determine which of the channel path statuses are acceptable and which statuses are unacceptable. The Support Element console reports when the channel path status becomes unacceptable.

  Review the settings under “Acceptable Status” on page 511. Optionally, use its check boxes and click **Apply** to change the acceptable status settings.

Apply
To apply changes you made to the channel path's acceptable status settings, click **Apply**.

Advanced Facilities
To open the Advanced Facilities window for the selected channel or channel path, click **Advanced Facilities...**.

Channel Problem Determination
To open the Channel Problem Determination window for the selected channel, click **Channel Problem Determination...**.

Cancel
To close the window without saving changes you made to the channel path's acceptable status settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

Instance Information

This window displays the current instance information for the selected channel path identifier (CHPID) of an image or the physical channel identifier (PCHID) for the selected channel of the CPC.

Instance Information includes the current status of the channel path, and other information about the channel path's operating conditions and characteristics.

Status
Displays the current status of the channel path.

Type
Displays one of the following:

- The channel type of the CHPID (displays for a selected CHPID of an image).
- The hardware type of the PCHID (displays for a selected channel of the CPC).
- The Crypto Express2 type (displays Accelerator or Coprocessor).

Crypto
Displays the crypto number assigned to the physical crypto adapter.

CSS.CHPID
Displays all the CSS.CHPIDs associated with that physical channel identifier (PCHID). A CSS identifies which channel subsystems the CHPID belongs to.

FID
Displays the function identifier (FIDs) for the selected channel.

CHPID Characteristics
Displays how the CHPID is defined in the IOCDS; shared, dedicated, or reconfigurable.

Adapter ID
Displays the adapter identification for the selected PCHID.

Port number
Displays the adapter port number for the selected PCHID.

Location
Displays the location number of the cage and card slot in which the channel path's channel hardware is installed. Displays the position number on the card in the slot of the channel path's jack.

Owning Image
If the central processor complex (CPC) is activated, this field indicates whether the channel path is configured to a single image or shared by multiple images.

All Owning Images
Displays one of the following:

- A list of all configured images associated with that CSS.CHPID (selected CHPID of an image).

- A list of all configured images that contain a CSS.CHPID associated with that physical channel identifier (PCHID) (selected channel of the CPC).

Network IDs
Identifies the physical layer 2 LAN fabric or physical broadcast domain. You can use this value to logically associate the system features, adapters, and ports to be physically connected to your network.

Swapped with
Displays the name of the PCHID that it is swapped with. If the PCHID is not swapped, this field displays none.

Acceptable Status

This window displays the current acceptable status settings for the channel path with the selected channel path identifier (CHPID) or the selected physical channel identifier (PCHID). *Acceptable status settings* determine which of the channel path statuses are acceptable and which statuses are unacceptable. Use the check boxes to change the settings:

- A check mark in a check box indicates an acceptable status.
- Otherwise, an empty check box indicates an unacceptable status.
- To change one setting to the other, click once on the check box.

The Support Element console continuously monitors the statuses of the channel path and compares them to the channel path's acceptable status settings.

While the statuses are acceptable, the background of the CHPID icon or PCHID icon has no color. An *exception* occurs when a status becomes unacceptable. The console reports an exception to the console operator by changing the background color of the CHPID or PCHID to the color set for indicating its specific unacceptable status. The color displayed to the right of each status in the group box is the color currently used for the background color of the CHPID or PCHID when the status is the cause of an exception. That is, the color set for a status is displayed only when the status is unacceptable and it is the current status of the channel path.

Note: To change the color set for a status, open **Support Element Settings**.

So setting the channel path's acceptable status settings allows you to control which statuses are reported as exceptions:

- Acceptable statuses, indicated by check marks in their check boxes, are not reported as exceptions.
- Unacceptable statuses, indicated by empty check boxes, are reported as exceptions.

Check stopped
The channel path is unavailable due to a permanent machine error affecting the channel hardware. The channel path is not operating.

Definition error
The channel path specified in the active input/output configuration data set (IOCDS) does not match the characteristics of the installed channel, or the channel type is incompatible with the current storage allocation, or the level of the installed channel hardware does not support the definition in the IOCD. The channel path is not operating.

Initializing
The firmware is being loaded into the channel card and then the channel card is starting.

Loss of signal
The channel path detected a link-signal error. The level of the signal on the link is below the value specified for reliable communication.

Loss of synchronization
The channel path detected a link-signal error. The bit synchronization with the signal was lost. The channel path is not operating

Not Defined
The channel path is not defined in the active IOCDS. The channel path is not operating.

No operational link
The channel path detected a link failure due to a not-operational sequence. The channel path is not operating.

No Power
The power is off for the hardware that supports the channel path. The channel path is not operating.

Operating
The channel path is operating.

Permanent error
The channel path is unavailable due to a permanent outboard error. The channel path is not operating.

Service
The channel path is in single channel service (SCS) mode and is not in the active I/O configuration. The channel path is not operating.

Suspended
The channel path is suspended. The channel path is not operating.

Wrap block
A wrap block is installed on the channel path's channel interface.

Note: Wrap blocks are used during special diagnostic tests performed on the channel. Wrap blocks must be removed prior to system initialization to allow the channel to initialize completely. The channel path is not operating.

Sequence time-out
The channel path detected a link failure due to a sequence time out. The channel path is not operating.

Sequence not permitted
The channel path detected a link failure due to an illegal sequence for a link. The channel path is not operating.

Terminal condition
The channel path is not available due to an interface-hung condition. This can occur after an interface or channel error if the control unit or device fails to disconnect from the interface when requested by the channel. The channel path is not operating

Offline signal received
The channel path detected an offline sequence, indicating that the sender is in offline mode and subsequent link-signal errors detected by the channel path are not to be reported. For an ES conversion channel, this condition can occur only when the channel is wrongly attached to another channel, switch, or control unit instead of an ESCON Converter. The channel path is not operating.

Test mode
The channel path is in test mode. The channel path is not operating

Bit error threshold exceeded
The number of bit errors the channel path detected while receiving or sending data is more than the threshold set for its bit error counter. The channel path is not operating

IFCC threshold exceeded
The number of interface control checks (IFCCs) the channel path detected is more than the threshold set for its IFCC counter. IFCCs may continue to occur, but their error logs will not be created and sent to the Support Element.

Stopped
The channel path is not operating.

I/O suppressed
The channel path has input/output (I/O) suppression active. I/O suppression prevents the channel subsystem from selecting any device and fetching the first channel command word (CCW) of a channel program. The channel path is not operating.

Fabric login sequence failure
This condition means that the channel detected a failure during that fabric login procedure

Port login sequence failure
This condition means that the channel detected a failure during the registration procedure. In order for a FICON channel to communicate with devices on a control unit, it must perform a Port Login with that control unit.

State change registration failure
This condition means that the channel detected a failure during the registration procedure. A FICON channel is required to register with the switch to receive state change notification

Invalid attachment failure
Occurs when the channel determines that it is connected to a switch, but the IOCDS specifies that is should be directly connected to a control unit or the contrary.

Save as default
To allow you to change the acceptable status for all of the current objects defined with the same status type, select **Save as default**. After you click **Apply**, a message window appears confirming that you want to proceed with this operation.

Background color of the CPC

While the statuses of the central processor complex (CPC), central processors (CPs), and channels are acceptable, the background of the CPC icon has no color. An *exception* occurs when a status becomes unacceptable. The console reports an exception to the console operator by changing the background color of the CPC to the color set for indicating its specific unacceptable status.

The background color of the CPC indicates unacceptable statuses as follows:

- Until CPC power is turned on and a power-on reset is performed, the background color of the CPC indicates an unacceptable CPC status.
- After CPC power is turned on and a power-on reset is performed:
  - The background color of the left side of the CPC indicates an unacceptable CP status.
  - The background color of the right side of the CPC indicates an unacceptable channel status.

Channel PCHID Assignment

Accessing the Channel to PCHID Assignment task

This task allows you to display the physical locations of all the installed and configured physical channels and the assigned physical channel identifier (PCHID) mapping. The CSS.CHPID associated with the PCHID and a description of the channel hardware type are displayed. The CSS.CHPID identifies the channel subsystem that the CHPID belongs to. You can view the front and back details of a specific cage. An action to write the view to a USB flash memory drive allows you to print the cage view.

To view the channel to PCHID assignments:

1. The central processor complex (CPC) must be power-on reset.
2. Locate the **CPC** to work with.
3. Open the **Channel to PCHID assignment** task.

   Channel to PCHID assignment window displays.
4. Click **View** from the menu bar to display the following menu options:
   - Sort by Channel Location
   - Sort by Cage and PCHID Number
   - Sort by Card Type and PCHID Number
   - Sort by Book and Jack and Fanout
   - Sort by Channel State
   - Sort by PCHID Number
   - Sort by Configured CSS.CHPIDs

- View Cage Details.

5. Click **Search** from the menu bar to display the following menu options:
   - Search by PCHID
   - Search by Configured CSS.CHPID.
6. Click Exit from the **Options** menu bar to exit this window.

Channel to PCHID Assignment

Use the **Channel PCHID Assignment** task to view information that defines the channel location by cage/slot/jack to a physical channel identifier (PCHID). You can sort the view actions by channel location, channel state, or PCHID number. You can also search for a specific PCHID number assignment or configured CSS.CHPID you want to locate.

The CSS.CHPID is a single-digit number that identifies the channel subsystem followed by a decimal point followed by a two-digit number that identifies the channel path. The CSS.CHPID(s) assigned to a PCHID in the IOCDS are displayed if a power-on reset is complete.

You can also view front and back details of a specific cage and an action to write the view to a USB Flash Memory Drive.

To display help for the current window, select **Help** from the menu bar.

The following menu bar choices are available on the **Channel to PCHID Assignment** window. You can find more detailed help on the following elements of this window:

Channel location to PCHID assignment

The Channel location to PCHID assignment displays information that defines the channel location.

Channel Location Cage/Card Slot/Jack
Displays the location number of the cage and card slot in which the channel path's channel hardware is installed. Displays the position number on the card in the slot of the channel path's jack.

Book-Fanout-jack
Displays the number of the book that is connected to the channel card, the fanout, and the jack number on the book that the STI is connected to.

Channel State
Displays the current state of the channel; standby, online, reserved, etc. The CPC must be power-on reset for this state to display.

Physical Channel ID (PCHID)
Displays the physical channel identifier (PCHID) assigned to the cage/slot/jack.

CSS.CHPID
Displays the configured CSS.CHPIDs assigned to a PCHID. The CSS.CHPID is a single-digit number followed by a decimal point followed by a two-digit number. Use the left and right scroll bar to locate all CSS.CHPIDs associated with a PCHID number.

Card Type
Displays the card type for the current channel.

View

To display information for the channel PCHID assignments, select **View** from the menu bar. You can sort information from the view actions by channel location, channel state, or by the physical channel identifier (PCHID) number.

Select an action from the list to get additional help.

Sort by Channel Location
Displays the channel to PCHID assignment sorted by cage, card slot, and jack.

Sort by Cage and PCHID Number
Displays the channel to PCHID assignment sorted by cage and then the current PCHID number assignment in ascending order.

Sort by Card Type and PCHID Number
Displays the channel to PCHID assignment sorted by card type and then the current PCHID number assignment in ascending order.

Sort by Book and Jack and Fanout
Displays the book number, the jack number on the book, and the Memory Bus Adaptor (MBA) number.

Sort by Channel State
Displays the channel state if the CPC is power-on reset; standby, online, reserved, etc.

Sort by PCHID Number
Displays the channel to PCHID assignment sorted by PCHID number.

Sort by Configured CSS.CHPIDs
Displays the channel to PCHID assignment sorted by the configured CSS.CHPID number.

View Cage Details
Displays the image of both front and back of the cage and the PCHID values in each card slot.

View Cage Details

Use **View Cage Details** to view the front and back of a specific cage. The cage view identifies the PCHID assignments and the configured CSS.CHPIDs associated with the card slot and jack. You can write the cage view to a USB Flash Memory Drive in a printable format.

Select Cage
Select the number of the cage you want to view from **Select Cage** list.

Side View
Select the front or back view radio button from the **Side View** box.

Apply
To apply the changes made to the cage view without closing the window, click **Apply**.

Write to USB Flash Memory Drive
To download the front and back view of the selected cage to a USB Flash Memory Drive, click **Write to USB Flash Memory Drive**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Search

Use the **Search** actions to locate and highlight a specific PCHID assignment or configured CSS.CHPID from the **Channel to PCHID assignment** window.

Enter search text
Enter the PCHID assignment or CSS.CHPID you want to locate.

OK
To locate and highlight a specific PCHID assignment or CSS.CHPID in the **Channel to PCHID Assignment** window, click **OK**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Channel Problem Determination

Accessing the Channel Problem Determination task

You can use the support element workplace to determine the state and status of specific channel paths in the input/output (I/O) configuration of the central processor complex (CPC). The label for each channel path's icon includes its physical channel identifier (PCHID), state, and status. When you need more detailed information on determining problems, you can use the support element workplace to perform channel problem determination. Perform channel problem determination to get the following types of information, referred to as *problem determination information*, for a channel path:

- Analyze channel information...
- Analyze subchannel data...
- Analyze control unit header...
- Analyze paths to a device...
- Analyze device status...
- Analyze serial link status...
- Display message buffer status...
- Fabric login status...
- Analyze link error statistics block...
- Optical Power Measurement.

If you have experience using other systems, you may have performed *input/output (I/O) problem determination* to get similar information for a channel path.

To perform channel problem determination:

1. Open the **Channel Problem Determination** task.

   The Partition Selection window lists the logical partitions which problem determination can be performed.
2. Select from the list the logical partition that you want to perform problem determination.
3. Click **OK**.

   The Channel Problem Determination window lists the types of problem determination information you can get for the selected channel.

   Note: The channel you selected to start the task is the task's initial input. One or more windows are displayed if additional input is needed to display the type of information you want.
4. Select the radio button beside the type of problem determination information you want, then click **OK**.

   Follow the instructions on each subsequent window, if any, to provide the additional input needed to display the type of information you selected.

   Upon providing the additional input, if any, the channel's problem determination information is displayed.

Choose a Disconnected Session

Choose a Disconnected Session

This window appears when you have logged back on to the console after previously disconnecting. A list of disconnected sessions is displayed for the specified user.

List of disconnected sessions
This list displays the sessions that have been previously disconnected by the specified user ID.

Session Id
Specifies the identification number associated with the disconnected session.

Disconnect Time
Specifies the time the session was disconnected.

Creation Time
Specifies the time the session originally started.

Running Tasks
Specifies the number of tasks that are currently running in that session.

Reconnect
To reconnect to the session you have selected in the list, click **Reconnect**.

New Session
To connect to a new session rather than a session that has been disconnected, click **New Session**.

Delete
To delete a disconnected session that you no longer need to work with, click **Delete**.

Note: If you delete the last disconnected session from the list, you will be immediately logged on with a new session since there are no longer any disconnected sessions to choose.

Cancel
To close this window and return to the welcome window without connecting, click **Cancel**.

Help
To display help for the current window, click **Help**.

Common Targeting

Common Targeting

Use this window to perform an action on a selected target object.

Click a menu option to select an action you want to perform on the target object. Detailed help is available when a target object and action are selected.

Click **Refresh** to redisplay the selection list.

Concurrent Upgrade Engineering Changes (ECs)

Accessing the Concurrent Upgrade Engineering Changes (ECs) task

Notes:

- The CPC(s) must be placed in Service Status before starting this task.
- You cannot perform this task remotely.

This task upgrades Engineering Changes (ECs) concurrently for a specified Central Processing Complex (CPC) eliminating the need for down time when you are adding the new functions.

To concurrently upgrade engineering changes:

1. Select a CPC (server).
2. Open the **Concurrent Upgrade Engineering Changes (EC)** task. The Concurrent Upgrade Engineering Changes window is displayed.
3. Choose the action to perform in the order as it is displayed.

   Preload EC
   Options for loading the engineering changes in order to upgrade the CPC to a new level.

   Activate EC
   After selecting a Preload option this action switches the CPC to a new level.

Query function availability from last activate
After activating the upgrade a table is displayed indicating new functions that were disabled or unavailable.

Query concurrent upgrade requirements
Determines if the concurrent upgrade requirements have been met.

4. Click **OK** to proceed with the upgrade.

For more detailed information on the Concurrent Upgrade Engineering Changes (CUEC) and how to use this task, see "Enhanced driver maintenance" on page 518.

Enhanced driver maintenance

This section discusses the Concurrent Upgrade Engineering Changes (CUEC) feature that eliminates the need for downtime when you are adding new functions. You can upgrade the firmware engineering change (EC) drivers to the next EC level without any performance impact during an upgrade. A system outage is no longer required in order to take advantage of most, if not all, new enhancements. Enhanced driver maintenance is performed by the support system.

Switch points

The firmware components include:

- Support Element (SE)
- Flexible Service Processor (FSP)
- Power
- LPAR
- Coupling Facility Control Code (CFCC)
- i390 / Millicode
- Channels.

Each of these firmware components has its own EC stream to release code fixes and new functions to the field.

When CUEC is used to upgrade the firmware, the driver GA^{n} to driver GA^{n+1} has designated switch points. This means that each GA^{n} firmware EC stream must be at a specified internal code change level, and the initial CUEC activation can only transition to a specified internal code change level for each GA^{n+1} EC stream.

Not every fix bundle supports CUEC. Therefore, as part of the fix-apply process, your operator must make a decision whether to apply internal code changes above a CUEC switch point. You must develop a plan that indicates when to use CUEC to go to the next GA level and map this plan to an IBM published plan for CUEC switch point release dates (refer to Resource Link (www.ibm.com/servers/resourcelink)). If another scheduled CUEC switch point release is shown to be prior to your targeted GA upgrade date, you can apply fixes above the current CUEC switch point. However, if no additional CUEC switch point releases are planned before the GA upgrade target, your operator should not apply internal code changes above the current CUEC switch point.

Note: It is not recommended to remove fixes in order to get back to a CUEC switch point.

Concurrent Upgrade Engineering Changes (EC) task

Use the **Concurrent Upgrade Engineering Changes (EC)** task to take you through the proper steps for a successful CUEC.

1. Select the CPC you are updating.

2. Open the **Concurrent Upgrade Engineering Changes (EC)** task. The Concurrent Upgrade Engineering Changes window is displayed.
3. Choose the action to perform in the order as it is displayed (refer to the appropriate sections for more information):
   - "Preload EC" on page 519
   - "Activate EC" on page 520
   - "Query function availability from last activate" on page 521 (recommended).
4. Click **OK** to proceed.

Preload EC

The **Preload EC** action is the first step in the CUEC process to initially preload the alternate SE with the GA^{n+1} code while the primary SE and the system continue to operate using the GA^{n} code.

From the Concurrent Upgrade Engineering Changes (EC) window:

1. Select **Preload EC** to load engineering changes in order to upgrade the CPC to a new level. (This option is available only if your user ID is assigned the service representative task role.)
2. The Preload Options window is displayed.
3. Choose an option, then click **OK** to proceed.

Initial preload options

The **Initial Preload** options put the base GA^{n+1} driver on the alternate SE using the CUEC AROM. Choose one of the **Initial Preload** options:

- **Initial Preload including internal code changes from the support system** – upgrades the CPC to a new level and then automatically retrieves and installs all applicable internal code changes from the support system.
- **Initial Preload only** – upgrades the CPC to a new level without retrieving related internal code changes.

The only difference in these two options is that the first option downloads any additional fixes that were released after that CUEC AROM was released.

When one of the initial preload options is selected, the HMC validates that the CUEC AROM appropriately matches the from-GA^{n} system EC. Then, a check is made to ensure that the CUEC GA^{n} switch point requirements are met. If CUEC minimum internal code change requirements are not satisfied, but no CUEC maximum requirement has been exceeded, the operator is given the option to concurrently apply additional GA^{n} internal code changes in order to meet the CUEC requirements. If at least one CUEC maximum internal code change requirement has been exceeded, the operator is told that the CUEC is not possible. It is not recommended to remove fixes. You must wait for the next CUEC switch point.

Once the validation process has successfully completed, the Hardware Management Console triggers the download of the new GA^{n+1} code onto the alternate SE. Configuration and customization data are preserved during this transition from GA^{n} to GA^{n+1} code.

Finally, if the CUEC initial preload option included the request to retrieve internal code changes, the alternate SE would retrieve from the support system any additional internal code changes that were not part of the CUEC AROM. These additional internal code changes would be applied on the alternate SE hard disk following certain defined restrictions because the CUEC activation process must concurrently manage the firmware updates in memory where that firmware executes.

Additional preload options

The **Additional Preload** options can be executed only after the initial preload has been performed. These options allow the download of additional fixes that were not part of the initial preload step.

- **Additional Preload of internal code changes from the support system** – retrieves and installs all applicable internal code changes from the support system.
- **Additional Preload of internal code changes from removable media** – retrieves and installs all applicable internal code changes from removable media.

Activate EC

The **Activate EC** option is the second step of the CUEC process.

From the Concurrent Upgrade Engineering Changes (EC) window:

1. Select **Activate EC**. (This option is available only if your user ID is assigned the service representative task role.)
2. Then click **OK** to proceed.
3. The following three phases are part of the activation process before the activation of the upgrade is complete:
   a. “Preparation” on page 520
   b. “Transition” on page 520
   c. “Completion” on page 520.

The following three phases are included for the activation of the upgrade.

Preparation

The preparation phase makes sure that the following requirements are verified before the code switch starts:

- The concurrent patch feature is enabled.
- The CUEC GA^{n} switch point requirements are met (if the internal code changes applied to the GA^{n} code on the primary SE changed since the CUEC preload).
- No pending conditions from previous CUEC or concurrent patch sessions exist.
- There is enough free memory for the additional GA^{n+1} HSA. The driver information contains the CUEC GA^{n+1} memory requirements. If there is not enough memory, then you are told how much memory to free. You must provide memory by deactivating a partition or varying off storage in a partition if the complete memory is used.

Transition

The transition phase is the heart of the CUEC activate because it is in this step that the GA^{n+1} code is applied in each firmware subsystem memory. The Support Element (SE) is the first subsystem to have its GA^{n+1} code loaded and this is done by executing a CUEC alternate SE switch. This causes the GA^{n+1} code to become the new primary SE while the GA^{n} code becomes the new alternate SE. The GA^{n+1} new primary SE must restart and perform a warm-start resynchronization with the other firmware subsystems. Once the primary SE completes its warm-start synchronization, it serially triggers each of the subsystems to load its GA^{n+1} firmware.

Completion

The completion phase includes a hardware message that could be displayed directing the operator to invoke two tasks to complete the GA^{n+1} transition from those exception firmware subsystems.

- **Query Channel/Crypto Configure Off/On Pending** - this task allows the operator to see which channels and cryptos must be configured offline and put back online in order to get the GA^{n+1} code loaded.
- **Query Coupling Facility Reactivations** - this task informs the operator whether any coupling facility (CF) partitions must be reactivated in order to move the CFCC code for that partition to GA^{n+1}.

Query function availability from last activate

Once the CUEC activate is complete the final step of the CUEC process is performed.

From the Concurrent Upgrade Engineering Changes (EC) window:

1. Select **Query function availability from last activate**, then click **OK**.
2. The Query Function Availability from Last Activate window is displayed. A list of functions which are not yet available or have not yet been enabled after the CUEC process completed is displayed in the window.

   or

   A message window is displayed, indicating that all functions are enabled and available.

This option addresses the exception cases where one or more new GA^{n+1} functions cannot be made available during the CUEC activation process. Some possible reasons why these functions are not available include:

- Not all subsystems have moved to the GA^{n+1} code level. The operator can use the **Query Channel/ Crypto Configure Off/On Pending** and **Query Coupling Facility Reactivations** Support Element tasks to ensure that the GA^{n+1} code level transitions have completed. Once this GA^{n+1} code level validation is completed, the operator can invoke the **Query Function Availability from Last Activate** option to see what functions are still not available.
- One or more exception functions might require some additional action to finalize the enablement/ availability for those functions. This could include an action such as configuring off/on for certain types of channel or processors.

See Resource Link (www.ibm.com/servers/resourcelink) for descriptions of the new functions available for the GA^{n+1} release. They can also inform you of any additional actions required to fully enable/make available any functions that can be displayed on the **Query Function Availability from Last Activate** window.

Completing the upgrade

Once you have permanently moved to the GA^{n+1} level on the primary system you need to bring the alternate system to the GA^{n+1} level. To accomplish this upgrade, proceed with the following:

1. Use the **Backup Critical Data** task on the GA^{n+1} system.
2. Using the CUEC AROMs, perform a hard disk restore on the GA^{n} system.
3. From the **Restore Critical Data** window, select the backup file needed to restore the critical data, then click **OK**.

Concurrent Upgrade Engineering Changes (ECs)

This task allows you to choose an action that you want to perform on a specified Central Processing Complex (CPC) for concurrently upgrading Engineering Changes (ECs).

Preload EC
To load Engineering Changes (ECs) in order to upgrade the CPC to a new level, select **Preload EC**.

Note: This option is available when you are accessing this task with a user ID definition that is based on the *Service Representative* task roles.

Activate EC
To switch the CPC to a new level of Engineering Changes (ECs), after selecting a **Preload option**, select **Activate EC**.

Note:

1. Some new functions may not be available until the next power-on reset.

2. This option is available when you are accessing this task with a user ID definition that is based on the *Service Representative* task roles.

Query function availability from last activate
To determine if any of the new functions are disabled or are not yet available after completing the **Activate EC** option, select **Query function availability from last activate**.

Query concurrent upgrade requirements

To determine if the concurrent upgrade requirements have been met, select **Query concurrent upgrade requirements**. The upgrade requirements include:

- Minimum/maximum levels
- Power-on reset pending conditions
- Channel/crypto configure off/on pending conditions
- Coupling facility reactivation conditions

If all the upgrade requirements are not met, click **Details...** on the **Query Concurrent Upgrade Requirements** window for more information.

OK
To proceed with the selection you have made, click **OK**.

Cancel
To exit this task without executing the selection you have made, click **Cancel**.

Help
To display help for the current window, click **Help**.

Activate Bundle

This window allows you to choose which bundles you want to activate on the Engineering Changes (ECs).

Activate all preloaded bundles
To activate all the preloaded bundles, select **Activate all preloaded bundles**.

Activate a specific preloaded bundle
To activate only a specific preloaded bundle, select **Activate a specific preloaded bundle**, then specify the bundle level in the **Bundle level** field. This option is not available to systems before Version 2.14.0.

OK
To proceed with the selection you made, click **OK**.

Cancel
To return to the previous window without running with the selections you made, click **Cancel**.

Help
To display help for the current window, click **Help**.

Preload Options

This window allows you to choose which preload options you want to perform to load the Engineering Changes (ECs).

The two **Initial Preload** options load files from a Concurrent Engineering Changes AROM DVD. Those files can be updated with applicable internal code changes as part of the **Initial Preload** or you can select one of the two **Additional Preload** options.

Initial Preload including internal code changes from the support system
To load Engineering Changes (ECs) in order to upgrade the CPC to a new level and then automatically retrieve and install all applicable internal code changes from the support system, select **Initial Preload including internal code changes from the support system**.

Initial Preload only
To load Engineering Changes (ECs) in order to upgrade the CPC to a new level without retrieving related internal code, select **Initial Preload only**.

Additional Preload of internal code changes from the support system
To retrieve and install all applicable internal code changes from the support system after completing one of the **Initial Preload** options, select **Additional Preload of internal code changes from the support system**.

Additional Preload of internal code changes from removable media
To retrieve and install all applicable internal code changes from removable media after completing one of the **Initial Preload** options, select **Additional Preload of internal code changes from removable media**.

After you click **OK**, the Select Media Device window is displayed.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

OK
To proceed with the selection you have made, click **OK**.

Cancel
To exit this task without executing the selection you have made, click **Cancel**.

Help
To display help for the current window, click **Help**.

Query Function Availability from Last Activate

This window lists the functions provided by the new level of Engineering Changes (ECs) that are not yet available for use after completing the **Activate** option.

EC
Specifies the Engineering Change (EC) number of the System EC stream.

Query Function Availability table
This table displays the functions that are disabled or unavailable after completing the **Activate** option. A message appears if the functions are enabled and available.

Function
Specifies the name of the enhancement.

Enabled
Indicates whether or not the function has been enabled as part of the concurrent upgrade. If **no** appears, the **Activate** option has failed and you need to contact your Service Representative.

Available
Indicates whether the function is currently provided. If the function is enabled and not available, the next power-on reset will make the function available.

OK
To return to the previous window after viewing the functions and their availability, click **OK**.

Help
To display help for the current window, click **Help**.

Query Concurrent Upgrade Requirements

This window displays the status of the concurrent upgrade requirements. The requirements include:

- Minimum/maximum level requirements
- Power-on Reset pending conditions
- Channel/Crypto configure off/on pending conditions
- Coupling Facility reactivation conditions
- Suggested Actions

OK
To close this window and return to the previous window, click **OK**.

Details...
To display more information on the concurrent upgrade requirements that were not met, click **Details...**.

Help
To display help for the current window, click **Help**.

Configure 3270 Emulators

Accessing the Configure 3270 Emulators task

Note: You cannot perform this task remotely.

This task configures the Hardware Management Console to automatically start one or more 3270 emulator sessions when the Hardware Management Console application starts.

A 3270 emulator is an application that allows 3270 terminal emulation from the Hardware Management Console to a host operating system. When configuring a 3270 emulator, you must specify the TCP/IP address of the target system.

To configure 3270 emulators:

1. Open the **Configure 3270 Emulators** task. The Configure 3270 Emulators window is displayed.
2. From this window you can add a new host address, delete an existing host address, or start a 3270 host emulator session.
3. Click **OK** to save your changes.

Configure 3270 Emulators

Use this task to configure the console's 3270 emulator.

The console's **3270 emulator** allows 3270 terminal emulation at the console to a host operating system. Configure the emulator to set up whether and how you want 3270 emulator sessions started whenever the console Application is started.

OK
To save your changes, click **OK**.

Cancel
To cancel your request to configure the emulator sessions and close this window without saving any changes, click **Cancel**.

Edit Keymap
To edit the 3270 emulator session keymap, click **Edit Keymap**.

Help
To display help for the current window, click **Help**.

See the following for additional information:

Configured 3270 Emulator Sessions

This window lists the current 3270 emulator sessions you have configured when starting the console Application.

When the emulator is **disabled**, starting the console Application does **not** start any 3270 emulator sessions. Any 3270 emulator sessions that are already active remain active. To start a disabled 3270 emulator session, you must select that address from the list and click **Start**.

New...
To add a new 3270 host address to the list of configured 3270 emulator sessions, click **New...**.

Delete
To remove a 3270 host address from the list of configured 3270 emulator sessions, select the host address, then click **Delete**.

Start
To start a 3270 host emulator session that was originally set to disabled, select the host address, then click **Start**.

Add 3270 Emulator Session

Use this window to add a 3270 host address to the list of configured 3270 emulator sessions available for the console and choose to have it enabled or disabled when the console Application is started.

Host Address

Specify a host address, to configure for the 3270 emulator, you want enabled or disabled whenever the console Application is started (and no 3270 emulator sessions are already active).

A specific port to use may be specified by appending it with a ':' (for example, `192.168.10.2:23`)

A specific LU name to use may be specified by prepending it with an '@' (for example, `LUname@192.168.10.2:23`)

To force the 3270 session to operate through a TLS tunnel, prepend the entry with ’L:’ (for example, `L:LUname@`*`yourserver`*`.com:923`)

If this task encounters a certificate error when "L:" is not prepended to the value in the host address, then the “Certificate Management” on page 438 task should be used to import the certificate used to protect the host.

When you finish configuring the console's 3270 emulator, click **OK** to save the settings.

Note: The number of emulator sessions is ignored if any 3270 emulator sessions are already active when the console Application is started. All active sessions remain active and no new sessions are started.

When the 3270 session is operated through a TLS tunnel, the authenticity of the certificate that is returned by the 3270 server is authenticated. If the certificate is not signed by a well known Certificate Authority (CA) certificate, the signing certificate(s) will need to be configured as trusted by this console. See “Manage Trusted Signing Certificates” on page 446 under the **Certificate Management** task for more details. In addition, the Common Name (CN) within the certificate that is returned by the 3270 server must match that specified for the Host Address value excluding the "L:" prefix and any port postfix specified.

Start at Console Startup
To start the 3270 emulator session when the console Application is started, select **Enabled**. Otherwise, select **Disabled**.

OK
To add the host address to the list of configured 3270 emulator sessions, click **OK**.

Cancel
To cancel your request to configure the emulator sessions, close this window without saving any changes, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Keymap

Use this task to edit the console's 3270 emulator keymap.

To change the default keyboard key mapping for your preference, edit the keymap.

When you edit the keymap for the first time the new keymap defaults to a mapping that resembles the default keymap for thePersonal Communications (PCOM) emulator. You can keep these settings or modify them.

However, before modifying the keymap, you should familiarize yourself with the “Keymap syntax Rules” on page 526. For more information, see the x3270 website (x3270.bgp.nu) and the How to Create a Custom x3270 Keymap website (x3270.bgp.nu/Keymap.html). The key points include:

- “Keymap syntax Rules” on page 526
- Key symbols (keysyms) you can specify
- Actions you can assign to the keysyms.

Keymap syntax Rules

A general overview of the keymap syntax rules include:

- The first line is always:

  x3270.keymap.*hmc*: #override

  where:

  hmc is the keymap name you will use for the console. This line must not change.
- The middle lines are in the format:

  modifier <Key> keysym : Action(args)\n\

  where:

  modifier is an optional keyboard modifier like `Ctrl` or `Shift`
  keysym is an X11 keysym: a symbolic name for a key, like `Prior` (the Page Up Key)
  Action is an x3270 action such as `Enter()` or `PF(7)`
  args are optional action arguments, such as the number of a PF key, like `PF(7)`.

  Note: These lines **must** end with the characters \n\.
- The last line is the same as the middle lines, except it **must not** end with the characters \n\.
- More specific key definitions must come before less specific definitions. For example, the definition for `Shift<Key>Backspace` must come before the definition for `<Key>Backspace`.
- There cannot be any comments or blank lines in the keymap.

To find out what keysyms are generated for any given key on your keyboard, start a 3270 Emulator session. Then select the **File->Trace Keyboard and Mouse Events** menu option, and click **No File** in the pop-up window. An xterm window appears. Click on the 3270 session window to bring it back to the forefront. Each time you press a key in the 3270 session window, several lines appear in the xterm window. The text enclosed in single quotes after the word "Event" is the keysym for the key(s) you pressed, and the text after the "->" is the current action defined for the key(s). Refer to the x3270 Manual Page website (x3270.bgp.nu/x3270-man.html#actions) for a list of actions you can use in your keymap.

Once you have completed editing the keymap, click **OK** to save the keymap. Some syntax checking is performed by this task to ensure the syntax has been followed as outlined above. Test any specific keysym changes you made to ensure they are working as you prefer. To test your changes, follow the instructions above to see what actions are generated for the keysyms you specifically changed. If changes you made are not working as expected, you should check that the emulator has accepted all your keysym mappings by selecting the **Options->Display Current Keymap** menu option. This will open the x3270 Keymap window. Scroll down to find the *hmc* keymap and its keysym mappings. If any keysyms you changed are not displayed, this means the emulator found a problem with that keysym syntax, the keysym or the action specified. You should edit the *hmc* keymap again, review this keysym mapping, make corrections as needed and test the changes again.

To completely remove this *hmc* keymap definition, delete the syntax from the input area and click **OK**. To add this *hmc* keymap definition again with its original syntax, start the entire process again once you have removed the definition.

These keymap settings will be saved as part of the Save Upgrade Data task so that you can preserve them across console upgrades.

Making the new keymap take effect

When you finish editing the keymap, click **OK** to save the keymap. To make the new settings take effect:

- Close all active emulator sessions.
- Restart the emulator sessions.

Additional options are available from this window:

OK
To save the changes to the emulator keymap, click **OK**.

Cancel
To cancel your changes to the emulator keymap, close this window without saving any changes, and return to the previous window. click **Cancel**.

Help
To display help for the current window, click **Help**.

Configure Backup Settings

Accessing the Configure Backup Settings task

This task allows you to define your backup settings if you are using an external server to backup your files.

To configure your server:

1. Open the **Configure Backup Settings** task. The Configure Backup Settings window is displayed.
2. Enter the required FTP site address, user ID, and password information.
3. To enable a secure FTP connection to your server, select **Use secure FTP**.
4. When you have completed the entries, click **OK** to apply the settings.

FTP Server Information / Configure Backup Settings

Use this window to configure FTP settings when you use an external server to back up your files or when you are transferring data for the following tasks:

- Analyze Console Internal Code
- Change Console Internal Code
- Retrieve Internal Code (targeting an object)
- Backup Critical Data
- Save Upgrade Data

Host name
Specify the host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then

click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.

- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To apply this information, click **OK**.

Clear
To remove all information from the input fields, click **Clear**.

Cancel
To close the window without providing information, click **Cancel**.

Help
To display help for the current window, click **Help**.

Configure Channel Path On/Off

Accessing the Configure Channel Path On/Off task

Notes:

- Configure Channel Path On/Off is considered a disruptive task. If the object is locked, you must unlock it before continuing.
- Depending on your user task role, you may only be able to view this task.

This task configures channel paths on and off. *Configure on* and *configure off* are channel path operations you can use to control whether channel paths are online or on standby in the active input/output (I/O) configuration:

- A channel path is *online* while configured on. It is in the active I/O configuration and it can be used.
- A channel path is on *standby* while configured off. It is in the active I/O configuration but it cannot be used until it is configured on.

If you have experience using other systems, you may have used a CHPID command with ON and OFF parameters to configure channel paths on and off.

You can use the Hardware Management Console workplace to configure channel paths on and off. However, operating systems will not be notified when you use the workplace to configure channel paths on or off. For example, if you configure off a channel path, the operating system running in any image that owns or shared the channel path is not notified, and the next operation from the operating system to the channel path causes an error. It is recommended you use operating system facilities rather than the Hardware Management Console workplace, whenever possible, to configure channel paths on and off.

To use the workplace to configure channel paths on or off:

1. Select a CPC image.
2. Open the **Configure Channel Path On/Off** task. The Disruptive Task Confirmation window is displayed. Since this task may be disruptive to the targeted CPC image, review the confirmation text in the window to decide whether or not to proceed with the task.
3. If you proceed with the task, the Configure Channel Path On/Off window is displayed.
4. The window displays the *current state* and *desired state* of each channel path.
5. Use the window list and actions to *toggle* the desired states of channel paths you want to configure on or off.
6. Click **OK** to make the desired states take effect.

Configure Channel Path On/Off

This window can be used to determine if channel paths can be configured on or off for a Central Processor Complex (CPC) image. For some user task roles the window can be used to configure the channel paths on or off. Configuring channel paths on and off controls whether they are online or on standby in the active Input/Output (I/O) configuration:

- A channel path is *online* while configured on. It is in the active I/O configuration, and it can be used.
- A channel path is on *standby* while configured off. It is in the active I/O configuration, but it cannot be used until it is configured on.

Notes:

1. Operating systems will *not* be notified when you use this window to configure channel paths on or off. For example, if you use the window to configure off a channel path, the operating system running in any image that owns or shares the channel path is not notified, and the next operation from the operating system to the channel path will cause an error. Therefore, whenever possible, it is recommended that you use operating system facilities rather than the **Configure Channel Path On/Off** task to configure channel paths on and off.
2. When the CPC is activated in logically partitioned (LPAR) mode, configuring off a reconfigurable channel path does *not* release it from its assignment to an isolated logical partition.
3. When the CPC is activated in LPAR mode, the **Online pending** state indicates the channel path was configured on while assigned to an inactive logical partition. The channel path will be online when the logical partition is activated.
4. This task may be view only for some user task roles.

To use the **Configure Channel Path On/Off** task:

- The CPC must be power-on reset.
- The CPC must support configuring channel paths from a Hardware Management Console.
- The target image must own at least one channel path.
- Select the image from the Work Pane view you want to configure on or off.

Additional functions on this window include:

OK

When you finish toggling the target states of the channel paths you want to configure on or off, click **OK** to allow the new target states to take effect.

Cancel

To close the Configure Channel Path On/Off window, click **Cancel**.

Help

To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Configure Channel Path on/off table

The window lists the following information for each channel path owned or shared by the image you selected to start the task. Select one or more channel paths, then select **Toggle** from the drop down box to toggle their target states.

ID

Displays the channel path identifier (CHPID) of each channel path.

Current State

Indicates the current state of each channel path.

Desired state

Indicates the target state of each channel path.

Messages
If you attempt to change the target state of a channel path that cannot be configured on or off, this column displays the message "Not Allowed" for the channel path to indicate that changing its state is not allowed.

The icons perform the following functions for the selected configure on/off table:

Select All/Deselect All
You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Current State

This window lists the current state and target of each channel path owned or shared by the image you selected to start the task. Use the select action drop down to *toggle* the target states of the channel paths you want to configure on or off.

- If the current state of a channel path is **Online** or **Online pending,** toggle its target state to **Standby** if you want to configure off the channel path.
- If the current state of a channel path is **Standby,** toggle its target state to **Online** if you want to configure on the channel path.

Online
Indicates the channel path is configured on. It is in the active Input/Output (I/O) configuration and it can be used.

Online pending
When the Central Processor Complex (CPC) is activated in logically partitioned (LPAR) mode, this state indicates the channel path was configured on while assigned to an inactive logical partition. The channel path will be online when the logical partition is activated.

Reserved
Indicates the channel path has service set on. It is not in the active I/O configuration, cannot be configured on, and cannot be used. It will remain out of the active I/O configuration until service is set off. A CHPID can be in the reserved state if it is not defined or incorrectly defined in the active IOCDS.

Standby
Indicates the channel path is configured off. It is in the active I/O configuration but it cannot be used until it is configured on.

Configure Data Replication

Accessing the Configure Data Replication task

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables or disables customized data replication. Customized data replication allows another Hardware Management Console to obtain customized console data from or send data to this Hardware Management Console.

Notes:

- The **Configure Data Replication** task is not supported between Hardware Management Consoles at Version 2.13.0 and Hardware Management Consoles at Version 2.12.1 or lower, due to the introduction of data format versions on Version 2.13.0. You can continue to use this task between Hardware Management Consoles at Version 2.12.1 or lower, or you can use this task within Hardware Management Consoles at Version 2.13.0.
- Customizable console data is accepted from other Hardware Management Consoles only after specific Hardware Management Consoles and their associated allowable customizable data types have been configured.

To customize data replication:

1. Open the **Configure Data Replication** task. The Configure Data Replication window is displayed.

   Note: If a message window is displayed for an extended amount of time (in some cases, several minutes), continue to wait for it to complete, and then determine if any registered data sources are non-communicative. You can click **Status** from the Configure Data Replication window for a "Not Communicating" data source. You can contact the support system if you need assistance.
2. Select **Enable** to obtain customizable data from or send customizable console data to this Hardware Management Console or select **Disable** to prevent the acceptance or sharing of customizable console data with other Hardware Management Consoles.
3. If you select **Enable**, the Configure Data Replication window is displayed.
4. Proceed with the task.

See the following information for details on customizing console data for data replication.

Customizable data replication

The Customizable Data Replication service allows configuration of a set of Hardware Management Consoles to automatically replicate any changes to certain types of data so that the configured set of Hardware Management Consoles automatically keep the data synchronized without manual intervention.

Notes:

- Customizable Data Replication is available only on Hardware Management Consoles at Version code 1.8.0 and later.
- Before you enable this replication service, you might want to save your original data settings in case you need to restore these settings at a future time. See the **Save/Restore Customizable Console Data** task.
- The **Configure Data Replication** task and the **Save/Restore Customizable Console Data** task are not supported between Hardware Management Consoles Version 1.x.x and Hardware Management Consoles Version 2.x.x. They are supported when you want to perform these tasks within Version 1.x.x or within Version 2.x.x.
- The **Configure Data Replication** task is not supported between Hardware Management Consoles at Version 2.13.0 and Hardware Management Consoles at Version 2.12.1 or lower, due to the introduction of data format versions on Version 2.13.0. You can continue to use this task between Hardware Management Consoles at Version 2.12.1 or lower, or you can use this task within Hardware Management Consoles at Version 2.13.0

See the Customizable Data Types listed in the Configure Data Replication section for the types of data that can be configured.

The Customizable Data Replication service can be enabled for the following types of operations:

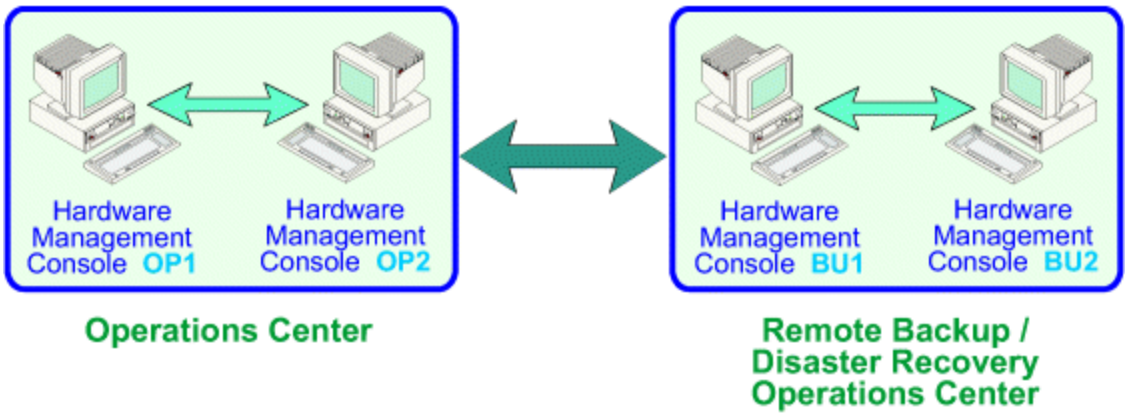
- **Peer-to-Peer** (see “Example 1: Peer-to-peer replication” on page 532)

  Provides automatic replication of the selected customized data types between peer Hardware Management Consoles. Changes that are made on any of these consoles are copied to the other consoles.
- **Primary-to-Replica** (see “Example 2: Primary-to-replica replication” on page 534.)

  Provides automatic replication of the selected customized data types from one or more designated primary Hardware Management Consoles to one or more designated replica Hardware Management Consoles. Changes that are made on a primary console are automatically copied to the replica consoles.

The following examples provide more detailed information:

Example 1: Peer-to-peer replication



1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has Access Administrator roles.
2. Open the **Configure Data Replication** task. The Configure Data Replication window is displayed.
3. Select **Enable** in the **Configure Data Replication** area.
4. Click **New** under **Data Source(s)**. The Configure New Replication Source window is displayed.
5. Select a *Hardware Management Console* to be used as a data source from the **Discovered Console Information** list, and click **Add**.

   or

   Enter the *TCP/IP address* of the Hardware Management Console to be a used as a data source in the **TCP/IP Address Information** input field, and then click **Find**.

   Note: Hardware Management Consoles ***must be*** at Version code 1.8.0 or later.
6. The Configure Data Replication window is displayed again as shown in Figure 27 on page 533.

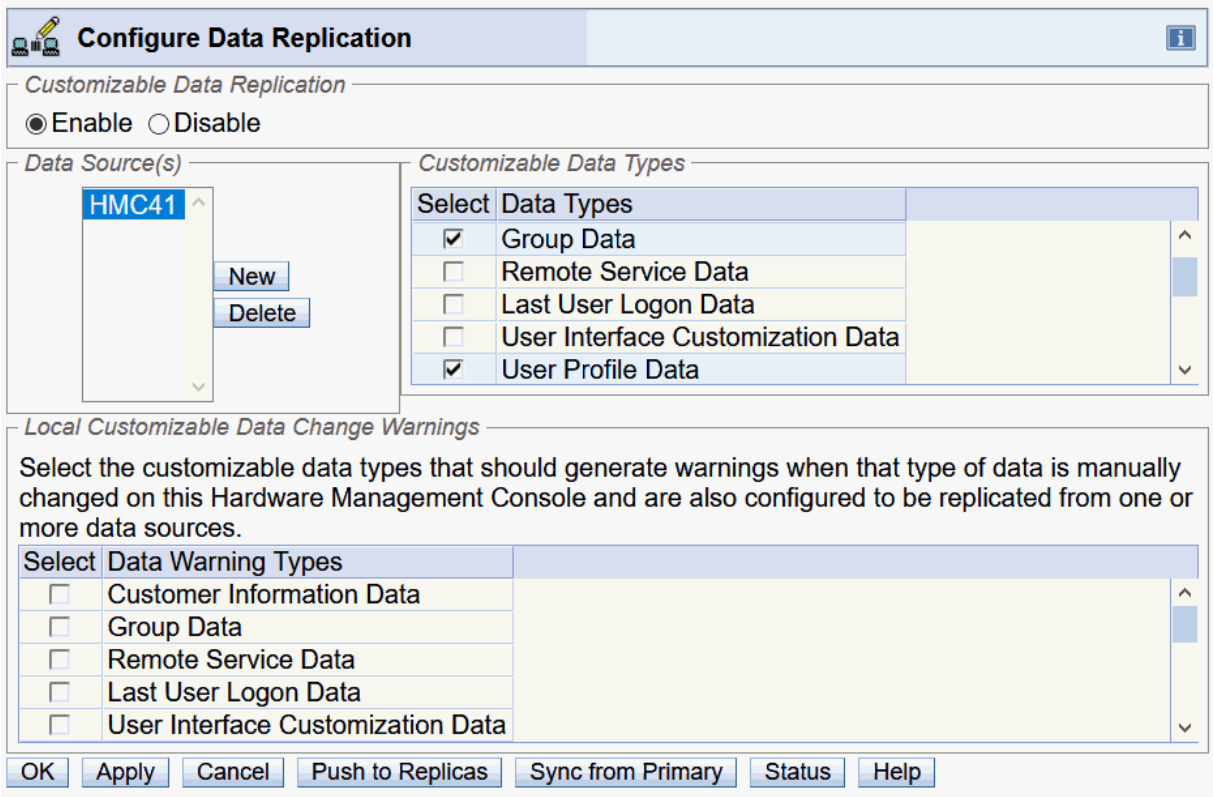
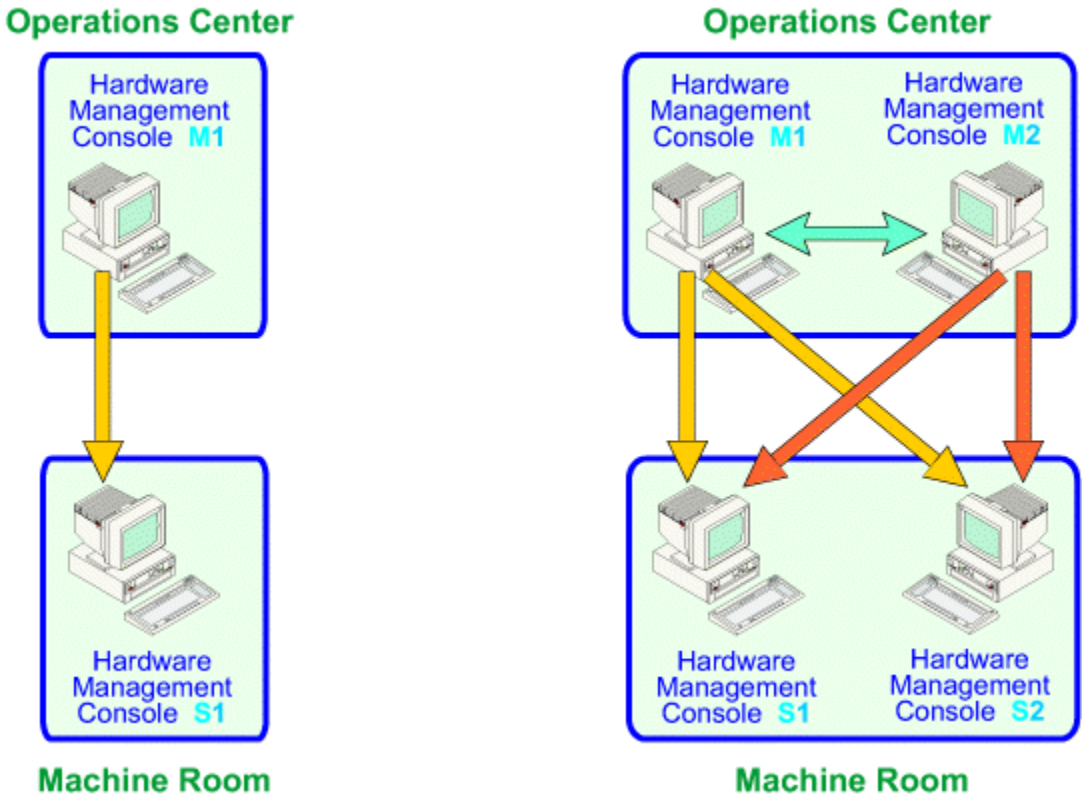


Figure 27. Configure data replication window - example 1

7. Select the types of data from the **Customizable Data Types** list that you want to replicate from a peer Hardware Management Console currently selected under **Data Source(s)**.
8. Choose one of the following actions:
   - Click **OK** to save the changes and close the Configure Data Replication window.
   - Click **Push to Replicas** to transfer all local levels to any communicating replica. The replicas, if they are running this level of code, are instructed to accept the levels from the primary, regardless of the value of their current levels.
   - Click **Sync from Primary** to invalidate the local levels for all properties that are defined to have a primary. This results in an immediate level set where the primary provides their levels to the local machine. This option is not available if the local Hardware Management Console is not defined to have any data sources.
   - Click **Status** to show the status of this task on this machine.
9. Repeat **steps 1** through **8** on each of the Hardware Management Consoles you want to act as peers with one another.
10. Once communication is established between the Hardware Management Consoles, the requested types of customizable data are automatically replicated from one Hardware Management Console to the other immediately following the change in the data itself.

Example 2: Primary-to-replica replication



Setting up a Primary Console(s)

1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has Access Administrator roles.
2. Open the **Configure Data Replication** task. The Configure Data Replication window is displayed.
3. Select **Enable** in the **Customizable Data Replication** area.
4. Click **OK** to close the Configure Data Replication window.

   Note: If you want to configure additional primary consoles, see “Example 1: Peer-to-peer replication” on page 532.

Setting up the Replica Console(s)

1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has Access Administrator roles.
2. Open the **Configure Data Replication** task. The Configure Data Replication window is displayed.
3. Select **Enable** in the **Customizable Data Replication** area.
4. Click **New** under **Data Source(s)**. The Configure New Replication Source window is displayed.
5. Select a *Hardware Management Console* to be used as a primary data source from the **Discovered Console Information** list, then click **Add**.

   or

   Enter the *TCP/IP address* of the Hardware Management Console to be a used as the primary data source in the **TCP/IP Address Information** input field, then click **Find**.

   Note: Hardware Management Consoles ***must be*** at Version code 1.8.0 or later.
6. The Configure Data Replication window is displayed again as shown in Figure 28 on page 535.

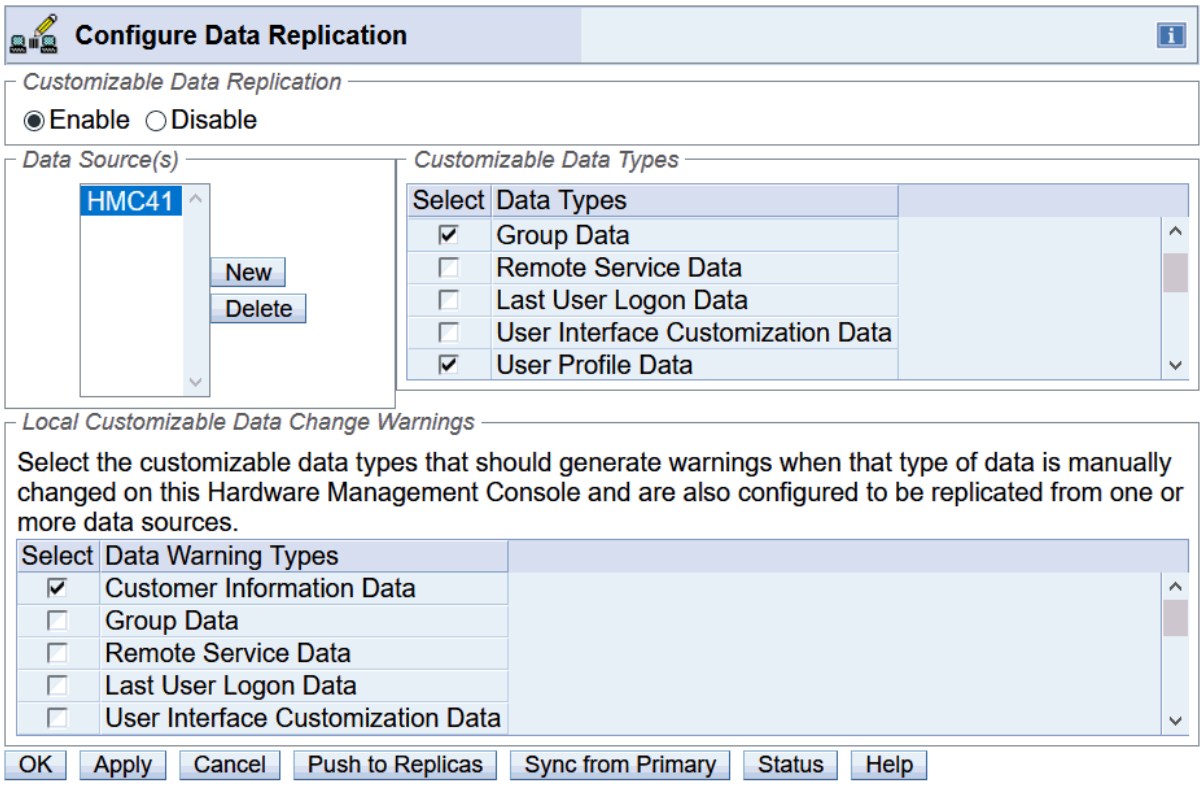


Figure 28. Configure data replication window - example 2

7. Select the types of data from the **Customizable Data Types** list that you want to accept from the Hardware Management Console currently selected under **Data Source(s)**.

   Note: When configuring a Hardware Management Console as a replica, you should check the types of customizable data from the **Local Customizable Data Change Warnings** list that should generate warnings to a user when manual changes are made to that data on this Hardware Management Console.

   If a task is used to change data on a Hardware Management Console that is receiving updates from a configured data source (a primary Hardware Management Console) and a warning is requested for the involved data, the user is shown a warning before the task exits. The warning displays the following choices:

   Request a reset of the data
   The task has already updated the data on the local machine. This option requests that the data is replaced with information from a primary Hardware Management Console the next time communications are active (or immediately if communications are currently active).

   Unconfigure data source for this specific type of data
   The data replication configuration is changed and this data type is not requested from any configured data sources.

   Ignore the warning and continue
   The data replication configuration is not changed but the level indicators on the local machine have advanced because of the local change. If this option is used, updates that are made on primary Hardware Management Consoles might not replicate to this replica.

8. Choose one of the following actions:

   - Click **OK** to save the changes and close the Configure Data Replication window.
   - Click **Push to Replicas** to transfer all local levels to any communicating replica. The replicas, if they are running this level of code, are instructed to accept the levels from the primary, regardless of the value of their current levels.

- Click **Sync from Primary** to invalidate the local levels for all properties that are defined to have a primary. This results in an immediate level set where the primary provides their levels to the local machine. This option is not available if the local Hardware Management Console is not defined to have any data sources.
- Click **Status** to show the status of this task on this machine.

9. Repeat **steps 1** through **8** on any additional Hardware Management Consoles that you want to configure as a replica.
10. Once communication is established between all of the Hardware Management Consoles, the primary console(s) remains synchronized with each other, providing redundancy in the event that one of the primary consoles becomes unavailable. The replica console(s) are kept synchronized with whichever primary console provides the data to them first.

Data replication

As data is replicated from one Hardware Management Console to another, an internal level indicator for the data being replicated is incremented each time the data is altered on the data source. Each Hardware Management Console keeps track of the level indicator for each type of data and will not accept data from a data source when the level indicator is not greater than that on the receiving Hardware Management Console.

If for some reason there is a need to force the replication of data from one or more data sources and the level indicator on the receiving Hardware Management Console is greater than that of the data sources, do the following:

1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has Access Administrator roles.
2. Open the **Configure Data Replication** task. The Configure Data Replication window is displayed (**Enable** should be selected).
3. Deselect all the data types from the **Customizable Data Types** list on the Configure Data Replication window.

   Note: If you just want to reset the level indicator for a particular data type, just deselect that data type.
4. Click **OK** to save the changes and close the Configure Data Replication window.
5. Start the **Configure Data Replication** task again by repeating **step 2**.
6. Select the types of data from the **Customizable Data Types** list that were just deselected in **step 3**.
7. Click **OK** to save the changes and close the Configure Data Replication window.

Note: Deselecting and then reselecting the data types resets the internal level indicators for the specified types of data and forces replication of the data from the data sources.

Configure Data Replication

Use this window to enable or disable the ability of this Hardware Management Console to act as a server of customizable console data and to indicate whether this Hardware Management Console can accept customizable console data that is sent by another Hardware Management Console.

Note: The **Configure Data Replication** task is not supported between Hardware Management Consoles at Version 2.13.0 and Hardware Management Consoles at Version 2.12.1 or lower, due to the introduction of data format versions on Version 2.13.0. You can continue to use this task between Hardware Management Consoles at Version 2.12.1 or lower, or you can use this task within Hardware Management Consoles at Version 2.13.0

For examples on how to use the **Configure Data Replication** task to set up peer-to-peer or primary-to-replica replication, see “Customizable data replication” on page 531.

After you “Enable” on page 537 or “Disable” on page 537 this service and save the settings, this setting becomes effective immediately.

If you select to enable this data replication task this Hardware Management Console is completely configured to act as a server of customized console data, you need to perform further configuration steps

(select data source(s), data types) to control whether this Hardware Management Console accepts customizable console data from other consoles. If there is a problem while configuring and communicating, a message appears at the top of the Configure Data Replication window, click **Status** for more details.

Enable

To allow another Hardware Management Console to obtain customizable console data from or send customizable console data to this Hardware Management Console, select **Enable**.

Note: Customizable console data is accepted from other Hardware Management Consoles only after specific Hardware Management Consoles and their associated allowable customizable data types was configured by using the Configure Customizable Data Replication window.

Disable

To prevent the acceptance or sharing of customizable console data with other Hardware Management Consoles, select **Disable**.

Data Source(s)

This list shows the Hardware Management Console to be allowed as sources for customizable data. As you select entries in this list, the customizable data types that are accepted from the selected Hardware Management Console are shown.

New
To display the "Configure New Replication Source" on page 540 window, which is used to define a new Hardware Management Console as a source of customizable console data for this console, click **New**.

Delete
To remove the currently selected Hardware Management Console in the **Data Source(s)** list, thus making the selected Hardware Management Console no longer a source of customizable console data, click **Delete**.

Customizable Data Types

Select one or more types of customizable console data that are accepted from the Hardware Management Console currently selected in the **Data Source(s)** list. The types of customizable console data that can be replicated are:

Acceptable Status Settings
Any status settings that are considered acceptable for all types of managed objects.

Associated Activation Profiles
Associated activation profile settings for CPC and CPC image objects that are defined in the **Customize/Delete Activation Profiles** task.

Customer Information Data
Customer information for a CPC or group of CPCs that includes the following information about the system being installed:

- Administrator information (customer name, address, telephone number, and so on)
- System information (administrator address)
- Account information (customer number, enterprise number, sales branch office, and so on)

Note: When you select this type of data for replication, this data includes information, such as a branch office, that can make sense only within a specific geographic region.

Group Data
All user-defined groups that are defined to the Hardware Management Console.

Note: When you select this type of data for replication, it is important to remember that the same managed objects are defined on both the receiving and sending Hardware Management Consoles for the replication of this type of data to be the most useful.

Monitor System Events Data
Data for the **Monitor System Events** task includes:

- SMTP server and port settings
- Minimum time between emails setting
- Event monitors

Object Locking Data
Whether to automatically lock all managed objects after they are used as target objects for a task or relock after a task runs.

Outbound Connectivity Data
Configuration data that is specified in the **Customize Outbound Connectivity** task for making outbound connections. This data type also includes configuration data that is specified in the **Configure IDAA Call Home** task for host names or IP addresses of IDAA consoles that are allowed to use this Hardware Management Console (HMC) as a call-home proxy.

Remote Syslog Server Data
Configuration data that is specified in the **Manage Syslog Servers** task for the syslog servers that the Hardware Management Console sends audit and event information to, including which data types are sent.

Remote Service Data
Automated service operations between the console and the support system, includes:

- Enablement of remote service
- Enablement of automatic service call
- Service telephone number configuration

Last User Logon Data
Restoring the enterprise-wide data of the newest logon information, replicating automatically from the replica to the primary.

User Interface Customization Data
Restoring the user interface customizations. For example: Masthead favorites and Home tab settings which include Work Pane Table sorts and filters, and Custom Table views. Replicating this data in a peer-to-peer setup allows the user interface to be replicated between all consoles.

User Profile Data

- Customized user IDs defined in the **User Management** task
- Customized user managed resource roles and task roles that are defined in the **User Management** task
- LDAP servers defined in the **User Management** task
- Password profile information that is defined in the **User Management** task
- Logon session properties
- Remote access by using a web browser
- All user settings that are defined in the **User Settings** and **Console Default User Settings** tasks:
  - Any confirmation settings
  - Controls such as displaying single object selections or console messaging
- LDAP user ID
- User pattern and user template definitions
- User settings for synthetic user IDs created by using a template definition

SNMP API Settings
SNMP API configuration information.

Local Customizable Data Change Warnings

Select one or more Data Warning Types to control which types of customizable data should generate warnings to the user when manual changes are made to that data on this Hardware Management Console.

Note: In normal circumstances, it is not recommended for manual changes to be made to a given type of customizable data when that type of data is also configured to be replaced from one or more data sources.

If a task is used to change data on a Hardware Management Console that is receiving updates from a configured data source (a primary Hardware Management Console) and a warning is requested for the involved data, the user is shown a warning before the task exits. The warning displays the following choices:

Request a reset of the data
The task has already updated the data on the local machine. This option requests that the data is replaced with information from a primary Hardware Management Console the next time communications are active (or immediately if communications are currently active).

Unconfigure data source for this specific type of data
The data replication configuration is changed and this data type is not requested from any configured data sources.

Ignore the warning and continue
The data replication configuration is not changed but the level indicators on the local machine have advanced because of the local change. If this option is used, updates that are made on primary Hardware Management Consoles might not replicate to this replica.

Additional functions are available from this window:

OK
To save the changes you made to this window and exit the task, click **OK**.

Apply
To apply the changes you made within this window, click **Apply**.

Cancel
To close this window without saving any changes, click **Cancel**.

Push to Replicas
To drive all local levels to any communicating replica, click **Push to Replicas**. The replicas, if they are running this level of code, are instructed to accept the levels from this primary, regardless of the value of their current levels.

Sync from Primary
To invalidate the local levels for all properties that are defined to have a primary, click **Sync from Primary**.

Note: This option is only available if the local Hardware Management Console is defined to have data sources.

Status
To display the status of the data replication task on this machine, click **Status**. The Data Replication Status window is displayed.

The information that is displayed includes the Currently Defined Data Sources, Current Data Entries, and any replicas that are not at the appropriate level.

Note: Check the status of this task after the connections had time to normalize.

The **Currently Defined Data Sources** provides the following information:

Name
Specifies the resolved host name of the remote data source.

Status
Specifies the last known communication status with the remote data source. The following status is possible:

Communicating
The registered data source is reachable and configured as a data replication source.

Not Communicating
The registered data source is unreachable over the network. A network error occurred while it is trying to contact it, or the Hardware Management Console is determining its current connection status to the source.

Connection Pending
Data replication is attempting its initial connection to a registered data source.

Connection Refreshing
Data replication is attempting a non-initial connection to a registered data source (while it is refreshing local data structures).

Connection Awaiting Start
The indicated data source has not yet connected. An initial connection attempt follows.

Peer Disabled
Connection is established with the registered data source but is disabled for data replication.

Peer Disconnected
The remote primary ended its connection with the local Hardware Management Console.

IP Addresses
Specifies the IPv4 and IPv6 addresses associated with the remote data source.

The **Current Data Entries** provides the following information:

Property Name
Specifies the name of the locally supported data entry.

Local Level
Specifies the revision level of the local entry's data.

Bound to a Primary HMC
Identifies whether the data entry is replicated against a remote data source.

Updated Since Console Start
Identifies whether the data entry replicated since console start.

Under some circumstances, replicas might appear to be at an inappropriate level for a short time because this notification is handled as a low priority notification item by the Data Replication infrastructure.

Help
To display help for the current window, click **Help**.

Configure New Replication Source

Use this window to configure a Hardware Management Console as a new source of customizable data for this console. The new replication source can be defined in one of two ways:

TCP/IP Address Information
You can specify the TCP/IP address of a Hardware Management Console in the **TCP/IP Address Information** field, then click **Find** to try to contact the Hardware Management Console at the specified address. If reached, the Hardware Management Console will be added as a new source of customizable console data; otherwise, an error message is displayed.

Discovered Console Information
You can select an already discovered Hardware Management Console from the **Discovered Console Information** list and click **Add** to add the selected Hardware Management Console as a new source of customizable console data.

After adding the desired customizable data types, you should configure them for the newly added source of customizable console data.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Configure IDAA Call-Home

Accessing the Configure IDAA Call-Home task

This task is used to configure the host names or IP addresses of IDAA consoles that are allowed to use this Hardware Management Console (HMC) as a call-home proxy. Additional configuration is needed on the IDAA console to enable this functionality.

Note: If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data that is specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the **Configure Data Replication** task.

To add a host name or IP address:

1. Open the **Configure IDAA Call-Home** task. The Configure IDAA Call-Home window is displayed.
2. To add a host name or IP address, click **Add**.
3. Provide a valid host name or IP address in the input area, then click **OK**. The host name or IP address is displayed in the Allowed IDAA Hosts table.
4. When you have finished adding the appropriate host names or IP addresses, click **Close** to exit the task.

Configure IDAA Call-Home

Use this task to configure the host names or IP addresses of IDAA consoles that are allowed to use this Hardware Management Console (HMC) as a call-home proxy. Additional configuration is needed on the IDAA console to enable this functionality.

Note: If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data that is specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the **Configure Data Replication** task.

Add
To add a host name or IP address as an allowed IDAA console, click **Add**. Provide the host name or IP address in the input area, then click **OK**. The host name or IP address is added to the list of Allowed IDAA Hosts table.

Delete
To delete the selected host name or IP address of an allowed IDAA console, click **Delete**.

Close
To close this window and exit the task, click **Close**.

Help
To display help for the current window, click **Help**.

Configure On/Off

Accessing the Configure Channel Path On/Off task

Notes:

- Configure Channel Path On/Off is considered a disruptive task. If the object is locked, you must unlock it before continuing.
- Depending on your user task role, you may only be able to view this task.

This task configures channel paths on and off. *Configure on* and *configure off* are channel path operations you can use to control whether channel paths are online or on standby in the active input/output (I/O) configuration:

- A channel path is *online* while configured on. It is in the active I/O configuration and it can be used.
- A channel path is on *standby* while configured off. It is in the active I/O configuration but it cannot be used until it is configured on.

If you have experience using other systems, you may have used a CHPID command with ON and OFF parameters to configure channel paths on and off.

You can use the Hardware Management Console workplace to configure channel paths on and off. However, operating systems will not be notified when you use the workplace to configure channel paths on or off. For example, if you configure off a channel path, the operating system running in any image that owns or shared the channel path is not notified, and the next operation from the operating system to the channel path causes an error. It is recommended you use operating system facilities rather than the Hardware Management Console workplace, whenever possible, to configure channel paths on and off.

To use the workplace to configure channel paths on or off:

1. Select a CPC image.
2. Open the **Configure Channel Path On/Off** task. The Disruptive Task Confirmation window is displayed. Since this task may be disruptive to the targeted CPC image, review the confirmation text in the window to decide whether or not to proceed with the task.
3. If you proceed with the task, the Configure Channel Path On/Off window is displayed.
4. The window displays the *current state* and *desired state* of each channel path.
5. Use the window list and actions to *toggle* the desired states of channel paths you want to configure on or off.
6. Click **OK** to make the desired states take effect.

Configure Channel Path On/Off

This window can be used to determine if channel paths can be configured on or off for a Central Processor Complex (CPC) image. For some user task roles the window can be used to configure the channel paths on or off. Configuring channel paths on and off controls whether they are online or on standby in the active Input/Output (I/O) configuration:

- A channel path is *online* while configured on. It is in the active I/O configuration, and it can be used.
- A channel path is on *standby* while configured off. It is in the active I/O configuration, but it cannot be used until it is configured on.

Notes:

1. Operating systems will *not* be notified when you use this window to configure channel paths on or off. For example, if you use the window to configure off a channel path, the operating system running in any image that owns or shares the channel path is not notified, and the next operation from the operating system to the channel path will cause an error. Therefore, whenever possible, it is recommended that you use operating system facilities rather than the **Configure Channel Path On/Off** task to configure channel paths on and off.
2. When the CPC is activated in logically partitioned (LPAR) mode, configuring off a reconfigurable channel path does *not* release it from its assignment to an isolated logical partition.
3. When the CPC is activated in LPAR mode, the **Online pending** state indicates the channel path was configured on while assigned to an inactive logical partition. The channel path will be online when the logical partition is activated.
4. This task may be view only for some user task roles.

To use the **Configure Channel Path On/Off** task:

- The CPC must be power-on reset.
- The CPC must support configuring channel paths from a Hardware Management Console.
- The target image must own at least one channel path.
- Select the image from the Work Pane view you want to configure on or off.

Additional functions on this window include:

OK

When you finish toggling the target states of the channel paths you want to configure on or off, click **OK** to allow the new target states to take effect.

Cancel

To close the Configure Channel Path On/Off window, click **Cancel**.

Help

To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Configure Channel Path on/off table

The window lists the following information for each channel path owned or shared by the image you selected to start the task. Select one or more channel paths, then select **Toggle** from the drop down box to toggle their target states.

ID

Displays the channel path identifier (CHPID) of each channel path.

Current State

Indicates the current state of each channel path.

Desired state

Indicates the target state of each channel path.

Messages

If you attempt to change the target state of a channel path that cannot be configured on or off, this column displays the message "Not Allowed" for the channel path to indicate that changing its state is not allowed.

The icons perform the following functions for the selected configure on/off table:

Select All/Deselect All

You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table.

Show Filter Row

Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters

Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort

Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts

Click **Clear All Sorts** to return to the default ordering.

Current State

This window lists the current state and target of each channel path owned or shared by the image you selected to start the task. Use the select action drop down to *toggle* the target states of the channel paths you want to configure on or off.

- If the current state of a channel path is **Online** or **Online pending,** toggle its target state to **Standby** if you want to configure off the channel path.
- If the current state of a channel path is **Standby,** toggle its target state to **Online** if you want to configure on the channel path.

Online
Indicates the channel path is configured on. It is in the active Input/Output (I/O) configuration and it can be used.

Online pending
When the Central Processor Complex (CPC) is activated in logically partitioned (LPAR) mode, this state indicates the channel path was configured on while assigned to an inactive logical partition. The channel path will be online when the logical partition is activated.

Reserved
Indicates the channel path has service set on. It is not in the active I/O configuration, cannot be configured on, and cannot be used. It will remain out of the active I/O configuration until service is set off. A CHPID can be in the reserved state if it is not defined or incorrectly defined in the active IOCDS.

Standby
Indicates the channel path is configured off. It is in the active I/O configuration but it cannot be used until it is configured on.

Configure Storage

Accessing the Configure Storage task

Use this task to work with the storage resources for a system on which Dynamic Partition Manager (DPM) is enabled. Through the **Configure Storage** task, you can configure connections between the system and storage devices, request storage for partitions to use, or view and manage connected storage resources. Although multiple systems can share the same storage resources, note that the scope of this task is *one single system only*.

Note: This task is available on the HMC only for a DPM-enabled system that has the DPM R3.1 storage management feature or a later DPM version applied.

To open the **Configure Storage** task, you can use the default SYSPROG, STORAGEADMIN, or SERVICE user IDs, or any user IDs that an access administrator has authorized to this task through customization controls in the **User Management** task. Some functions in the **Configure Storage** task require the use of the default STORAGEADMIN user ID, or a user ID defined through the **User Management** task with equivalent permissions. Unless your user ID has permission to use the **Configure Storage** task, you receive an error message when you try to open the task.

You can access this task from the main console page by selecting **Configure Storage** in the Tasks Index, or by completing the following steps.

1. Expand the **Systems Management** node.
2. Select a specific DPM-enabled system.
3. Open the task by selecting **Configure Storage** from either the context menu next to the system name, or the Configuration task group.
   - If no administrators have started the initial configuration of storage for this system, the task opens to the **Connect System to Storage** page by default. For the initial configuration, administrators use the **CONNECT TO STORAGE** wizard to define storage resources for this system.

- If the initial configuration has been started already, the task opens to the **Storage Overview** page by default. From this page, administrators can select the following navigation links to change the page view. The navigation links vary, depending on the authorization of your user ID.
  - Select **REQUEST STORAGE GROUP** or **CREATE STORAGE GROUP** to request FICON or FCP disk storage, or NVMe storage, for partitions to use.
  - Select **REQUEST TAPE LINK** or **CREATE TAPE LINK** to request access for partitions to an FCP tape library.
  - Select **STORAGE CARDS** to modify the configuration of FICON or FCP adapter cards that are installed on the system.
  - Select **FICON CONNECTIONS** to complete or modify the FICON configuration of physical storage devices.

4. When you are ready to close the task, click **X** on the **Configure Storage** tab.

Configure Storage

The **Configure Storage** task provides the controls through which you can configure and manage the storage resources for a Dynamic Partition Manager (DPM)-enabled system. Through this task, system and storage administrators collaborate to connect a system to devices in the storage area network (SAN) through a simplified, visual, and automated process that does not require extensive knowledge of mainframes or Linux systems. Administrators also use this task to request and fulfill storage resources for use by partitions on that system.

In effect, the **Configure Storage** task replaces the use of the **Manage Adapters** task to configure and manage storage adapters. Administrators can use the task to configure adapters for access to Fibre Connection (FICON) extended count key data (ECKD) direct-access storage devices (DASD), or Fibre Channel Protocol (FCP) Small Computer System Interface (SCSI) disk storage devices and tape storage devices. If the system has one or more IBM Adapter for NVMe1.1 features, administrators can use this task to view Non-Volatile Memory Express (NVMe) storage adapters, as well.

Although multiple systems can share the same storage resources, note that the scope of this task is *one single system only*.

To open the **Configure Storage** task, you can use the default SYSPROG, STORAGEADMIN, or SERVICE user IDs, or any user IDs that an access administrator has authorized to this task through customization controls in the **User Management** task. Some functions in the **Configure Storage** task require the use of the default STORAGEADMIN user ID, or a user ID defined through the **User Management** task with equivalent permissions. For access to all functions in the **Configure Storage** task, users must have the same permissions as both the default SYSPROG and STORAGEADMIN user IDs. Also, access permission to all storage adapters is required to configure storage cards, and access permission to all FICON adapters is required to configure FICON connections. For more information about authorization, see “Authorize users of the Configure Storage task” on page 547.

To facilitate the collaboration between system administrators and storage administrators, DPM automatically generates detailed requests for system administrators to send, and provides inline notification of results when the storage administrator has fulfilled the request. For integrated requests and notifications, storage administrators (recipients) must have an email address associated with their user IDs, and Simple Mail Transfer Protocol (SMTP) settings must be defined. Users who send email through the **Configure Storage** task do not require an assigned email address because DPM can generate one based on the user name, but the suggested practice is to assign email addresses for senders as well, so recipients know which person sent the email.

- For information about setting up email addresses, see step “3.b” on page 548 in “Authorize users of the Configure Storage task” on page 547.
- For information about setting up SMTP, see the online help for the **Monitor System Events** task.

If email support is not configured, users have the option of either copying or downloading storage requests to send them through other methods.

The **Configure Storage** task consists of the following subtasks.

Connect to Storage

Use the **Connect to Storage** wizard to set up the initial storage configuration for a DPM-enabled system. For access to external storage devices, the initial setup includes defining the protocol of the adapter cards that are installed in the system I/O drawers, and building a visual copy of the storage hardware devices in the SAN and their FICON connections to this system. These hardware devices include disk storage subsystems, fabrics, and switches.

Through this process, DPM generates the virtual configuration that is required to connect the system to the physical SAN hardware; this virtual configuration is equivalent to the contents of an Input/Output Configuration Program (IOCP) file for the system. DPM also generates an exportable file of cabling details for the adapter cards that you have defined as either FICON or FCP.

If the system has one or more IBM Adapter for NVMe1.1 features, note that you cannot use this task to configure NVMe storage adapters, but you can view them. DPM detects any NVMe carrier card and its solid state drive (SSD) and displays them in the frames and drawers where they are installed. Also, DPM generates a separate file of details for all installed NVMe adapters that you can export through this task.

For this task, you need to use a user ID that has access permission to all storage adapters and access permission to all FICON adapters. If you do not have authorization to complete the configuration activities, or if you need help from a co-worker, you can invite your storage administrator to complete the configuration. DPM automatically generates an editable invitation for you to send, which includes a link through which the storage administrator can go directly to the appropriate page in the **Configure Storage** task.

When you are ready to use the **Connect to Storage** wizard, see the instructions in "Connect to Storage" on page 549.

Request Storage Group

Depending on the authorization of your user ID, select **REQUEST STORAGE GROUP** or **CREATE STORAGE GROUP** to request FICON or FCP or NVMe storage resources for partitions to use.

A *storage group* is a logical group of storage volumes that share certain attributes. These attributes vary, depending on the type of storage resource.

When you submit your request for an FCP or FICON storage group, DPM automatically generates the world wide port names (WWPNs) that are allocated to virtual storage resources when the storage group is attached to a partition. Also, DPM automatically generates a request that you can send to one or more storage administrators to fulfill through tools for managing storage subsystems. Because NVMe storage groups do not require the involvement of a storage administrator, DPM automatically creates the storage group, which is immediately ready for use.

You can define FCP or FICON storage groups with or without the use of a template. A *template* is a copy of a request for an FCP or FICON storage group. If administrators at your company have created templates, you can select an available template and, with minimal changes, quickly submit a request for a new storage group. Note that you cannot use a template to define an NVMe storage group.

- To create a FICON or FCP storage group, with or without using a template, see "Request or create a FICON or FCP storage group" on page 560.
- To create an NVMe storage group, see "Request or create an NVMe storage group" on page 565.
- To create and manage storage group templates, see "Create and manage templates for FICON or FCP storage groups" on page 622.

Request Tape Link

Depending on the authorization of your user ID, select **REQUEST TAPE LINK** or **CREATE TAPE LINK** to provide access for partitions to one FCP tape library in the storage area network (SAN).

A *tape link* defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN. These connection attributes include storage resources such as system adapters, world wide port names (WWPNs), and the number of partitions that can share the connection.

Creating a tape link can be as easy as providing a name for the tape link, and checking the default value for the number of connecting paths. In this case, the storage administrator selects the tape library and the system adapters to use for the tape link. When you request or create a tape link, DPM automatically generates the WWPNs that storage administrators use to fulfill the tape link request through tools for managing storage subsystems.

If you want additional control over the resources for a tape link, you can use this task to select specific partitions to which DPM attaches your tape link; set the maximum number of partitions that share the tape link; select a tape library; and select the system adapters. You also can use this task manage FCP tape libraries in the DPM environment.

For more details, see "Request or create a tape link" on page 567.

Storage Overview

Use the **Storage Overview** to view information about all of the storage groups and tape links that are defined for a DPM-enabled system. You can access the **Storage Overview** page by selecting **STORAGE OVERVIEW** in the **Configure Storage** task.

The **Storage Overview** page includes the Storage groups table, which contains one row for each storage group, and the Tape links table, which contains one row for each tape link. To view more details about a specific storage group or tape link, click anywhere in a table row to open the Storage Group details page or Tape Link details page. The fulfillment state indicates whether the storage group or tape link is available for use. Depending on the permissions that are associated with your user ID, you can select actions (such as modify or delete) for a specific storage group or tape link. You can also map volumes for a FICON storage group if you use the default STORAGEADMIN user ID, or a user ID with equivalent authorization.

If no storage groups or tape links exist, the table includes a selectable tile through which you can request or create a new storage group or tape link.

For more details, see "Storage Overview" on page 574.

Configure Storage Cards

Use the **Configure Storage Cards** task to modify the currently configured FCP or FICON adapter cards installed in a DPM-enabled system. You can access the **Configure Storage Cards** task by selecting **STORAGE CARDS** in the **Configure Storage** task. To view and complete this task, you must have access permission to all storage adapters.

Note that you cannot use this task to configure NVMe storage adapters, but you can view them through this task; reconfiguration requires properly removing the carrier card and its SSD from the drawer and reinstalling them in a different physical location, as instructed by a service representative.

For more details, see "Configure Storage Cards" on page 610.

Configure FICON Connections

Use the **Configure FICON Connections** task to complete the initial configuration, or to modify the current configuration, of the FICON-based, external storage hardware devices that are connected to a DPM-enabled system through FICON or FCP adapters. These hardware devices include disk storage subsystems, fabrics, and switches.

Storage administrators who have been invited to complete the initial configuration can access this task through a link in the invitation. Otherwise, you can access the **Configure FICON Connections** page directly, by selecting **FICON CONNECTIONS** in the **Configure Storage** task. To view and complete this task, you must have access permission to all FICON adapters.

For more details, see "Configure FICON Connections" on page 614.

Authorize users of the Configure Storage task

Use this procedure to create a new user for a system administrator who can also perform functions that are usually restricted to storage administrators. This new user has access permissions to all functions that are available through the **Configure Storage** task. When you create a new user, you can assign an email address so the new user can, if necessary, participate in the request, invitation, and notification functions that are integrated into the **Configure Storage** task.

Before you begin

Log in to the HMC with the default ACSADMIN user ID, or a user ID defined through the **User Management** task with equivalent permissions.

About this task

To open the **Configure Storage** task, administrators can use the default SYSPROG, STORAGEADMIN, or SERVICE user IDs, or any user IDs that an access administrator has authorized to this task through customization controls in the **User Management** task.

Some functions in the **Configure Storage** task require the use of the default STORAGEADMIN user ID, or a user ID defined through the **User Management** task with equivalent permissions. For access to all functions in the **Configure Storage** task, users must have the same permissions as both the default SYSPROG and STORAGEADMIN user IDs. Also, access permission to all storage adapters is required to configure storage cards, and access permission to all FICON adapters is required to configure FICON connections.

To define a user with these permissions, you have several options:

- Adding storage administrator roles to a user ID that is based on the default SYSPROG role.
- Adding system programmer roles to a user ID that is based on the default STORAGEADMIN role.
- Creating a custom role that has permission to the following tasks:

  Configure Storage - System Programmer
  Configure Storage - Storage Administrator

This procedure provides step-by-step instructions for the first option.

Procedure

1. In the HMC navigation pane, select **HMC Management** or **Tasks Index** and select the link to open the **User Management** task.

   The User Management dashboard is displayed.

2. Select the New User action icon ( ).

   The New User wizard opens to the Welcome page.

3. Select **Next** to open the Name page, and complete the following steps.
   a) For Create Option, select **New based on**, and select SYSPROG from the list.

      By default, selecting SYSPROG gives the new user permission to the **Configure Storage** task, as well as permission to the object types FCP Storage Group, FICON Storage Group, and FICON Adapter.

   b) For User Details, provide a name and optional description. The suggested practice is to also specify an email address in the Email Address field, so the new user can participate in the request, invitation, and notification functions that are integrated into the **Configure Storage** task.

   c) Select **Next** to go to the next page.

4. On the Authentication page, select an authentication type and provide any additional required details. Then select **Next** to go to the next page.

5. On the Roles page, select the following storage administrator roles.

   - Storage Administrator Objects
   - Storage Administrator Tasks

   Then select **Next** to go to the next page.

6. On the Summary page, review the information for the new user, and select **Finish**.

Results

The new user has the task and role permissions that are required to complete all actions that are available through the **Configure Storage** task. The new user also can send or receive requests or invitations, and receive notifications about work that has been completed through the **Configure Storage** task.

Connect to Storage
Use the **Connect to Storage** wizard to set up the initial storage configuration for a DPM-enabled system. Although multiple systems can share the same storage resources, note that the scope of this task is *one single system only*. Because DPM automates the selection of some configuration elements, using this task does not require extensive knowledge of mainframes or Linux systems; however, specific activities must be completed by a storage administrator. At appropriate points in the task flow, you can invite one or more storage administrators to complete these activities. DPM automatically generates an invitation that you can send, to which you can add your own greeting and more details, if necessary.

Before you begin

- For integrated requests and notifications, storage administrators (recipients) must have an email address associated with their user IDs, and Simple Mail Transfer Protocol (SMTP) settings must be defined. Users who send email through the **Connect to Storage** task do not require an assigned email address because DPM can generate one based on the user name, but the suggested practice is to assign email addresses for senders as well, so recipients know which person sent the email.
  - Email addresses for users are assigned through the **User Management** task.
  - The SMTP server and port settings are defined through the **Monitor System Events** task.

  If your installation does not have SMTP configured, you have the option of downloading or copying the generated invitation to send to one or more administrators.
- To open the **Configure Storage** task, you can use the default SYSPROG, STORAGEADMIN, or SERVICE user IDs, or any user IDs that an access administrator has authorized to this task through customization controls in the **User Management** task. Some functions in the **Configure Storage** task require the use of the default STORAGEADMIN user ID, or a user ID defined through the **User Management** task with equivalent permissions.

  If you do not have authorization to complete the configuration activities in step “4” on page 553, you can invite your storage administrator to complete the configuration. More details about the invitation process are provided in steps “4” on page 553 and “5” on page 559.
- If the system has one or more IBM Adapter for NVMe1.1 features, you cannot configure those adapters through this task, but you can view them: DPM detects any NVMe carrier card and its solid state drive (SSD) and displays them in the frames and drawers where they are installed.
- If you plan to request or create tape links to provide partitions with access to tape libraries in the SAN, you need to configure some storage cards to use the FCP protocol in step “3” on page 552. However, do not define tape libraries as part of the FICON connections in step “4” on page 553; instead, follow the procedure in “Request or create a tape link” on page 567.

About this task

Through this task, system and storage administrators collaborate to connect a system to devices in the storage area network (SAN) through a simplified, visual, and automated process that does not require extensive knowledge of mainframes or Linux systems. This process does, however, require administrators to know high-level information about the physical elements of the SAN, such as the names of storage subsystems, the types of devices and communication protocols, intended use, and so on. This information is usually available through a system plan for the company's physical IT site.

Starting with the system plan, system and storage administrators use the **Connect to Storage** task to define the initial storage configuration, which consists of the following activities.

- Defining the protocol of theFICON Express adapters that are installed in the system I/O drawers. DPM automatically detects the installed adapters, which you can define as either FICON or FCP devices.

Based on the number of cards that you specify, DPM automatically selects a combination of the unconfigured cards, but you can override these selections, if necessary. Note that you can only view installed NVMe adapters; you cannot configure NVMe adapters through this task.

- Building a visual copy of the storage hardware devices in the SAN and their FICON connections to this system. This configuration can contain at most two physical sites where storage devices are located. The primary site is always where the DPM-enabled system is physically located. System administrators can define physical elements, such as switches, fabrics, and disk storage subsystems, but storage administrators are required to define port connections and logical control units (LCUs). DPM automatically generates an invitation that you can send to one or more storage administrators.

  If the DPM-enabled system is not yet physically attached to SAN hardware through cables, DPM provides several automated options for this configuration process; for example, storage administrators have the option of having DPM select port connections. However, if the system is already cabled, you need to supply information that reflects the physical connections that are already in use.

Completing these activities produces the following results:

- Fully configured adapter cards on the DPM-enabled system.
- Fully enabled FICON connections that link the system to physical elements in the SAN.
- An exportable file of an FCP and FICON adapter cabling plan that you can use to physically connect the system to SAN hardware. The file is in Comma Separated Values (CSV) format that you can view in a spreadsheet application.
- An exportable file of the NVMe adapter plan, which lists details about the installed adapters, only if the system has one or more IBM Adapter for NVMe1.1 features. The file is in Comma Separated Values (CSV) format that you can view in a spreadsheet application.

After DPM generates the exportable files, you can access them through the **Actions** menu above the frame display on the Configure Storage Cards page. For a sample spreadsheet of an exportable plan, see the *Dynamic Partition Manager (DPM) Guide*, which is available through the Library link on IBM Resource Link at http://www.ibm.com/servers/resourcelink

Procedure

1. Open the **Configure Storage** task.

   For the initial storage configuration, the task opens to the **Connect System to Storage** page.
2. On the **Connect System to Storage** page, select **START**.

   The **Configure Storage Cards** page opens to a visual abstraction of each physical I/O drawer in the system. Each drawer has a front and rear display, each with two domains, as well as adapter-card slots. An I/O drawer can contain different types of adapter cards, so DPM highlights only the slots containing an adapter card that you can use for connections to storage devices.

   Depending on the configuration of the system, you might need to use navigation controls to view all of the frames, drawers, and cards. For systems with only one frame, use the scroll bar or expand/collapse controls to view adapters in the frame drawers. For multiple-frame systems, use the overview map to change the viewport display, as shown in Figure 29 on page 551.

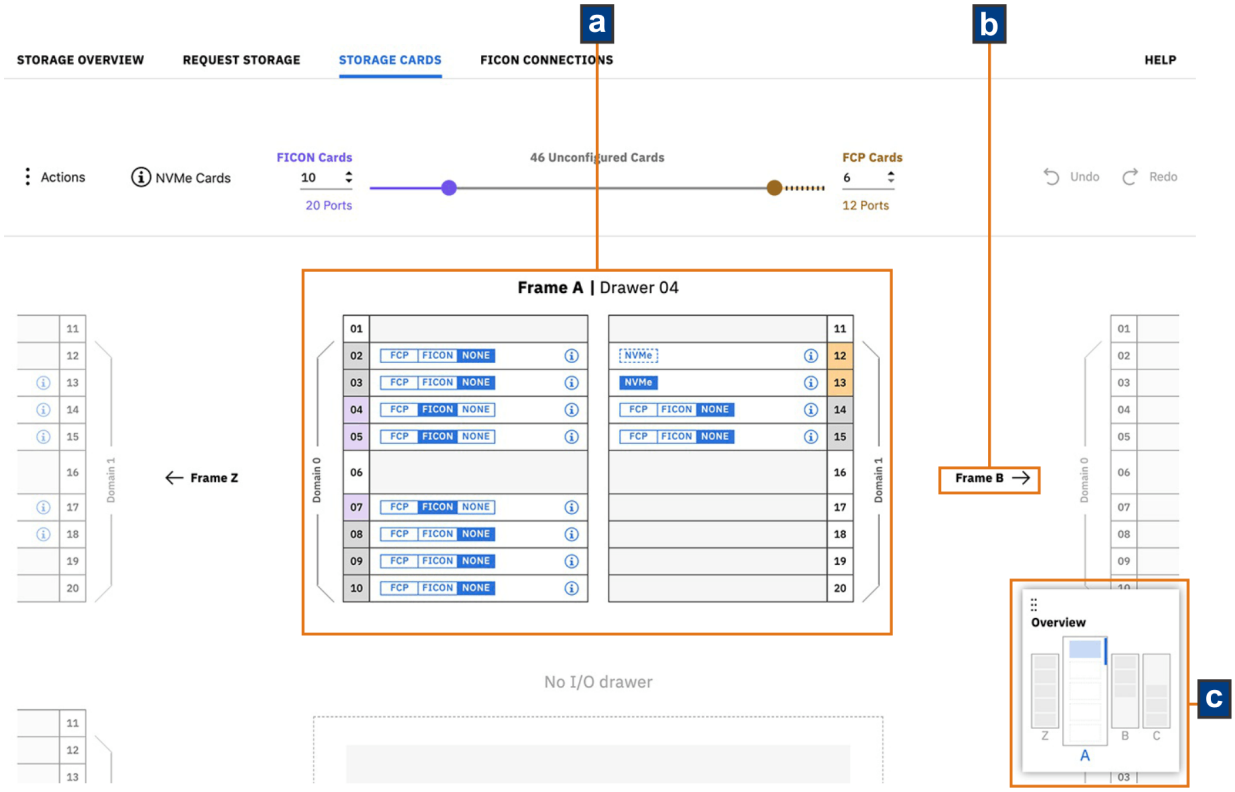


Figure 29. Overview map and other viewport navigational controls

a. This screen capture shows Frame A centered in the viewport.

b. Selectable frame buttons on either side of Frame A provide a way to change the viewport to either the previous or next frame in the system. These buttons are displayed only when the system is configured with additional frames to the left or right of the current frame.

c. The overview map shows not only how many frames are in the system, but also which frame and which I/O drawer within that frame are currently displayed in the viewport. In this example, Frame A has only one I/O drawer installed, which is shown as a solid blue rectangle. When another frame with multiple I/O drawers becomes the current frame in the viewport, any additional I/O drawers that are not currently in the viewport are shown as white rectangles with blue outlines. To change the display in the viewport, select a different frame in the overview map or use the frame buttons. Scroll up or down to view different I/O drawers within the current frame, if any.

If the system has one or more IBM Adapter for NVMe1.1 features, the frame display also indicates the current location of any installed NVMe carrier card. For an overview of any NVMe adapters that are installed in the system, hover your cursor over the information icon (ⓘ) to the left of the **NVMe Cards** label. To download a CSV file of details about the NVMe storage adapters, use the **Actions** menu to select **Export NVMe Plan**.

Each NVMe adapter consists of two pieces of hardware: an IBM-supplied carrier card installed in a system I/O drawer, and the solid state drive (SSD) that customers purchase. The page display identifies which hardware is installed and whether the adapter is in use.

- When an NVMe carrier card is installed but does not contain an SSD, the NVMe adapter label is shown as a white rectangle with a dotted blue outline. When the carrier card is empty, selecting the information icon opens a window that contains the adapter location; the card type; the adapter ID; and a control to toggle the LED light on the physical card on or off.
- When an SSD is installed in the carrier card, the NVMe adapter label is a solid blue rectangle. When an SSD is installed, selecting the information icon opens a window that contains the adapter location; the card type; the adapter ID; the size and serial number of the SSD; the toggle for the LED light; and a link to the **Adapter Details** task.

- A red dot indicates that DPM recently detected the NVMe adapter.

3. On the **Configure Storage Cards** page, define the unconfigured adapter cards as either FICON or FCP.
   a) Use the slider or input fields to specify the number of each type of adapter.
   Figure 30 on page 552 shows the UI controls for specifying the number of each adapter type.

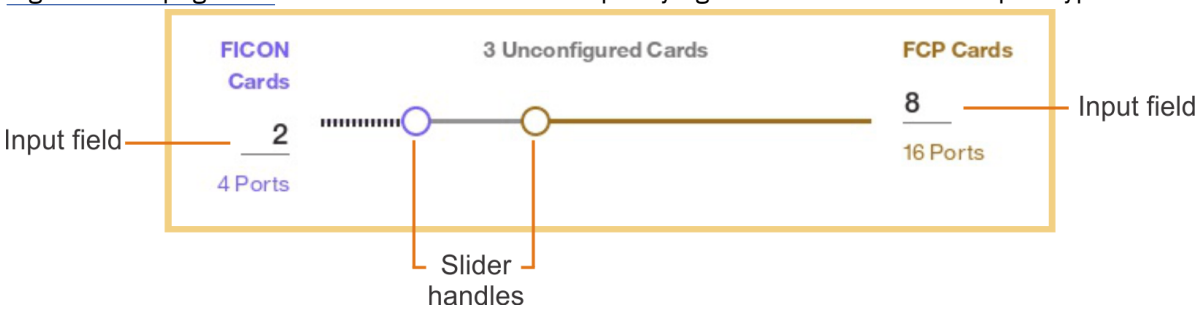


Figure 30. Slider and input fields for FICON or FCP adapter cards

- When you use the sliders or input fields to enter the number of FICON or FCP cards, DPM automatically selects a combination of the unconfigured cards to satisfy your request. This combination is *redundant*; that is, the configured cards of each type are spread across domains and drawers to ensure availability, in case of a card or drawer failure. You can override these selections by selecting the appropriate protocol label in each card: FICON or FCP. Selecting NONE resets the adapter card to the unconfigured state. Depending on the type of adapter card and its cabling, you might not be able to change the protocol through these labels. For these adapter card types, the protocol labels are disabled.

  How many FICON or FCP adapters you specify depends on your system plan; for example, if this system is expected to host test rather than production workloads, you might specify fewer adapter cards. Redundancy might be less important for a test workload, as well.
- To display more information about a particular FICON or FCP adapter, select the information icon (ⓘ) to open a display that contains details such as the adapter location and card type, the adapter ID, and physical worldwide port numbers (WWPN) for each port on the adapter. This display also includes a link to open the **Adapter Details** page of the **Manage Adapters** task.

Figure 31 on page 553 shows a sample portion of the frame display on the **Configure Storage Cards** page, with the most recently configured adapter cards marked with a red dot.

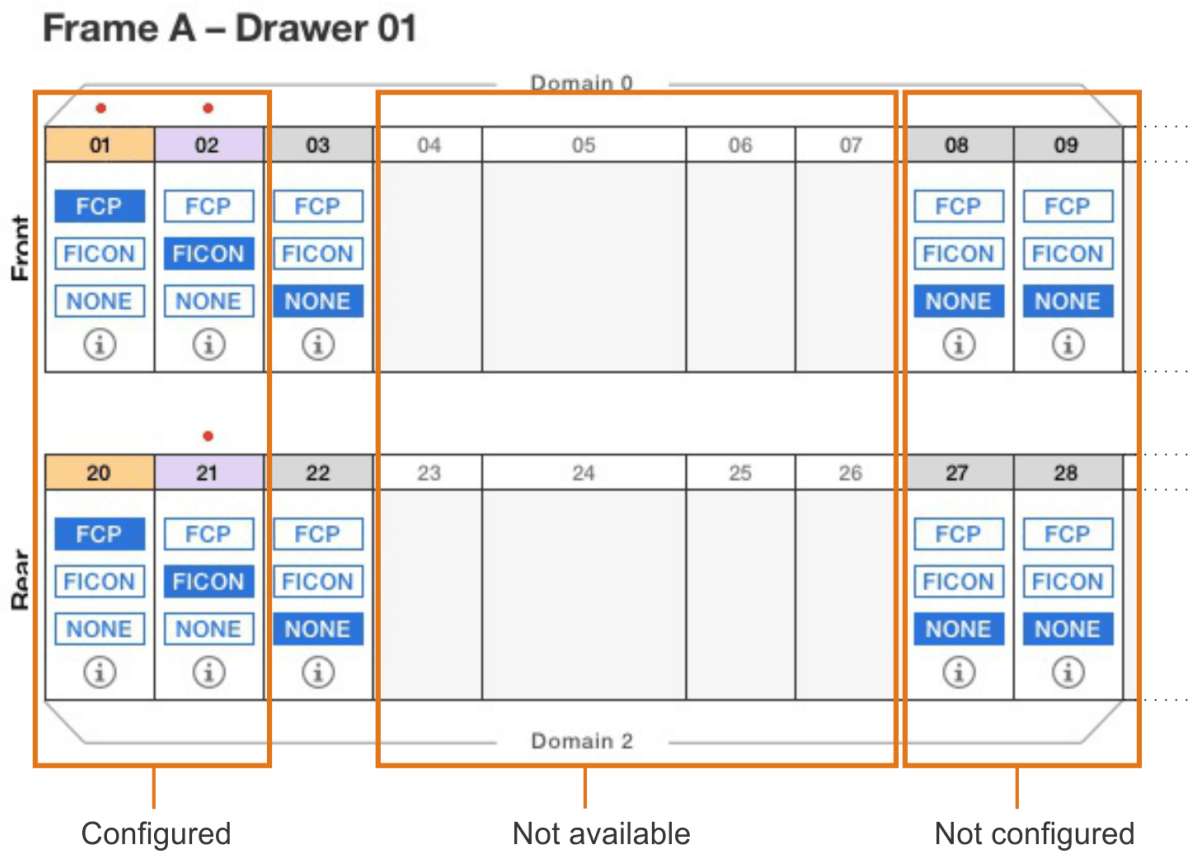


Figure 31. Sample display of a partial frame drawer, with domains and adapter cards

b) When you have finished defining the FICON or FCP adapter cards, select **Next**.

The **Configure FICON Connections** page opens.

4. On the **Configure FICON Connections** page, define the external storage hardware that is or will be connected to this DPM-enabled system through FICON or FCP adapters. Add physical storage elements to the primary site and, optionally, to a secondary site. Do not define tape libraries as storage subsystems in this step. To create the required connections to access to tape libraries in the SAN, follow the procedure in "Request or create a tape link" on page 567.

   As you provide names for these elements, note that supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters.

   This page provides a basic visual layout of the storage configuration, along with hover help to guide you through the process of defining a replica of the storage hardware that is or will be connected to the system. The replica must match the planned or actual configuration of storage subsystems and switches. Your SAN configuration can consist of point-to-point (direct) connections or switch connections, but not both.

   Figure 34 on page 559 shows a sample display of a partial configuration for two sites.

   If you want to define a secondary site, you can select **Add empty site** to add headings and controls for manually defining that site, or select **Add and clone to the secondary site** to clone the elements that you have already defined for the primary site. The name of the secondary site must be different from the name of the primary site, and the same length and supported-character rules apply to both names. You can clone the primary site any time after you add the first storage subsystem or switch to the primary site. DPM duplicates the primary site subsystems, fabrics, and switches, along with adapter ports and LCUs, but you must provide unique names and IDs for the storage subsystems and switches.

   - For a configuration with point-to-point (direct) connections, DPM automatically replicates the physical paths between the system and all cloned storage subsystems.

- For a configuration with fabrics and switches, DPM automatically replicates physical paths as you provide a unique switch ID for each cloned switch.

If you need assistance from a co-worker, you can invite your storage administrator to complete the configuration. To do so, either select **Next** or the **Invite Storage Admin** link on the **Configure FICON Connections** page to generate an invitation, and go to step "5" on page 559.

As you work through the following steps, you open different subtask windows to make selections or perform actions, then select **DONE** to save your changes or **CANCEL** to discard them; either button selection returns you to the **Configure FICON Connections** page. Note that, while you are working in a specific subtask window, the **Undo** and **Redo** buttons revoke or restore changes only within that window. On the **Configure FICON Connections** page, however, the Undo/Redo history includes the changes that you saved in a subtask window, as well as any selections you made on the **Configure FICON Connections** page itself. For example, suppose that you select the **Connect Adapter Ports** link in the System box and, on the **Connect System** window, you select two or more configured adapter ports in the system I/O drawers, and select **DONE** to save those changes. Back on the **Configure FICON Connections** page, you can use **Undo** and **Redo** to delete those two connections or restore them, without having to reopen the **Connect System** window.

a) Start by adding a name for the primary site.

   The name can be 1 - 32 characters in length.

b) To fill in the display for the primary site, select the plus sign to add a box that represents a specific physical element in the SAN.

   1) If your SAN configuration consists of point-to-point (direct) connections rather than switches, skip to the next step to add storage subsystems. Otherwise, select the plus sign to add and name a fabric, and then add one or more FICON switches. Fabric names must be unique among fabrics, and cannot exceed 32 characters. Switch IDs must be unique within a fabric, and consist of hexadecimal values in the range 01 - EF. If necessary, repeat this process to add more fabrics and switches. You can create a maximum of 256 fabrics per site, and a maximum of 239 switches per fabric.

      By default, each fabric is defined as a high integrity fabric through a toggle setting. A high integrity fabric is configured to use 2-byte link addresses, rather than 1-byte link addresses. The suggested practice is to define all fabrics as high integrity fabrics.

      - If you define a fabric as high integrity, you must ensure that the physical switches are configured to use 2-byte link addresses. If they are not configured for 2-byte link addresses, set the toggle to off.
      - As you add each new fabric, the high integrity toggle setting matches the setting in effect for the previously defined fabric. If you are adding fabrics to the primary site only, you can set the toggle to off for some fabrics, and on for others.
      - When you add or clone a secondary site, DPM automatically sets the high integrity setting to on for all fabrics on the primary site. When you define a cascaded switch on the secondary site, DPM locks the toggle setting for the fabric. If a fabric does not have any defined switches on the secondary site, you can change the high integrity setting to off.

   2) Under the Subsystems label, select the plus sign to add a storage subsystem, and provide a name for it. If necessary, repeat this process to add and name more subsystems, specifying a unique name for each. Storage subsystem names must be unique among storage subsystems, and cannot exceed 64 characters. You can create a maximum of 256 storage subsystems per site.

c) Select the **Connect Adapter Ports** link in the System box.

   The **Connect System** window opens to a visual display of the configured adapters with their ports (typically two ports per adapter), along with either the storage subsystems (for direct connections without switches) or switches that are defined for the primary site. If you have defined storage subsystems or switches for the secondary site, you need to select **Show** to display them.

   Adapters are displayed by frame; for multiple-frame systems, a viewport indicator is displayed so that you can easily switch to view a different frame. The indicator shows how many frames are in

the system, and which frame is currently displayed in the viewport. To change the display, select a different frame in the viewport indicator or use the frame buttons.

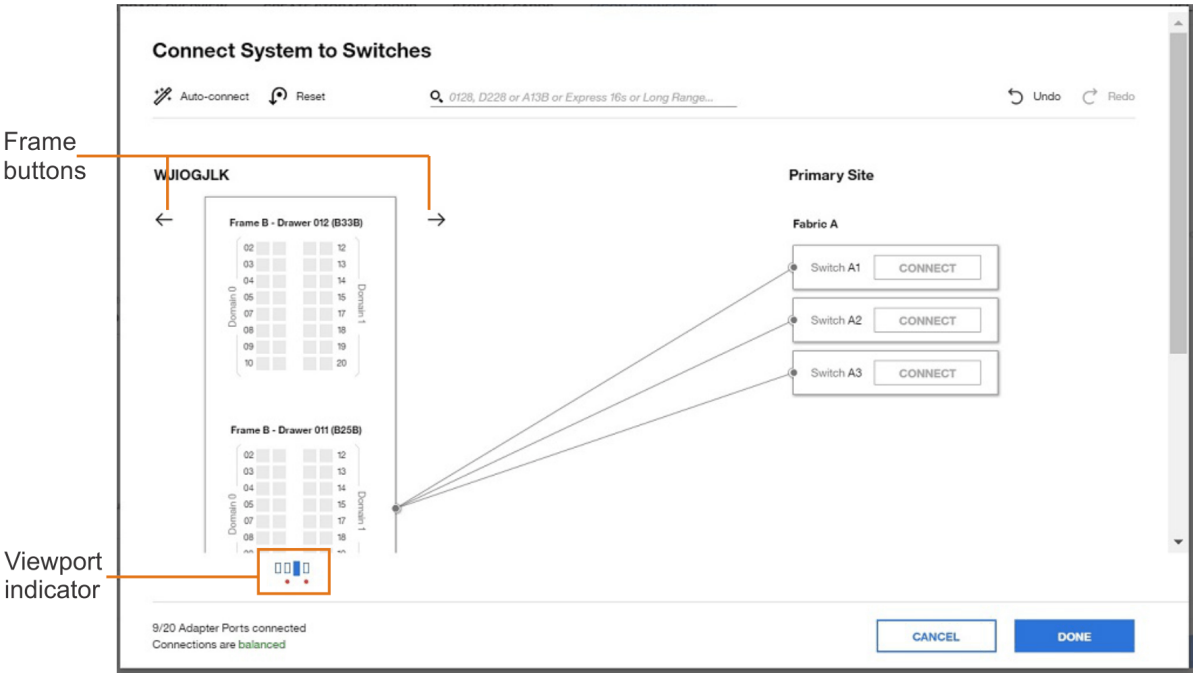


Figure 32. Viewport indicator and frame buttons

If the system is not cabled yet, the suggested practice is to select the **Auto-connect** icon ( ) to have DPM automatically connect all unconnected ports, but you can select each port yourself. You cannot select unconfigured adapter ports, which are shown in gray. For availability, connect each storage subsystem or switch to at least two adapter ports, each of which resides in a different frame and domain of the system. If the automatic updates from **Auto-connect** span more than the current frame of a multiple-frame system, a red dot is displayed under the updated frames in the viewport indicator, and a message is displayed next to the appropriate frame button.

1) Select two or more configured adapter ports in the system I/O drawers. While making your selections, you can hover over each adapter port to display more details, including the adapter name, location, ID, card type, and cable type. You can also use the search field to highlight one or more adapter ports, using a search string for any of these adapter port properties. Available adapter ports with properties that match the search string are highlighted with a blue outline.
   - The search provides an auto-suggest function to help you more quickly select an adapter port with properties matching the search string that you enter.
   - If adapter ports that match the search string are not in the currently displayed frame of a multiple-frame system, the display automatically changes to show the closest frame containing search results. If more adapter ports that match the search string reside in other frames, a text label that indicates the number of those matching adapter ports is displayed above one or both frame buttons, depending on the location of the additional adapter ports.
   - If an adapter port in the search results is already in use and cannot be configured, DPM does not highlight that adapter port unless you hover your cursor over a search tag containing the adapter port in the search field. If you hover your cursor over the box for the in-use adapter port in the frame display, a message in the adapter details window indicates that the adapter port cannot be changed.
   - The search field can expand to multiple lines, if you require more space to enter search strings or adapter names.
2) Select **CONNECT** in a specific storage subsystem or switch to connect it to the selected adapter ports. Note that the box for each adapter port now displays the storage subsystem or switch ID,

and a line now connects the system to the storage subsystem or switch. Line numbers indicate the total number of adapter ports connected to the storage subsystem or switch.

For storage subsystems, the ID consists of the letter A to indicate the primary site (B indicates the secondary site, if any) and a sequential number, starting with 1 (one). This ID is also appended to the storage subsystem box label in this display.

3) Repeat as necessary until all storage subsystems or switches are connected to the system. For the best results, make sure that the indicator (at the foot of the window, under the adapter port display) identifies the connections as balanced. You are not required to do so but, if **BALANCE CONNECTIONS** is enabled, you can select that button to have DPM modify the port connections such that all connected switches have as close to the same number of port connections as possible. If the automatic updates from **BALANCE CONNECTIONS** span more than the current frame of a multiple-frame system, a red dot is displayed under the updated frames in the viewport indicator, and a message is displayed next to the appropriate frame button.

   For example, suppose that you have connected the system to four switches: three in one fabric, and one in another fabric. One switch, switch B4, has six port connections, and the other switches have fewer connections (five, four, and three).

   - If you select **BALANCE CONNECTIONS**, DPM adds available port connections so that each of the four switches have as many connections as the switch with the highest number of six port connections.
   - If the number of available port connections does not allow each switch to have six connections, DPM removes connections from switch B4 and adds them to the other switches, to distribute the number of port connections as evenly as possible among the four switches. If DPM cannot remove port connections on the switch because they are in use, **BALANCE CONNECTIONS** is disabled.

   Note that using **Auto-connect** and **BALANCE CONNECTIONS** are similar in that DPM attempts to evenly balance connections across subsystems or switches, but the two connection methods differ in the following ways.

   - **Auto-connect** connects all available ports, while **BALANCE CONNECTIONS** uses only enough ports to ensure that each connected switch has as many port connections as the switch with the most port connections.
   - **Auto-connect** does not reconfigure any already connected ports, while **BALANCE CONNECTIONS** can reconfigure already connected ports, if necessary.

4) When you have finished, select **DONE** to return to the **Configure FICON Connections** page. Note that lines connect each storage subsystem or switch to the system, with each line indicating the number of connections.

d) If you are using direct connections without switches, skip to step “4.f” on page 557 to define LCUs; otherwise, continue to the next step to connect switches.

e) For each storage subsystem in the display, select the **Connect Ports** link. Complete this step only if you are using fabrics and switches in your configuration.

   The **Connect Subsystem to Switches** window opens to a visual display of the ports on each switch that is defined on the same site as the storage subsystem. (To see all defined fabrics and switches, you might need to scroll down or use the expand or collapse controls.) For availability, the suggested practice is to connect each storage subsystem to at least one switch per fabric, and at least two ports on each switch. You can define a maximum of 64 connections to switches on each subsystem. For the best results, make sure that the redundancy indicator (at the foot of the window) identifies the connections as redundant.

   1) In the box for the first switch, select whether you want to view the switch port numbers in decimal or hexadecimal notation. You can also specify the switch size, by typing an integer from 1 - 256 in the input field, which is part of the port counter at the bottom of the switch box.
   2) Select one or more ports in the switch. Note that a line displays the connection between the storage subsystem and the switch, with a number that indicates the total of selected ports for that switch.

If necessary, use the search field to locate one or more switch ports, using a two-digit number for each port, in the notation that you have chosen to view the switch ports (decimal or hexadecimal). If you enter a number in a notation that does not match the notation that you have selected for viewing switch ports, DPM indicates that the search value is invalid. You can select **Connect all** to connect the valid switch ports that are listed in the search field to the storage subsystem. If the result of this action will cause the total number of switch connections to the storage subsystem to exceed the maximum of 64, **Connect all** is disabled.

3) Select one or more ports in other switches that are displayed, either manually or by selecting **Clone to** and selecting one or more target switches.
   - If the result of cloning will cause the total number of switch connections to the storage subsystem to exceed the maximum of 64, **Clone to** is disabled.
   - If the target switch is smaller than the switch you are cloning, DPM automatically increases the size of the target switch to match the cloned switch.
   - The cloned switch port numbers match the source port numbers. For example, suppose that you select ports 0, 8, 21, and 28 on Switch 10, and clone those ports to Switch 20. When you expand the display of Switch 20, ports 0, 8, 21, and 28 are selected.
4) When you have finished, select **DONE** to return to the **Configure FICON Connections** page. Note that lines now connect the subsystem to the switches on which you selected ports.
5) Repeat this process as necessary, for each subsystem.

f) For each storage subsystem in the display, select the **Define LCUs** link.

The **Define LCUs and Logical Paths** window opens.

1) Select the plus sign to add one or more LCUs for the storage subsystem. The Add LCUs window opens.
2) On the Add LCUs window, type one or more LCU numbers in the LCU Numbers field, or select the table icon () to open the LCU input matrix. You can specify a range of LCU numbers, or individual numbers, or both. LCU numbers must be unique within the storage subsystem; valid values are in the range 00 - FF. You can specify a maximum of 256 LCUs per storage subsystem. The suggested method to use is the matrix because it shows which LCUs are already configured; configured LCUs are gray, as shown in Figure 33 on page 558.

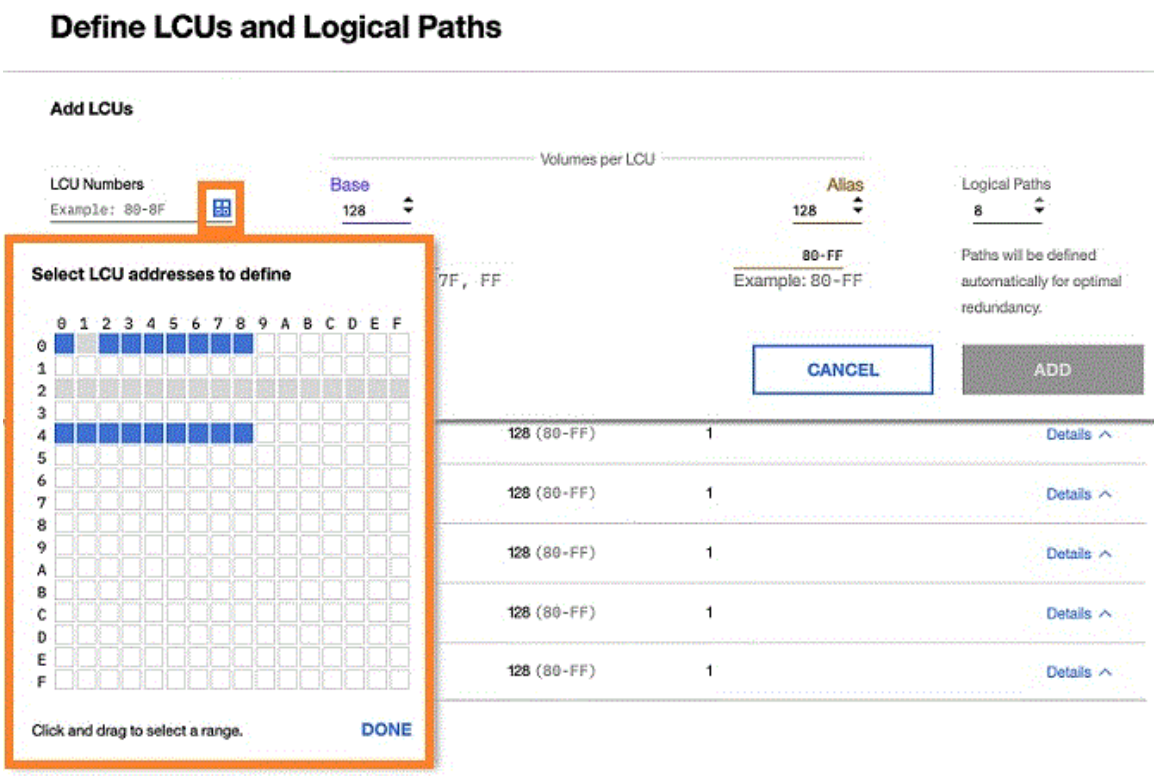


*Figure 33. Sample display of the LCU input matrix (highlighted) on the **Define LCUs and Logical Paths** window*

3) Use the **Base** and **Alias** fields to specify the number of base and alias volumes to define for each LCU. Either type the number or click the up or down arrows increase or decrease the number. You can specify up to a combined total of 256 base and alias volumes for one LCU.
4) If necessary, change the value specified in the **Logical Paths** field, which represents the requested number of paths. The maximum value for an LCU is 8 logical paths.
5) Select **ADD** to add the LCUs. DPM automatically selects paths to maximize redundancy and to reduce common points of failure. The **Define LCUs and Logical Paths** window now contains a table that lists each LCU or group of LCUs, along with the number of base volumes, the number of alias volumes, and the number of logical paths for each LCU. DPM groups LCUs that have the same number of base volumes, the same number of alias volumes, and the same configured paths. To view all of the LCU numbers (addresses) in the group, select the information icon in the LCU column (the resulting display is similar to the LCU input matrix, but it is read-only). The table entry for a group lists the total number of LCUs in the left margin of the table row, which you can select to expand the group entry.

   By selecting **Details**, you can expand the LCU table entry to view or edit details about the logical paths to the system. The expanded view is another table that contains a row for each path. If you have already connected the system to one or more switches, this table lists the assigned switch, switch port, adapter ID, and adapter location. If the logical path goes through cascaded switches, this table includes another SWITCH column between the SWITCH PORT and ADAPTER ID columns.

   If necessary, you can select **EDIT** to modify or delete any of the information on the **Define LCUs and Logical Paths** window. To prevent a path from being changed or deleted, you can select the lock icon. If you edit a path statement, it is locked by default. Note that some changes that you make through the edit function might result in the LCU being removed from a group.

   When you have finished, select **SAVE** to exit edit mode.
6) Optional: To copy one or more of the defined LCUs to another subsystem, select **Clone to**. The cloned LCU numbers match the source LCU numbers. If any LCUs with matching numbers are

already defined for the target subsystem, DPM prompts you to confirm the cloning operation before overwriting the target subsystem's LCU configuration.

7) Select **DONE** to return to the **Configure FICON Connections** page. Note that the box for the storage subsystem now lists the total number of defined LCUs.

When you have finished adding LCUs, note that the box for each subsystem contains a check mark (). Figure 34 on page 559 shows a sample display of a partially completed configuration.

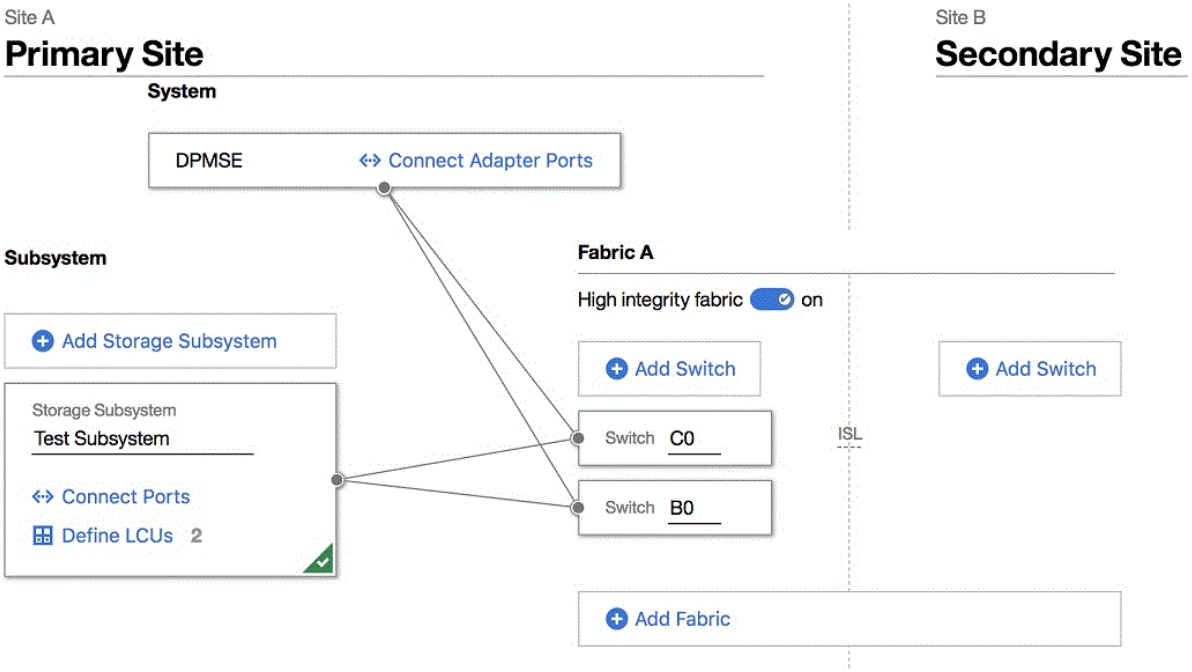


Figure 34. Sample display of two sites with physical storage hardware configured for the primary site

g) Check the display for warning indicators () or highlighted red text to make sure that you have supplied names and connections as required.

h) Select **NEXT**.

5. On the Finish page, select one or more of the following options.

   The content of this page varies, depending on the configuration activities you completed in step "4" on page 553, and whether you already invited a storage administrator to complete the configuration. Depending on the content, you have the following options.

   - If the page display includes an invitation, you can modify and send it to one or more storage administrators.
   - You can export the cabling details file and view it in a spreadsheet application.
   - You can select either **Finish** or **Invite & Finish** to close the **Connect to Storage** task.

Results

Depending on the configuration activities you completed in step "4" on page 553, you have either fully or partially configured storage for the DPM-enabled system.

If you have invited one or more storage administrators to complete the configuration, they can log in to the HMC and open the **Configure Storage** task through a link in the invitation, and complete the configuration, as described in "Configure FICON Connections" on page 614. When they have finished their work, they can notify you by selecting the **Invite System Admin** link or by selecting **Save**. In either case, DPM generates an editable notification whose recipient is, by default, the user who sent the original invitation to complete the FICON configuration.

What to do next

- Use the **Request Storage** task to define storage resources, known as storage groups, for partitions to use. For more information, see "Request or create a FICON or FCP storage group" on page 560 or "Request or create an NVMe storage group" on page 565.
- If you exported the cabling details file before the FICON configuration was completed, you can download an updated copy. Note that physical storage hardware (subsystems, switches, and so on) must be connected by cables, and storage cards must be configured before you can use the **Request Storage** task.
- If you need to modify this initial storage configuration at a later time, open the **Configure Storage** task and, depending on what you need to change, select **STORAGE CARDS** or **FICON CONNECTIONS**.
  - Note that DPM does not allow the reconfiguration of any adapter card that is already in use.
  - Note that you cannot modify the high integrity fabric setting when LCUs are in use for switches in the fabric. If you need to modify the high integrity fabric setting, you must first remove all of the paths from the LCUs that are using that fabric, and then modify the high integrity fabric setting. After modifying the setting, you can restore the paths by adding them back to the LCUs.
  - Note that you cannot use the **STORAGE CARDS** task to reconfigure NVMe storage adapters; reconfiguration requires properly removing the carrier card and its SSD from the drawer and reinstalling them in a different physical location, as instructed by a service representative.

    If you must remove an NVMe adapter, the suggested practice is to remove the NVMe adapter from any storage group that might be using the SSD as a volume, before removing the SSD or carrier card. To remove the NVMe adapter from a storage group, complete the following steps.

    1. On the **Configure Storage Cards** page, look for the lock icon next to any NVMe adapter labels.
       - If the lock icon is not displayed, no storage groups are using the adapter, and no further action is required.
       - If the lock icon is displayed, record the serial number of the SSD and continue to the next step.
    2. Go to the Storage Overview and check for any NVMe storage groups by looking for NVMe in the Type column (use the search or sort functions, if necessary). For each NVMe storage group, open the Storage Group details page and look for the matching serial number in the table on the **VOLUMES** tab. When you find the matching SSD serial number, note whether the volume is defined as a boot volume, and continue to the next step.
    3. Select the **PARTITIONS** tab to review the status of a partition that might have attached the storage group. Only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared.
       - If the Partitions table is empty, you can skip to step "4" on page 560 to delete the SSD volume.
       - If a partition is listed on this tab and the SSD is a data volume (not a boot volume), you can skip to step "4" on page 560 to delete the SSD volume. However, if a currently active partition has attached this storage group, deleting the SSD volume is a disruptive change unless you first use the **Stop** task to stop the partition.
       - If the SSD is defined as a boot volume, you need to define another SSD volume in the storage group as the boot volume and copy the operating system image to that new SSD volume. Then proceed to step "4" on page 560.
    4. Select the **Modify** icon to modify the storage group and, on the **VOLUMES** tab, delete the SSD volume from the list of volumes for the storage group.

Request or create a FICON or FCP storage group
Depending on the authorization of your user ID, select **REQUEST STORAGE GROUP** or **CREATE STORAGE GROUP** to request FICON or FCP disk storage for partitions to use. Using this task does not require extensive knowledge of mainframes or Linux systems; however, a storage administrator must fulfill any requests for storage through tools for managing storage subsystems. After you have defined your storage requirements, DPM automatically generates a request that you can send to one or more storage administrators. You can edit the generated request to add your own greeting and more details, if

necessary. Note that, before you can successfully request storage, physical storage hardware (subsystems, switches, and so on) must be connected by cables, and storage cards must be configured.

Before you begin

- If you want to request Non-Volatile Memory Express (NVMe) storage for partitions to use, follow the procedure in "Request or create an NVMe storage group" on page 565.
- If you want to request FCP tape storage for partitions to use, follow the procedure in "Request or create a tape link" on page 567.
- For integrated requests and notifications, storage administrators (recipients) must have an email address associated with their user IDs, and Simple Mail Transfer Protocol (SMTP) settings must be defined. Users who send email through the **Request Storage** task do not require an assigned email address because DPM can generate one based on the user name, but the suggested practice is to assign email addresses for senders as well, so recipients know which person sent the email.
  - Email addresses for users are assigned through the **User Management** task.
  - The SMTP server and port settings are defined through the **Monitor System Events** task.

  If your installation does not have SMTP configured, you have the option of downloading or copying the generated request to send to one or more storage administrators.
- To request a storage group through the **Configure Storage** task, you can use the default SYSPROG or SERVICE user IDs, or any user IDs that an access administrator has authorized to the **Configure Storage** task through customization controls in the **User Management** task.
- You can define FCP or FICON storage groups with or without the use of a template.

  If you select a template that an administrator has created for use at your installation, you can modify the template contents. Depending on the template contents, creating a storage group can be as quick and easy as providing a unique name for the storage group, and sending a fulfillment request to a storage administrator. If you need to add to or modify the template contents to create your storage group, use the instructions in the following procedure for guidance.

  For information about creating templates, see the instructions in "Create and manage templates for FICON or FCP storage groups" on page 622.

About this task

To request storage for partitions to use, you define one or more storage groups. A *storage group* is a logical group of storage volumes that share certain attributes. For example, one attribute is shareability: you can define a storage group as either dedicated for use by only one partition, or shared by multiple partitions. FICON and FCP storage groups can be shared by multiple partitions, and multiple storage groups can be attached to one partition.

When you submit your request for one or more storage groups, DPM automatically generates the world wide port names (WWPNs) that are allocated to virtual storage resources when the storage group is attached to a partition. After your request is submitted, the storage administrator selects the physical storage volumes to fulfill your request.

Procedure

1. Open the **Configure Storage** task and select either **REQUEST STORAGE** or **CREATE STORAGE GROUP**.

   If any templates are available, select the template that you want to use. Otherwise, select the **Without Template** option. Note that templates are based on the storage group type: FCP or FICON. An administrator can create one or more templates for each type, even if no storage adapter cards of that type are configured for the system.
2. On the **Specify Storage Attributes** page, specify the attributes that you want for the new storage group.

a) For Type, select the type of storage: FICON or FCP.

This setting represents the type of storage devices that the storage group can use, and also controls the other attributes or default settings that are displayed on this page.

b) For Shareability, select either **Dedicated** or **Shared**.

If you select **Dedicated**, then only one partition is able to use this storage group. If you select **Shared**, specify the number of partitions that can share this storage group by moving the **Partitions** slider, typing a number in the input field, or clicking the up or down arrows to increase or decrease the number. The maximum number of partitions is set automatically to the system limit.

c) For Connectivity, specify the number of paths to be available for use by each operating system with access to this storage group.

The number of paths that you can define varies, depending on the storage group type. For FCP, the limit is the total number of adapters that are configured as FCP on the system; for FICON, the limit is the number of adapters that are configured as FICON on the system, up to a maximum of eight. The number that you select affects overall bandwidth, performance, and redundancy. Specify the number by moving the **Paths** or **Paths per Operating System** slider, typing a number in the input field, or clicking the up or down arrows to increase or decrease the number.

FCP
The suggested practice is to define at least two paths.

FICON
The suggested practice is to set the number of paths to the standard eight.

d) For a dedicated FCP storage group only, select **Optimized for 2nd level virtualization** when you want to enable the direct assignment of host bus adapters (HBAs) so an operating system or its guests can access the storage group.

Although the controls in the **Configure Storage** task allow you to select this attribute only for a dedicated (not shared) FCP storage group, you can optimize 2nd level virtualization for separate partitions so they can share the same storage disks. For instructions, see "Optimize 2nd level virtualization and share the same FCP disks across partitions" on page 625.

If you select this check box, specify the number of additional connections (HBAs) that can be assigned directly to the operating system or its guests. Specify the number by moving the **Additional HBAs** slider, typing a number in the input field, or clicking the up or down arrows to increase or decrease the number.

DPM distributes additional HBAs as equally as possible, taking into account both fabrics and adapters that will be assigned to this storage group, as indicated through the Connectivity attribute setting. For example, suppose that your storage configuration has two fabrics (A and B), the Connectivity attribute is set to 2, and you specify 7 additional HBAs. In this case, DPM creates a total of nine HBAs: one HBA for an adapter on fabric A and one for an adapter on fabric B to satisfy the Connectivity attribute setting, plus the seven additional HBAs. DPM assigns the seven additional HBAs as equally as possible, with four assigned to the adapter on fabric A, and the remaining three assigned to the adapter on fabric B.

e) Select **NEXT** to continue.

3. On the **Add Storage Volumes** page, specify the size and type of each volume to be added to the storage group.

If you are using a template for this storage request, the table on this page might contain predefined volumes that you can modify. Otherwise, this page initially contains a table heading with controls for defining a volume. The table columns vary, depending on the type of storage group (FCP or FICON) that you are creating. As you add volumes, the table is populated with a table row for each volume. Volumes of the same size are grouped into one expandable and collapsible row, with the total number of volumes in the group shown to the left of the table row. Use the arrow next to the total number to expand or collapse the table row. The table footer indicates the total size of the storage group, as you add or delete volumes.

Steps to define volumes for an FCP storage group

a. To specify the capacity of the volume, enter a number in the **Gibibytes** field or click the up or down arrows to increase or decrease the amount of gibibytes (GiBs).

b. For Type, select either **Data** or **Boot**. Select **Boot** only if this volume is to contain bootable programs, such as the image of the operating system to be installed in a partition. You can specify only one type for each volume, but you can define more than one volume of each type for the storage group.

c. Optional: Enter a description of this volume.

d. Optional: If you want to duplicate this volume definition, specify the number of copies by typing a number in the **Copies** field or clicking the up or down arrows to increase or decrease the number.

e. Select **ADD** to add this volume and its copies, if any. Details about the newly added volumes are displayed in a scrollable table, along with a footer that indicates the total number of volumes added and total amount of GiBs. If you added multiple volumes of the same size and type, they are grouped in a collapsible row. You can edit any of the table entries.

f. Repeat this process, as necessary, to define all of the volumes that you want to add to the storage group. If necessary, you can delete any volume from the table by selecting the trash can icon.

g. When you have finished defining volumes, select **NEXT** to continue.

Steps to define volumes for a FICON storage group

a. For Model, select one of the predefined models or Custom (EAV), depending on the size of volume that you want for the storage group. If you select a model, DPM automatically fills in the appropriate value for the Gibibyte and Cylinders fields.

b. If you selected Custom (EAV) for the model, enter one of the following amounts:

- The amount of GiBs in the Gibibyte field (DPM automatically calculates and displays the corresponding cylinder amount in the Cylinders field).
- The amount of cylinders in the Cylinders field (DPM automatically calculates and displays the corresponding GiBs amount in the Gibibyte field).

c. For Type, select either **Data** or **Boot**. Select **Boot** only if this volume is to contain bootable programs, such as the image of the operating system to be installed in a partition. You can specify only one type for each volume, but you can define more than one volume of each type for the storage group.

d. Optional: Enter a unique, four-digit hexadecimal device number in the range 0000 - ffff for this volume; otherwise, DPM automatically assigns a device number when the storage group is first attached to a partition. The suggested practice is to have DPM automatically assign device numbers to avoid conflicts.

e. Optional: Enter a description of this volume.

f. Optional: If you want to duplicate this volume definition, specify the number of copies by typing a number in the **Copies** field or clicking the up or down arrows to increase or decrease the number.

g. Select **ADD** to add this volume and its copies, if any. Details about the newly added volumes are displayed in a scrollable table, along with a footer that indicates the total number of volumes added and total amount of GiBs. If you added multiple volumes of the same size and type, they are grouped in a collapsible row. You can edit any of the table entries.

- If you selected Custom (EAV) but you change the Gibibytes or Cylinders field to a value that exactly matches the size of a predefined model, Custom (EAV) remains the Model value unless you explicitly change it.
- If you requested copies of this volume, DPM assigns device numbers in sequential order. For example, if you entered 1057 for the volume and requested four copies, the assigned device numbers are 1057, 1058, 1059, 105A, and 105B. You can edit these values, if necessary.

Note that, to avoid any numbering conflicts, DPM might change these device numbers later, when the storage group is attached to a partition.

h. Repeat this process, as necessary, to define all of the volumes that you want to add to the storage group. If necessary, you can delete any volume from the table by selecting the trash can icon.

i. When you have finished defining volumes, select **NEXT** to continue.

4. On the **Name and Duplicate** page, specify the name of your new storage group. Optionally, provide a description and, if you want to easily duplicate the storage group, enter the number of duplicates and select **DUPLICATE**.

   - For the name of the storage group, specify a value that is 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. The name must uniquely identify the storage group from all other storage groups that are defined for this system.
   - For the optional description, use up to the maximum of 200 characters.
   - If you request any duplicates, DPM uses the storage group name that you provided, and appends an underscore and sequential number to give each duplicate a unique name. You can edit the name of any duplicate, but all names must be unique.

   When you have finished, select **NEXT** to continue.

5. On the **Confirm** page, review the summary of your storage request.

   If necessary, select **EDIT** to change the attributes, name, description, duplicates (if any), or volumes. When you have finished, select **NEXT** to continue.

6. On the next page, review the automatically generated storage request, and send it to one or more storage administrators.

   The content of this page varies, depending on whether your installation has an SMTP server configured for integrated requests and notifications. If an SMTP server is configured, the page heading is **Send Request**; otherwise, the page heading is **Manually Send Request**. To complete your storage request, follow the steps for the appropriate page.

   On the Send Request page

   a. Select one or more storage administrators to receive your request.

   b. Optional: Add a personal message to the generated request.

   c. Select **SEND REQUEST** to send the request. If you requested duplicate storage groups, the text on this button indicates the number of requests to be sent.

   On the Manually Send Request page

   a. Either download or copy the generated request and send it to one or more storage administrators.

   b. Select **FINISH** to continue.

   DPM displays a message confirming that the requested storage groups were created.

Results

After your request is submitted, the storage administrator selects the physical storage volumes to fulfill your request.

- For an FCP storage group, DPM periodically checks for the requested volumes, and updates their fulfillment status on the **Storage Overview** tab of the **Configure Storage** task. When the storage administrator completes the configuration through tools for managing storage subsystems, DPM changes the storage group status to Complete.
- For a FICON storage group, the storage administrator not only completes the configuration through tools for managing storage subsystems, but also maps the base volumes (which were created on the storage subsystem to fulfill your request) to volumes that you requested for the storage group. DPM changes the storage group status to Complete only after the volumes have been mapped through the

Map Volumes action in the **Configure Storage** task. The **Map Volumes** action is accessible only through the **Storage Details** page for a FICON group, and is accessible only to storage administrators who are using the default STORAGEADMIN user ID, or a user ID with equivalent permissions.

What to do next

- You can create another storage group or select **GO TO STORAGE OVERVIEW** to view the status of the requested storage groups. If you are viewing a page in the **Configure Storage** task when the fulfillment status for the storage group changes to Complete, you receive an online notification.
- If you have defined boot and data volumes that are the same size, and your storage administrator fulfills your storage request with a preinstalled boot volume, you need to make sure that the correct volume is identified as the boot volume. Using the preinstalled boot volume ID that you receive from your storage administrator, go to **Storage Overview**, select the storage group to open the Storage Group details page, look up the volume ID on the **VOLUMES** tab, and make sure that the type for the preinstalled volume is Boot. If it is not, select the **Modify** icon to change the volume type.
- Use the **Partition Details** task to attach one or more storage groups to an existing partition, or attach them when you create a new partition through the **New Partition** task. You can attach storage groups that are not fulfilled yet; however, DPM issues a warning if you try to start a partition or apply changes to an existing partition before the storage group is fulfilled. Although the partition can be started, the operating system and applications that run on it might not function properly because some storage is not available until the fulfillment status for the storage group changes to Complete.

Request or create an NVMe storage group
Depending on the authorization of your user ID, select **REQUEST STORAGE GROUP** or **CREATE STORAGE GROUP** to request or create a Non-Volatile Memory Express (NVMe) storage group for a partition to use. NVMe storage is available only when the system has one or more IBM Adapter for NVMe1.1 features.

Before you begin

- If you want to request FICON or FCP storage for partitions to use, follow the procedure in "Request or create a FICON or FCP storage group" on page 560.
- To request a storage group through the **Configure Storage** task, you can use the default SYSPROG or SERVICE user IDs, or any user IDs that an access administrator has authorized to the **Configure Storage** task through customization controls in the **User Management** task.

About this task

In contrast to FICON and FCP adapters that provide access to external storage devices, NVMe storage adapters provide high-speed storage within a system. Each NVMe adapter consists of two pieces of hardware: an IBM-supplied carrier card installed in a system I/O drawer, and the solid state drive (SSD) that customers purchase.

To enable the use of NVMe storage on a DPM-enabled system, you need to create a storage group that contains one or more SSD volumes. Note that only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared.

To create an NVMe storage group, you need to select SSD volumes from a list of available SSDs, and name the new storage group. After you begin selecting SSDs for your storage group in step "3" on page 566, one or more SSDs might become unavailable; in this case, DPM highlights the SSD table entry with an error icon ( ). Before you can continue, you must remove the in-use SSD.

Procedure

1. Open the **Configure Storage** task and select either **REQUEST STORAGE** or **CREATE STORAGE GROUP**.

   The **Create Storage Group** page opens.

2. On the **Create Storage Group** page, select the **NVMe** tile under the "Without Template" heading.

   The **Add Storage Volumes** page opens. If SSDs are installed and available for use, the page display contains two tables: Volumes to be added and Available Volumes.

3. In the Available Volumes table, review the entries to determine which NVMe SSDs to add to the storage group.

   Note that the table display might contain collapsed rows when one or more SSDs have the same capacity and type; to expand these rows, select the number in the leftmost table column.

   a) Use the following information to select SSDs for your storage group.

   CAPACITY
   Indicates the size of the SSD volume in gibibytes (GiB).

   SERIAL NUMBER
   Specifies the serial number of the SSD volume.

   LOCATION
   Specifies the physical location of the NVMe carrier card in the I/O drawer of the system.

   b) Optionally, change the attributes of the SSD volume.

   - For Type, select either **Data** or **Boot**. Select **Boot** only if this volume is to contain bootable programs, such as the image of the operating system to be installed in a partition. You can specify only one type for each volume, but you can define more than one volume of each type for the storage group.
   - Enter a unique, four-digit hexadecimal device number in the range 0001 - ffff for this volume; otherwise, DPM automatically assigns a device number when the storage group is first attached to a partition. To avoid conflicts, the suggested practice is to have DPM automatically assign device numbers.
   - Enter a description of this SSD volume.

   c) Select **ADD** in the table row of each SSD that you want to add to the NVMe storage group.

   After you select an SSD, the SSD entry moves to the Volumes to be added table. Newly added volumes are indicated by a red dot in the leftmost column of the table.

   d) When you finish adding volumes, select **NEXT** to continue to the next page.

4. On the **Name and describe** page, specify the name of your new storage group. Optionally, provide a description.

   - For the name of the storage group, specify a value that is 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. The name must uniquely identify the storage group from all other storage groups that are defined for this system.
   - For the optional description, use up to the maximum of 200 characters.

   Select **NEXT** to continue to the next page.

5. On the **Confirm and create** page, review the summary of your storage group.

   a) If necessary, edit the name, description, or the volumes to be added.

   b) When you are satisfied with the details on the **Confirm and create** page, select **CREATE** to create the NVMe storage group.

Results

DPM creates the NVMe storage group and changes the screen display to the **Storage Overview**, where you can view the new storage group in the list. Note that the fulfillment state is Complete so the new storage group is ready for use.

What to do next

Use the **Partition Details** task to attach one or more storage groups to an existing partition, or attach them when you create a new partition through the **New Partition** task. Only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared.

Request or create a tape link
Depending on the authorization of your user ID, select **REQUEST TAPE LINK** or **CREATE TAPE LINK** to provide access for partitions to one FCP tape library in the storage area network (SAN). Also, you can use this task to manage FCP tape libraries in the DPM environment.

Before you begin

- Before you can successfully request or create a tape link, physical storage hardware (subsystems, switches, and so on) must be connected by cables, and storage cards must be configured. If the **REQUEST TAPE LINK** or **CREATE TAPE LINK** option is disabled, none of the system adapter cards are configured as FCP. Select **STORAGE CARDS** to view and configure the available system adapters.
- For **REQUEST TAPE LINK**, you can use the default SYSPROG or SERVICE user ID, or any user IDs that an access administrator has authorized to the **Configure Storage** task through customization controls in the **User Management** task.
- For **CREATE TAPE LINK**, you need a user ID with the same permissions as both the default SYSPROG and STORAGEADMIN user IDs.
- If your user ID is the default SYSPROG user ID or an equivalent user ID with the same permissions, DPM automatically generates a request that you can send to one or more storage administrators; this email includes zoning instructions for the storage administrators to follow to fulfill your request.

  For integrated requests and notifications, storage administrators (recipients) must have an email address associated with their user IDs, and Simple Mail Transfer Protocol (SMTP) settings must be defined. Users who send email through the **REQUEST TAPE LINK** or **CREATE TAPE LINK** task do not require an assigned email address because DPM can generate one based on the user name, but the suggested practice is to assign email addresses for senders as well, so recipients know which person sent the email.

  – Email addresses for users are assigned through the **User Management** task.
  – The SMTP server and port settings are defined through the **Monitor System Events** task.

  If your installation does not have SMTP configured, you have the option of downloading the generated request to send to one or more storage administrators.
- If you have a user ID with the same permissions as both the default SYSPROG and STORAGEADMIN user IDs, you can use the email that DPM automatically generates as a reminder to yourself to do the required zoning, or you can send it to other storage administrators to complete the required zoning for you. Depending on the SMTP configuration, you can either make use of the integrated email and notifications, or download the generated request to send it manually.

About this task

A *tape link* defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN. These connection attributes include storage resources such as system adapters, world wide port names (WWPNs), and the number of partitions that can share the connection. This connection is ready for use after the storage administrator completes zoning tasks through tools for managing storage subsystems. *Zoning* is the process of grouping two sets of WWPNs into one zone: the host WWPNs for the system and the target WWPNs for the tape drives in a tape library. This grouping enables communication between the system and the tape library, while preventing communication with other systems or SAN devices.

Creating a tape link can be as easy as providing a name for the tape link, and checking the default value for the number of connecting paths. In this case, the storage administrator selects the tape library and the system adapters to use for the tape link. Figure 35 on page 568 provides a graphical illustration of the physical and logical resources that are required for a tape link, and the process flow for requesting or creating one.

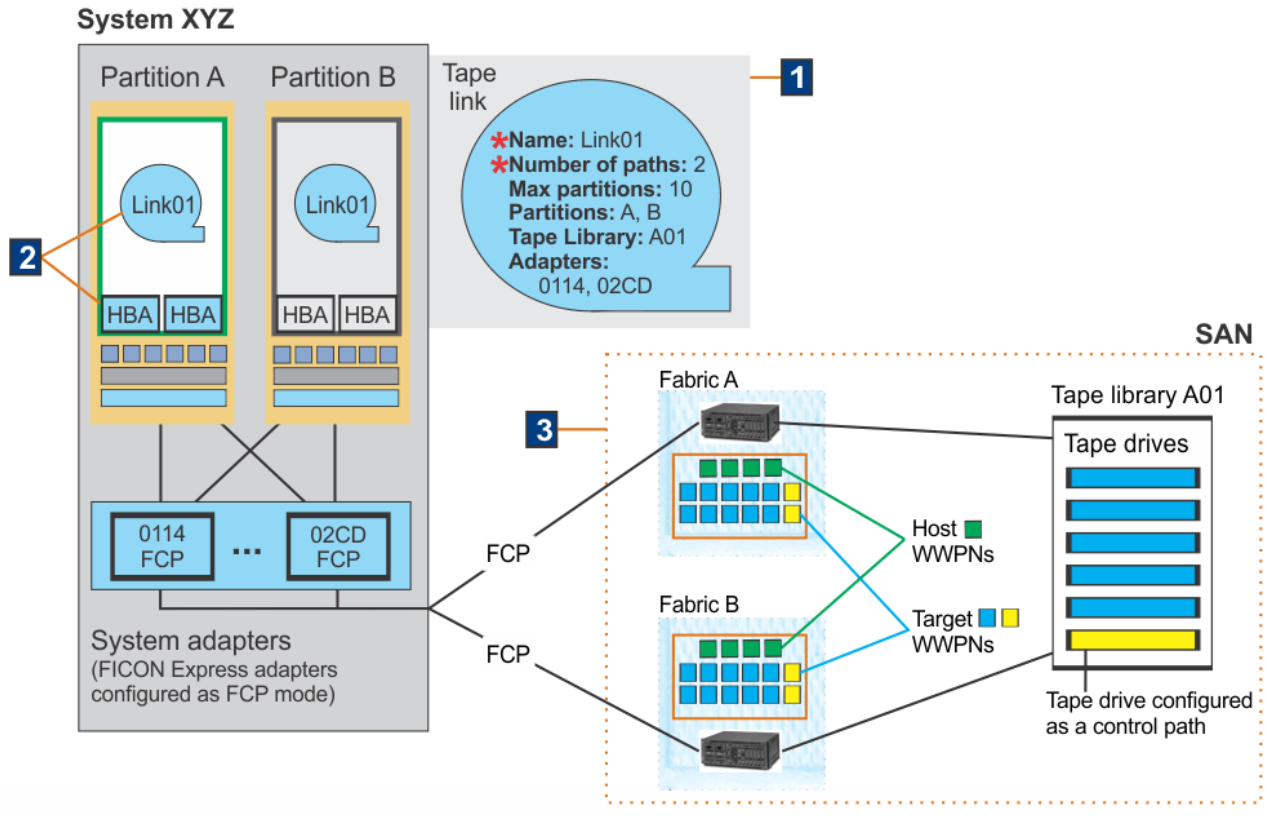


Figure 35. A tape link connects one or more partitions to one FCP tape library in the SAN

In Figure 35 on page 568:

1. You can request or create a tape link by providing a name for the tape link, and checking the default value for the number of connecting paths, which is set to 2. You can change this value to increase the number of connecting paths (decreasing the value to 1 is possible, but not a suggested practice). This example uses the default value, which means that two system adapters are required for a tape link named Link01.

   If you want additional control over the resources, you can optionally select specific partitions to which DPM attaches your tape link; set the maximum number of partitions that share the tape link; select a tape library; and select the system adapters. For this example, suppose that you select the following items.

   - Partitions A and B (A is active and B is stopped).
   - Tape library A01, which is already connected to system XYZ.

   When you select a tape library, DPM preselects adapters that are connected to the tape library already, and that provide optimal redundancy. Optimal redundancy for adapters is based on the following factors, which are listed in priority order from highest to lowest: on the location in the I/O drawers, on the drawer domain, on the current allocation, and on the connection to SAN fabrics. (If no adapters meet those criteria, DPM assigns placeholders for the storage administrator to select.) In this example, DPM selects FCP adapter 0114, which is connected to Fabric A, and 02CD, which is connected to Fabric B.

   After you confirm your request:

   - DPM automatically generates the WWPNs that storage administrators use to fulfill the tape link request. In this example, four host WWPNs are required: the number of paths (2) multiplied by the number of selected partitions (2).

- DPM also generates zoning instructions for the storage administrators who receive the request. For this example, the instructions list the four required host WWPNs; the two selected adapters; the fabrics to which those adapters are connected; and the tape library name.

2. After you send your request, DPM creates the tape link, sets its fulfillment state to Pending, and starts to run automated background checks every 10 minutes to determine when the required storage resources for this tape link are available. In these background checks, DPM tries to detect the tape drives (logical units or LUNs) for the WWPNs that are assigned to this tape link.

   Also, if you selected any specific partitions as part of your request, DPM asynchronously attaches the tape link to those partitions, automatically generating the virtual host bus adapters (HBAs) that the partitions need for access to the tape library. This attachment process might take some time, depending on the status and number of the selected partitions. The attachment to stopped partitions is relatively quick, but attachment to active partitions can take longer because these partitions might be busy. In this example, DPM creates two HBAs for partition A (which is active), and two for partition B (which is stopped).

3. To complete the connection from the system to the tape library, the storage administrator uses the generated instructions to configure the SAN devices. To properly configure a tape link connection to a tape library, the storage administrator:

   - Selects the tape library and the number of tape drives that are accessible through the tape link. In this example, you already selected tape library A01, so the storage administrator selects six tape drives in that library. Each of the six tape drives in tape library A01 are accessible through two target WWPNs (one for each port on the tape drive).
   - Ensures that one tape drive in the library is configured as a control path.
   - Zones the host and target WWPNs in each fabric. In this example, for the tape link connections to be complete, the storage administrator zones the four host WWPNs with the twelve target WWPNs in each fabric (A and B).

Depending on the zoning and the status of assigned resources, the fulfillment state for the tape link can change to Complete, Incomplete, or Pending with mismatches. Only when the fulfillment state of the tape link changes to Complete, DPM performs dynamic I/O operations to complete the connection to the tape library for started partitions, such as Partition A. For stopped partitions, such as Partition B, DPM performs dynamic I/O operations only when the stopped partition is started.

More information about fulfillment states is available through the **Tape Link details** page and its associated online help; this information includes possible user actions to resolve potential problems. To access the **Tape Link details** page, go to the **Storage Overview** page, scroll to the Tape Links table, and select the table row of the tape link that you want to review.

Procedure

1. Open the **Configure Storage** task and select either **REQUEST TAPE LINK** or **CREATE TAPE LINK**.

   The **Request tape link** or **Create tape link** page opens. The page display includes a tile for a new tape link request, and the FCP tape libraries table, which lists any tape libraries that DPM has discovered in the SAN. Above this table, the display includes either descriptive text or a time stamp indicating the last time, if any, that DPM discovered any correctly zoned FCP tape libraries. For discovered tape libraries, the table includes the tape library name (serial number), model, and state.

   You can request or create a tape link without specifying an available tape library. If you do not specify one, a storage administrator selects an available tape library for your tape link, when completing the required zoning tasks.

   - If the Tape libraries table is empty, or you want to view an updated list of available tape libraries that you can select in a later step, continue to step “2” on page 570.
   - If you do not want to view an updated list, or do not plan to specify a tape library for your tape link, skip to step “3” on page 570.

2. On the **Request tape link** or **Create tape link** page, update the list of tape libraries that are available for selection. (You can view the tape libraries on this page, but cannot select one for a tape link until step “5” on page 571.)

   To open the actions menu, select the ellipsis (•••) in the table header. The actions that you can select vary, depending on the permissions that are associated with your user ID, and on the zoning that is in place for the tape libraries in the SAN.

Option	Description
If no tape libraries are listed in the table	You have the option of selecting the tile in the center of the table, or opening the actions menu to select either **Request initial zoning** or **Start initial zoning**. Each of those three options cause DPM to generate an email with initial zoning instructions for a storage administrator. The instructions include the system management world wide port name (WWPN), which is a dedicated host WWPN that does not enable access to data in the tape library; its sole purpose is to enable DPM to discover (or detect) tape libraries in the SAN. The instructions tell the storage administrator to complete the following zoning tasks in fabrics (switches) for *each* tape library to be connected to the system. • Zone the system management WWPN with the target WWPN of at least one tape drive in the tape library. • Configure the tape drive associated with the target WWPN as a control path.
If the table has entries but you do not see the tape library that you want to use, or the time stamp is not recent	Select **Discover libraries** to cause DPM to perform a one-time check of the current connections to tape libraries in the SAN. Depending on the number of system adapters that are defined as FCP storage adapters, and the number of target ports that are currently zoned, this discovery check could take some time. **Discover libraries** is not available for selection until an administrator either requests initial zoning or requests a new tape link. If necessary, you can select **Resend zoning request** or **Update zoning** to resend the zoning instructions that DPM previously generated for the initial zoning request.

   When the initial zoning is complete or the **Discover libraries** check completes, the time stamp and table content are updated, and a notification message is displayed over the upper right corner of the page. The table displays the current state of any detected tape libraries.

   Available
   At least one physical path reaches the tape library. (Note that you cannot delete a tape library that is in this state.)

   Not available
   No physical path, including the system management WWPN path, reaches the library. This state usually indicates a tape library that was correctly zoned and used for one or more tape links, but is no longer connected. For a tape library in this state, you can select the **Remove libraries** action to display a trash can icon that you can select to remove the library from the table.

3. On the **Request tape link** or **Create tape link** page, select the **FCP tape link** tile under the "New request" heading.

   The **Name and partitions** page opens.

4. On the **Name and partitions** page, specify the name of your new tape link and an optional description. You can also specify other optional settings related to the partitions that can use this tape link.

   a) Provide the name and an optional description of the new tape link.

Tape link name
For the name of the tape link, specify a value that is 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. The name must uniquely distinguish this tape link from all other tape links that are defined for this system.

Description (optional)
For the optional description, use up to the maximum of 200 characters.

b) Optional: Select partitions to which you want the tape link attached, or define the maximum number of partitions that can attach the tape link, or both.

Select partitions (optional)
Use this section to identify the partitions to which you want DPM to attach the tape link. To fill in the table in this section:

1) Select **SELECT PARTITIONS** to open a dialog through which you can view details about available partitions on the system: the partition name; its current status (Active, Stopped, and so on); and the user-supplied description, if any.
2) Use the check box to select each partition, then select **ADD** to close the dialog and populate the partitions table on the **Name and partitions** page. You can remove any partition in that list by selecting the delete icon (trash can) in the corresponding table row.

Define the maximum number of partitions
Use this section to set the maximum number of partitions to which the tape link can be attached. The default value is 1. If you select partitions to attach the tape link, this number adjusts to match the number of selected partitions. You can either leave this adjusted value in place, or set the maximum manually: use the spinner or type the number that you want to set as the maximum.

The maximum value can exceed the number of selected partitions, if any; however, the maximum value cannot exceed the system limit for concurrently active partitions. The text for this field indicates the limit for concurrently active partitions on your system. Also, the maximum value cannot be less than the number of partitions that you have selected.

c) Select **NEXT** to continue to the next page.

The **Library and paths** page opens.

5. On the **Library and paths** page, select a tape library (optional) and decide whether to change the default number of paths for the tape link. You can also select specific system adapters to use for this tape link.

a) Optional: To select a tape library, select an entry for a specific library in the Tape library list. If no tape libraries are shown, or you do not select a specific tape library, the storage administrator selects a tape library when fulfilling your request for the tape link.

Note: The names of tape libraries in this list are the same as those shown in the Tape libraries table on the **Request tape link** or **Create tape link** page. If the state of one or more of these tape libraries is Not available, the tape library name is displayed in this list, but you cannot select it.

b) Decide whether to change the default number of connecting paths from the system to the tape library in the SAN. This connectivity setting has an impact on bandwidth, performance, and redundancy.

- The default value is 2, which you can change by using the "Number of connecting paths" slider, text entry field, or spin button.
- The maximum value is set to the number of system adapters that are currently configured as FCP adapters.

c) Decide whether you want to exchange any assigned adapters for your tape link.

- If you prefer to have the storage administrator either select the system adapters for your tape link, or to use the adapters that DPM automatically assigns (if any), you can select **NEXT** to continue to the next page, and skip to step “6” on page 573 of these instructions.

- Otherwise, select the check box to expand the **Advanced path settings** section and continue to step "5.d" on page 572.

d) View and optionally exchange the assigned adapters for your tape link.

The **Advanced path settings** section includes the Assigned adapters table, which contains the same number of table rows as the number of defined connecting paths. You might need to scroll through the table to view all of the rows. If you change the number of connecting paths while you are viewing the advanced path settings, the number of table rows changes according to your selection for connecting paths.

The content of the table rows depends on whether you selected a tape library in step "5.a" on page 571.

- If you did not select a tape library, each table row is a placeholder for an adapter that the storage administrator defines when fulfilling your tape link request.
- If you did select a tape library, DPM preselects adapters that are connected to the tape library already, and that provide optimal redundancy. Optimal redundancy for adapters is based on the following factors, which are listed in priority order from highest to lowest: on the location in the I/O drawers, on the drawer domain, on the current allocation, and on the connection to SAN fabrics. If no adapters meet those criteria, DPM assigns placeholders for the storage administrator to select.
  - Connected adapters are identified by the word "Matching" in the MATCH column; for better visibility, this word is highlighted with a colored background.
  - If the total number of preselected adapters is less than the number of connecting paths that you selected, placeholder rows represent the remaining number of adapters for the storage administrator to assign.

You can use **Advanced path settings** to exchange any assigned adapters with other available adapters, to select an available adapter to fill in a placeholder row, or to replace an assigned adapter with a placeholder row. If you decide to select adapters yourself, for the best results, try to assign adapters that reside in different system I/O drawers and in different domains; that are not on the same card; and that are connected to different fabrics. Inline messages provide warnings if the selected adapters do not meet these criteria.

To exchange an assigned adapter or placeholder row, complete the following steps.

1) Select the exchange icon () in the table row for an adapter that you want to replace. A dialog opens and displays information about the assigned adapter or placeholder row that you want to exchange, and available adapters to replace it.
2) If you want a storage administrator to select an adapter for you, select **Adapter to be assigned by the storage administrator** under the Available adapters heading. Otherwise, use the information in the Available adapters table to select a replacement adapter. Note that any adapter with an existing error condition is marked with an incomplete icon (). The suggested practice is to avoid selecting such adapters.

   MATCH
   If you selected a tape library and any adapters are already connected to it, this column contains the label "Matching" for connected adapters. Otherwise, this column is empty.

   NAME
   Specifies the name of the FCP adapter. DPM assigns a default adapter name in the form *adapter_type pchid partial_location*, which can help you determine whether you are selecting adapters that, for optimal redundancy, reside in different drawers and different domains. For example, in the sample default name `FCP 0171 Z22B-11`:

   - FCP is the type.
   - `0171` is the physical channel path identifier (PCHID).
   - `Z22B` is the plug location of the I/O drawer, with the first letter denoting the frame in which the drawer resides.

- 11 is the slot in the drawer in which the adapter is plugged.

FABRIC ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch. For optimal redundancy, use this value to select adapters that are connected to different fabrics.

ADAPTER ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

TYPE
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

LOCATION
Specifies the physical location of the adapter in the I/O drawer of the system.

ALLOCATION
Indicates the percentage of host bus adapters (HBAs) that are currently allocated to this adapter, shown in a bar graph and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. If the percentage is high (for example, 90%), consider assigning a different adapter.

3) Select **Replace** to apply your selection, close the dialog window, and return to the **Library and paths** page.
4) Repeat these steps, as necessary, to replace any more assigned adapters or placeholder rows.

e) Select **NEXT** to continue to the next page.

The **Confirm** page opens.

6. On the **Confirm** page, review the summary of details for your tape link. For the Partitions and Paths sections, you might have to select **Show all** to view all of the partitions and paths.

a) If necessary, select **EDIT** for Name, Partitions, Library, or Paths, to go back to the corresponding page and make changes.

Depending on system conditions, one or more errors might be detected; in this case, one or more error icons indicate what page you need to edit to resolve the errors. For example, if you selected an adapter that has since developed an error condition, an error icon is displayed next to the adapter in error, the Paths heading, and the LIBRARY & PATHS label in the progress bar above the **Confirm** page title.

b) When you are satisfied with the details on the **Confirm** page, select **NEXT** or **DONE** to continue to the next page.

Note that these buttons are disabled if you have not corrected all error conditions that require correction before you can request or create the tape link.

7. On the next page, send the automatically generated email to one or more storage administrators.

The content of this page varies, depending on whether your installation has an SMTP server configured for integrated requests and notifications. If an SMTP server is configured, the page heading is **Send request**; otherwise, the page heading is **Manually send request**. In either case, however, this page contains a plain-text attachment (with the .txt file format) with zoning instructions for storage administrators to use, including WWPNs and the selected tape library, adapters, and fabrics. If you did not select a tape library or any adapters, storage administrators are instructed to select a tape library, adapters, and fabrics of their choice.

To complete your tape link request, follow the steps for the appropriate page.

Send request

a. Select one or more storage administrators to receive your request.
b. Select **SEND** to send the request.

Manually send request

a. Download the generated request and send it to one or more storage administrators.

b. Select **FINISH** to continue.

Results

DPM creates the FCP tape link, changes the screen display to the **STORAGE OVERVIEW** page, and displays a message confirming that the requested tape link was created. In the Tape Links table, the fulfillment state for the tape link remains as Pending until the following conditions are met:

- The storage administrator completes the configuration through tools for managing SAN switches. Note that, depending on the zoning and the status of assigned resources, the fulfillment state for the tape link can change to Complete, Incomplete, or Pending with mismatches.
- DPM asynchronously attaches the tape link to the partitions, if any, that you selected as part of your tape link request. This attachment process might take some time, depending on the status and number of the selected partitions. The attachment to stopped partitions is relatively quick, but attachment to active partitions can take longer because these partitions might be busy.

  Only when the fulfillment state of the tape link changes to Complete, DPM performs dynamic I/O operations to complete the connection to the tape library for started partitions. For any stopped partition, DPM performs dynamic I/O operations only when the stopped partition is started.

What to do next

- To view more details about a specific tape link, click anywhere in a table row to open the Tape Link details page. For more information, see “Tape Link details” on page 597.
- To view, discover, or remove tape libraries from the DPM environment, select **REQUEST TAPE LINK** or **CREATE TAPE LINK**. For more information, see “Manage tape libraries” on page 626.
- If you did not select any specific partitions as part of your tape link request, use the **Partition Details** task to attach one or more tape links to an existing partition, or attach them when you create a new partition through the **New Partition** task. Through those tasks, you can view but cannot attach tape links that are in a pending fulfillment state (Pending or Pending with mismatches). For more information, see the online help for the appropriate task.

Storage Overview

Use the **Storage Overview** to view information about all of the storage groups and tape links that are defined for a DPM-enabled system. You can access the **Storage Overview** page by selecting **STORAGE OVERVIEW** in the **Configure Storage** task.

The **Storage Overview** page includes the Storage groups table, which contains one row for each storage group, and the Tape links table, which contains one row for each tape link. To view more details about a specific storage group or tape link, click anywhere in a table row to open the Storage Group details page or Tape Link details page. The fulfillment state indicates whether the storage group or tape link is available for use. Depending on the permissions that are associated with your user ID, you can select actions (such as modify or delete) for a specific storage group or tape link.

If no storage groups or tape links exist, the table includes a selectable tile through which you can request or create a new storage group or tape link.

- For more information about the table entries on the **Storage Overview** page, see “Columns and controls in the Storage groups table” on page 574 or “Columns and controls in the Tape links table” on page 576.
- For more information about the Storage Group details page, see “Storage Group details” on page 578.
- For more information about the Tape Link details page, see “Tape Link details” on page 597.

Columns and controls in the Storage groups table

Depending on the number of defined storage groups, you might need to scroll to view additional table rows; alternatively, use **Show items** to change the number of table rows to display. The table footer indicates the total number of storage groups that are listed in the table. You can also filter the table by

entering a search string; re-sort the table entries by selecting a column heading; and resize table columns.

NAME
Specifies the user-defined name of the storage group.

TYPE
Specifies the type of storage group: FICON or FCP or NVMe.

PARTITIONS
Specifies the number of partitions to which the storage group is attached.

SHAREABLE
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

TOTAL CAPACITY
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

DESCRIPTION
Specifies the user-provided description, if any, of this storage group. The description can be up to 200 characters in length.

FULFILLMENT STATE
Identifies the current state of the storage group. DPM runs a background check of storage resources for FCP storage groups and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours). Users can manually start a background check by selecting the **Connection Report** icon, and selecting the **Update report** icon (↻).

Checking migration
An existing DPM configuration was either upgraded on the same system, or migrated to another system that has DPM R3.1 or a later DPM version applied. This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

For more details about the migration or upgrade processes, see the *Dynamic Partition Manager (DPM) Guide*, which is available through the Library link on IBM Resource Link at http://www.ibm.com/servers/resourcelink

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

ACTIONS
In any table row, select the ellipsis (•••) to display a selectable list of actions that you can take for the storage group. The listed actions vary, depending on the type of storage group, and on the permissions that are associated with your user ID.

Connection Report
This action opens the connection report for the selected FCP or FICON storage group. For more details, see “Connection Report for an FCP Storage Group” on page 594 or “Connection Report for a FICON Storage Group” on page 596.

Delete Storage Group
For a FICON or FCP storage group, this action opens an automatically generated request to delete the selected storage group, which can be in any fulfillment state. For an NVMe storage group, this action opens a confirmation window for the delete request. Regardless of the storage group type, this action is disabled when the storage group is attached to any partitions.

To delete a FICON or FCP storage group, address the delete request to one or more storage administrators, optionally add a personal message, and select **SEND** to send the request. You need to enter your password to confirm the deletion request.

Duplicate Storage Group
This action opens the **Request Storage** task, through which you can duplicate the selected FICON or FCP storage group.

Map Volumes
This action opens the Map Volumes window through which a storage administrator can assign volumes for a FICON storage group only. This action is listed only for the default STORAGEADMIN user, or a user with equivalent permissions. For more details, see “Map Volumes” on page 588.

Modify Storage Group
For a FICON or FCP storage group, this action opens the **Request Storage** task. For an NVMe storage group, this action opens the Storage Group details page in Modification mode. You cannot modify a storage group that is in one of the following states: Pending with mismatches and Checking migration.

Although you can modify some FICON or FCP storage group information through the Storage Group details page, you must use the modify action to change the storage group attributes (type, shareability, and so on). For more details, see “Modify an FCP or FICON storage group” on page 589.

For an NVMe storage group, you can add or delete volumes, as well as modify any editable fields directly through the Storage Group details page, when the page is in Modification mode. Modification mode is indicated by a large blue bar that contains the Modification label, plus the **CANCEL** and **SAVE** buttons. For more details, see “Modify an NVMe storage group” on page 592.

Resend Request
This action opens a window containing a modification request that identifies actions for a storage administrator to perform to change the fulfillment state of a FICON or FCP storage group to Complete. This option is enabled only when the storage administrator has not yet completed all storage configuration tasks that are required to fulfill the most recent creation or modification request for the storage group.

Address the request to one or more storage administrators, optionally add a personal message, and select **SEND** to resend the request as email.

Columns and controls in the Tape links table

Depending on the number of defined tape links, you might need to scroll to view additional table rows; alternatively, use **Show items** to change the number of table rows to display. The table footer indicates the total number of tape links that are listed in the table. You can also filter the table by entering a search string; re-sort the table entries by selecting a column heading; and resize table columns.

NAME
Specifies the user-defined name of the tape link.

TYPE
Specifies the type of tape link: FCP.

PARTITIONS
Specifies the number of partitions to which the tape link is attached.

SHAREABLE
Specifies whether the tape link can be shared among partitions, or whether it is dedicated to only one partition.

TAPE LIBRARY
Specifies the serial number of the tape library that partitions can access through this tape link. If the value is "Not specified", the storage administrator has not yet selected a tape library for this tape link.

DESCRIPTION
Specifies the user-provided description, if any, of this tape link. The description can be up to 200 characters in length.

FULFILLMENT STATE
Identifies the current state of the tape link. DPM runs a background check of storage resources for FCP tape links and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours).

Complete
All of the storage resources listed in a create or modify request are available, properly configured and zoned, and DPM detects only those resources.

Incomplete
One or more storage resources for the tape link are marked as incomplete because the resource is missing, or in an error or degraded condition. Because DPM periodically checks the availability of storage adapters, switches, and tape libraries that are in use for a tape link, resources that were functioning properly can become incomplete.

Pending
One or more requested storage resources are not yet available or zoned correctly, or the tape link is not yet attached to all partitions that were specified in the original create request or a modify request.

Pending with mismatches
DPM detects system adapters that do not match the original create request or a modify request. Either the number of system adapters does not match the number of connecting paths, or the detected adapters do not match specific adapters that were assigned to the tape link.

ACTIONS
In any table row, select the ellipsis (•••) to display a selectable list of actions that you can take for the tape link. The listed actions vary, depending on the permissions that are associated with your user ID. Note that some actions produce an automatically generated request to send to a storage administrator. For integrated requests and notifications, storage administrators (recipients) must have an email address associated with their user IDs, and Simple Mail Transfer Protocol (SMTP) settings must be defined. If email support is not configured, users have the option of downloading storage requests to send them through other methods.

Resend Request
This action opens a window containing an automatically generated request that includes zoning instructions for incomplete or pending storage resources. You can select this action only when the tape link is in one of the following fulfillment states: Incomplete, Pending, or Pending with mismatches. If the tape link state is Incomplete because of adapter errors, or the state is Pending because tape link attachment operations are in progress, this action is disabled until the errors are resolved or the attachment operations are complete.

Open Details
This action changes the page display to the **Tape Link details** page for a specific tape link.

Modify
This action changes the page display to the **Tape Link details** page in modification mode. Modification mode is indicated by a large blue bar that contains the Modification label, plus the **CANCEL** and **SAVE** buttons.

Delete

This action opens a window containing an automatically generated request to delete the selected tape link, along with attached instructions for deleting the tape link from the SAN configuration. You can delete a tape link that is in any fulfillment state; however, the **Delete** action is disabled if the tape link is attached to any active partitions, or when any asynchronous attachment or detachment operations are in progress. If the tape link is attached to any stopped partitions, you can either cancel or continue with the delete request through a confirmation dialog.

During the delete process, DPM detaches the tape link from each partition before deleting the tape link itself. Depending on the number of partitions, the delete request might take some time, during which one or more stopped partitions might be started. In this case, the delete operation is canceled, but you receive an error dialog that lists the partitions to which the tape link remains attached. Through this dialog, you can restart the delete operation.

Storage Group details

Use the Storage Group details page to view or modify information about a specific storage group on a DPM-enabled system. The Storage Group details page consists of a summary, a set of action icons, and tabbed sections that you can select to change the lower portion of the page display.

For specific fulfillment states, note that various summary fields, tabbed sections, and table entries have a pending, incomplete, or warning icon to alert you to details that might need your attention or action. For example, if a volume is being deleted, the following information is displayed.

- The value in the Fulfillment state summary field is Pending.
- The Volumes summary field lists both the current and future total number of volumes for the storage group.
- A pending icon ( ) is displayed next to the **VOLUMES** tab.
- A pending icon is displayed next to the table row of the volume to be deleted, and the information in that row is crossed out.

For pending states, the summary fields and table entries indicate not only the current information, but also the pending change. For example, if the storage group currently has 2 volumes and a pending request will add two more volumes, the Volumes field in the summary lists both the current number and future number: 2 -> *4*

The heading on this page includes the storage group name, which you can edit. If you modify the name, specify a value that is 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. The name must uniquely identify the storage group from all other storage groups that are defined for this system.

If you make any changes that might affect a running partition to which the storage group is attached, DPM provides warning messages that indicate which partitions are affected. If you confirm the changes, and need more details about the affected partitions, go to the **HISTORY** tab and review the information in the ACTION column. In some cases, the changes that you make can require updates in the operating system that the affected partition hosts; these details are available through links in the ACTION column entry.

For more details about the elements of the Storage Group details page, see the following topics.

- “Summary section of the Storage Group details page” on page 578
- “Action icons on the Storage Group details page” on page 580
- “Tabs on the Storage Group details page” on page 580

Summary section of the Storage Group details page

The summary fields display the attributes and current state of the storage group. Note that the pending icons (or), incomplete icon ( ), and warning icon ( ) indicate details that might require your attention or action.

Type
Specifies the type of storage group: FICON or FCP or NVMe.

Total capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Volumes
Specifies the total number of storage volumes that are assigned to the storage group. Any alias volumes for a FICON storage group are not included in this count.

Shareability
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition. The user-supplied maximum number of partitions is included in this field.

Description
Specifies the user-supplied description for this storage group.

Fulfillment state
Specifies the current state of the storage group. DPM runs a background check of storage resources for FCP storage groups and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours). Users can manually start a background check by selecting the **Connection Report** icon to open the Connection Report, and selecting the **Update report** icon ().

Checking migration
An existing DPM configuration was either upgraded on the same system, or migrated to another system that has DPM R3.1 or a later DPM version applied. This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

For more details about the migration or upgrade processes, see the *Dynamic Partition Manager (DPM) Guide*, which is available through the Library link on IBM Resource Link at http://www.ibm.com/servers/resourcelink

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

The **VOLUMES** or **ADAPTERS** tab, and specific table entries for the tab display, are marked with the incomplete icon ().

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems. When a creation, modification, or deletion request is in progress, the affected summary fields, section tabs, and table entries are marked with the pending icon ().

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size. The **VOLUMES** tab has a pending icon () next to it, and the table rows for mismatched volumes are marked with a warning icon ().

Connectivity
Specifies the number of paths that are available for use by each operating system with access to a FICON or FCP storage group.

Storage group ID (UUID)
Specifies the DPM-generated universally unique identifier (UUID) for this storage group.

Action icons on the Storage Group details page

The actions that are displayed depend on the fulfillment state of the storage group, the type of storage group, and the authorization of the user who is accessing the Storage Group details page.

Connection Report
This action opens the connection report for the selected FCP or FICON storage group. For more details, see “Connection Report for an FCP Storage Group” on page 594 or “Connection Report for a FICON Storage Group” on page 596.

Delete
For a FICON or FCP storage group, this action opens an automatically generated request to delete the selected storage group, which can be in any fulfillment state. For an NVMe storage group, this action opens a confirmation window for the delete request. Regardless of the storage group type, this action is disabled when the storage group is attached to any partitions. To determine which partitions are using the storage group, select the **PARTITIONS** tab on the Storage Group details page.

To delete a FICON or FCP storage group, address the delete request to one or more storage administrators, optionally add a personal message, and select **SEND** to send the request. You need to enter your password to confirm the deletion request.

Map Volumes
This action opens the Map Volumes window through which a storage administrator can assign volumes for a FICON storage group only. This action is listed only for the default STORAGEADMIN user, or a user with equivalent permissions. For more details, see “Map Volumes” on page 588.

Modify
For a FICON or FCP storage group, this action opens the **Request Storage** task. For an NVMe storage group, this action opens the Storage Group details page in Modification mode. You cannot modify a storage group that is in one of the following states: Pending with mismatches and Checking migration.

Although you can modify some FICON or FCP storage group information through the Storage Group details page, you must use the modify action to change the storage group attributes (type, shareability, and so on). For more details, see “Modify an FCP or FICON storage group” on page 589.

For an NVMe storage group, you can add or delete volumes, as well as modify any editable fields directly through the Storage Group details page, when the page is in Modification mode. Modification mode is indicated by a large blue bar that contains the Modification label, plus the **CANCEL** and **SAVE** buttons. For more details, see “Modify an NVMe storage group” on page 592.

Resend Request
This action opens a window containing a modification request that identifies actions for a storage administrator to perform to change the fulfillment state of a FICON or FCP storage group to Complete. This option is enabled only when the storage administrator has not yet completed all storage configuration tasks that are required to fulfill the most recent creation or modification request for the storage group.

Address the request to one or more storage administrators, optionally add a personal message, and select **SEND** to resend the request as email.

Tabs on the Storage Group details page

The tabbed sections provide more details related to the storage group. The tabbed sections vary, depending on the type of storage group. Note that the pending icons (or), incomplete icon ( ), and warning icon ( ) indicate details that might require your attention or action.

When you select a tab, the content of the Storage Group details page changes. For more details about each tab, see the following topics.

- “VOLUMES” on page 581

- “PARTITIONS” on page 584
- “ADAPTERS” on page 585
- “WWPN” on page 586 (displayed for FCP storage groups only)
- “HISTORY” on page 586

VOLUMES

The **VOLUMES** tab display varies, depending on the type of storage group. For an FCP or NVMe storage group, the tab displays a single table that lists all volumes associated with the storage group. For a FICON storage group, the tab displays two tables: Base Volumes and Alias Volumes. Depending on the number of base volumes, you might need to scroll to view the Alias Volumes table.

Volumes of the same capacity and type are shown in a group, with the total number of volumes in the group shown to the left of the table row. Use the arrow next to the total number to expand or collapse the table row. If any volumes have associated errors or warnings, those volumes are listed at the beginning of the table. For more information about resolving device conflicts associated with FICON alias volumes, see “Resolve alias volume device number conflicts” on page 587.

The **VOLUMES** tab display also varies depending on the current fulfillment state of the storage group. Table 12 on page 581 lists the fulfillment states, describes the table display, and provides possible actions you might take to resolve any issues. Note that, in some cases, more than one type of pending request might be in effect.

Table 12. Effect of fulfillment status on the Volume tab display

Fulfillment state	Volume tab display	Possible action
Checking migration This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.	The display contains an empty Volumes table.	When DPM completes the check, it changes the fulfillment state to Complete or Pending with mismatches. In some cases, this check detects a storage group that cannot be fulfilled because logical unit numbers (LUNs) are not visible. For such cases, the fulfillment state does not change from Checking migration. For DPM to recheck the storage group and change the fulfillment state, the storage administrator must fix the configuration in the storage subsystem, and an administrator must open the **Connection Report** and select the **Update report** icon ().
Complete This fulfillment state indicates that DPM has successfully detected all of the logical and physical elements that support the volumes in this storage group. Note that DPM can mark a FICON storage group as Complete even if some requested alias devices were not included because of device number conflicts with base volumes.	The display contains a table entry with complete information for all volumes in this storage group.	None. If alias volumes are excluded from a FICON storage group, scroll to view the Alias Volumes table; if some alias volumes were not included, an inline message prior to the table indicates the number of alias volumes that were excluded, and provides a link through which you can open a new window to view and resolve specific device number conflicts.

Table 12. Effect of fulfillment status on the Volume tab display (continued)

Fulfillment state	Volume tab display	Possible action
Incomplete This fulfillment state indicates that one or more volumes are incomplete. Volumes can be marked as incomplete under the following conditions. • When DPM can no longer detect them in the FICON configuration. • When DPM found a problem when checking the results of a system migration or firmware upgrade process to the DPM R3.1 storage management feature or a later release. • When DPM detects that an NVMe adapter has become degraded or the NVMe SSD was incorrectly removed from its carrier card.	An incomplete icon ( ) is displayed in the table entry of each incomplete volume.	To diagnose the problem for an FCP or FICON storage group, select the **Connection Report** action icon ( ). When an NVMe storage group is marked as Incomplete, go to the **HISTORY** tab and check entries in the Actions table to find more details about the specific error. • You can remove the volume that is marked with the incomplete icon, but you do not need to take any action as long as the NVMe storage group contains other volumes that are usable. The Incomplete fulfillment status and incomplete icons continue to be displayed for the SSD until a repair is completed under the direction of a service representative. • If you do not remove the volume and the NVMe SSD in error is later reinstalled or replaced, DPM detects the repair, and either changes the fulfillment state to Complete or to Pending with mismatches. Note that, if the SSD in error is replaced by a different SSD, DPM automatically changes the serial number of the volume.
Pending (creation request) When a creation request is in progress, this fulfillment state indicates that some information in the volume table is not available yet.	A pending icon ( ) marks incomplete table rows until DPM provides the information.	In the case of a FICON storage group, a storage administrator must select the Map Volumes action icon ( ) and complete that task before DPM can complete the table.
Pending (modification request) This fulfillment state indicates that a modification request is in progress for one or more volumes.	A pending icon ( ) marks the table entries for volumes to be modified. The CAPACITY column indicates not only the current volume size, but also the pending change.	None. When the modification request is satisfied, the pending icons are removed, and the CAPACITY column values are updated to show only the modified size.
Pending (deletion request) This fulfillment state indicates that a deletion request is in progress for one or more volumes.	A pending icon ( ) marks the table entries for volumes to be deleted, and the values in those table entries are crossed out.	None. When the deletion request is satisfied, the table entries are removed from the display.

Table 12. Effect of fulfillment status on the Volume tab display (continued)

Fulfillment state	Volume tab display	Possible action
Pending with mismatches This fulfillment state indicates that DPM has detected changes to the number, size, or accessibility of volumes in the storage group. The following items describe the various conditions under which DPM assigns this fulfillment state to an FCP or NVMe storage group. 1. DPM detected more volumes for an FCP storage group than the number that was originally requested. 2. DPM detected the correct number of volumes in an FCP storage group, but the volume sizes are either larger or smaller than originally requested. 3. DPM detected a volume but that volume is not accessible through all of the worldwide port numbers (WWPNs) that are available for use with an FCP storage group. 4. As part of a repair, an NVMe SSD was replaced by an SSD with a larger or smaller capacity.	All of the mismatched volumes are displayed at the top of the table, enclosed in a box. A warning icon (⚠) is displayed in the CAPACITY column of each mismatched volume. Both the previous and current sizes are shown in the CAPACITY column, along with a message that explains the mismatch.	• The first two conditions for an FCP storage group can be resolved by selecting either **REQUEST DELETION** to remove the volumes or **KEEP IN GROUP**. Use the check boxes to select the mismatched volumes that you want to keep or delete. Note that you can modify the type or description of these mismatched volumes, and these changes are saved when you select **KEEP IN GROUP**. • The third condition for an FCP storage group can be resolved only by a storage administrator, through the storage management subsystem; checking the connection report can help identify the errors that need to be corrected. • For a replacement NVMe SSD that is not the same size as the removed SSD, you can either keep the replacement SSD as a volume in the storage group, or modify the storage group to remove the replacement SSD or add different SSDs.

The following list describes the columns for the tables in the **VOLUMES** tab display. Note that the modifiable attributes (type, device number, and description) specified for any NVMe SSD volume persist, even after you delete the volume from the storage group, or delete the storage group itself.

STORAGE SUBSYSTEM
Specifies the name of the storage subsystem in which the base or alias volume resides. This column is only included in the Base Volumes and Alias Volumes tables for a FICON storage group.

VOLUME ID
Specifies the identifier for a base or alias volume. The ID is a combination of the logical control unit (LCU) number and volume ID. This column is only included in the Base Volumes and Alias Volumes tables for a FICON storage group.

VOLUME UUID
Specifies the universally unique identifier (UUID) of the volume. This column is only included in the Volumes table for an FCP storage group.

CAPACITY
Specifies the size of the volume in gibibytes (GiBs). This column is only included in the Volumes table for an FCP storage group, and in the Base Volumes table for a FICON storage group.

SERIAL NUMBER
Specifies the serial number of the installed NVMe SSD. This column is only included in the Volumes table for an NVMe storage group.

TYPE
Specifies the volume type as either Boot or Data. You can change this volume attribute from Data to Boot only when no active partitions are using this volume; you must select **SAVE** to save this change. This column is included in the Volumes table for an FCP storage group, in the Volumes table for an NVMe storage group, and in the Base Volumes table for a FICON storage group.

LOCATION
Specifies the physical location of the NVMe adapter in an I/O drawer of the system. This column is only included in the Volumes table for an NVMe storage group.

DEVICE NO.
Specifies the DPM-generated or user-supplied 4-digit hexadecimal device number for the volume. This column is only included in the Base Volumes and Alias Volumes tables for a FICON storage group, and in the Volumes table for an NVMe storage group.

Note that you can overwrite this value by typing in the column field only when the storage group is not attached to any partitions. If you change the device number, specify a four-character hexadecimal device number. For FICON storage groups, volume device numbers must be in the range 0000 - ffff, and must be unique within a storage group and across all attached partitions and partition resources. For NVMe storage groups, volume device numbers must be in the range 0001 - ffff, and must be unique within a storage group and across all attached partitions and partition resources.

DESCRIPTION
Specifies the user-supplied description, if any, for this volume. Note that you can overwrite this value by typing in the column field. You can use up to the maximum of 200 characters.

CONFIG DETAILS
Contains a link that opens a new window, Configuration details, to display configuration details that you can copy to the clipboard. System administrators require these volume configuration details under the following circumstances:

- When they initially configure partition resources through configuration files on the operating system that the partition hosts. These volume configuration details are required to ensure that the storage group is visible to the operating system that runs on the partition.
- When they are configuring an installer to access a storage device that is defined as the boot device for a partition.

The **GET DETAILS** link is available and enabled only for the following volumes.

- Base volumes in a FICON storage group, only when the base volume is already mapped to a logical unit (LUN).
- All volumes in an FCP storage group, only when the storage group is currently attached to at least one partition.
- Volumes that are defined as boot or data volumes. Data volumes are included because you can change a data volume to a boot volume at any time.

For more information, see "Configuration details" on page 587.

PARTITIONS
The **PARTITIONS** tab lists the partitions to which the storage group is attached. If necessary, you can select one or more partitions in the table and detach the storage group from them by selecting **DETACH STORAGE GROUP**. This action can be disruptive when the partitions are in Active state, are in Paused state, or are using a volume in the storage group as a boot volume. In such cases, a warning, error, or informational message is displayed and you are prompted to confirm the detachment. Note that only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared.

The following list describes the columns in the Partitions table.

NAME
Specifies the name of the partition. The name is a hyperlink through which you can open the **Partition Details** task.

STATUS
Specifies the operating status of the partition. The two status values of most interest are Active and Paused because you cannot select partitions in those two states to detach the storage group from them. For descriptions of other possible status values, open the **Partition Details** task and view the online help for the Status section.

DESCRIPTION
The user-supplied description, if any, of the partition.

For an FCP storage group only, each row in the Partitions table can be expanded to show details about the host bus adapters (HBAs) that the partition is using to access storage.

- If necessary, you can select **CHANGE ADAPTERS** to review the adapters assigned to a storage group and remove or replace them with other adapters that are available for use by a partition.
  - You can change an adapter only when an HBA with a backing adapter is available.
  - If an FCP adapter is configured while the storage group is attached to an active partition, DPM cannot detect and list the new adapter as available for use by any partition. In this case, before you can assign the new adapter, stop all active partitions to which the storage group is attached, and select the **Connection Report** icon to start a background check of the available connections for this storage group. Then you can assign the new adapter and restart the partitions.

  For more details about changing adapters, see "Change the adapters assigned to an FCP storage group" on page 593.
- If an adapter that is assigned to an HBA becomes incomplete, the table entry for the HBA and the table entry for the partition are both marked with an incomplete icon ( ). If one or more adapters are incomplete, the fulfillment status of the storage group is Incomplete.
- If the storage group is in a pending fulfillment state, only the HBA name and editable device number are displayed in the Host Bus Adapters table.

The following list describes the details in the Host Bus Adapters table.

NAME
Specifies the name of the HBA.

DEVICE NUMBER
Specifies the hexadecimal device number of the HBA. If you change the device number, specify a four-character hexadecimal device number. For FICON storage groups, volume device numbers must be in the range 0000 - ffff, and must be unique within a storage group and across all attached partitions and partition resources.

WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a port in a storage subsystem that is connected to the system.

FABRIC ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

ADAPTER ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

ASSIGNED ADAPTER
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

ADAPTERS
The **ADAPTERS** tab lists the adapters that are assigned to the storage group.

- If adapters are not yet assigned, the **ADAPTERS** tab has a pending icon ( ) next to it, and the Adapters table is empty. The total at the foot of the Adapters table lists how many adapters are assigned to the storage group.
- If an existing adapter becomes incomplete, the **ADAPTERS** tab has an incomplete icon ( ) next to it, and the table entry for that adapter is highlighted with the incomplete icon. If one or more adapters are incomplete, the fulfillment status of the storage group is Incomplete.

NAME
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

ADAPTER ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

TYPE
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names and NVMe adapter names.

LOCATION
Specifies the physical location of the adapter in the I/O drawer of the system.

ALLOCATION
Indicates the percentage of host bus adapters (HBAs) that are currently allocated to this adapter, shown in a bar graph and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. For an NVMe adapter, the allocation value is either 0 (when the adapter is available for use) or 100 (when a partition is using the adapter).

WWPN
The **WWPN** tab lists the worldwide port numbers (WWPNs) that are available for use. This tab is displayed only for an FCP storage group. The tab display contains two tables: one table that lists each WWPN that is in use by a partition, and one table that lists unused WWPNs. The following list describes the columns that are displayed in each table.

WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a port in a storage subsystem that is connected to the system.

STATE OF WWPN
Indicates the current state of the WWPN.

Validated
DPM detected the WWPN and found the logical unit number (LUN) that represents the storage device that is configured in the storage controller.

Not validated
The storage administrator has not activated this WWPN.

Incomplete
DPM could not detect this WWPN on all required fabrics and the subsystem. Incomplete WWPNs are marked with an incomplete icon ( ). If one or more WWPNs are incomplete, the fulfillment status of the storage group is Incomplete.

NAME (VHBA)
Specifies the name of the host bus adapter (HBA) that provides a partition with access to external storage area networks (SANs) and devices that are connected to a system. This column is displayed only in the table of WWPNs that are in use.

PARTITION
Specifies the name of the partition that is using the WWPN. This column is displayed only in the table of WWPNs that are in use.

HISTORY
The **HISTORY** tab lists the actions that users have taken for this storage group. The most recent action is listed at the top of the History table. Information in the ACTION column not only briefly describes the activity, but also preserves details such as requests that were sent to storage administrators for fulfillment. If the storage group is deleted, you can access the history details only for the next 30 days, by using the HMC Web Services API for DPM.

The History table contains the following columns.

TIME
Specifies the date and time when the action was taken, in the format `yyyy-mm-dd hh:mm AM|PM`

USER
Specifies the user ID of the person who initiated the action. If DPM initiated the action, "no user" is displayed in this column.

ACTION
Describes the action that was performed. Note that some words in the description are selectable links through which you can view details about the specific action. For example, for a modification request, you can use the link to open the email that DPM generated for that request. Depending on the action that was performed, the associated details can include instructions for additional user action; for example, changing a device number can require issuing a configuration command on the operating system. In these cases, a red dot is displayed next to the table row until a user selects the link to view the details.

When the storage group is attached to one or more partitions, some changes that are made to the storage group can require corresponding changes on the operating system that the partition hosts. In this case, use the link in the ACTION column entry to display a list of required updates.

FULFILLMENT STATE
Specifies the fulfillment state that resulted from the action.

Resolve alias volume device number conflicts
Use this window to view and resolve the device number conflicts between the base and alias volumes of a FICON storage group.

This window displays the following two tables.

Base Volumes
The Base Volumes table lists the volumes with device numbers that conflict with the alias volumes. To include the alias volumes, change the device number of the base volume. This table includes the following details.

- The storage subsystem in which the base volume resides.
- The volume ID that identifies the base volume.
- The base volume type: Boot or Data.
- The device number of the base volume, which is editable depending on the shareability of the FICON storage group, whether the storage group is already attached to a partition, and the current state of that partition.

Excluded Alias Volumes
The Excluded Alias table lists the alias volumes with device numbers that conflict with the base volumes. This table includes the following details.

- The non-editable device number of the alias volume.
- The volume ID that identifies the alias volume.
- The status of the alias volume, which indicates whether the volume is included in the storage group. Initially, all alias volumes are shown as excluded. If you change the device number of the corresponding base volume, the status of the alias volume changes to resolved and included.

Configuration details
Use the **Configuration details** window to view information that you need to enable a partition's operating system or installer to access a volume of a FICON or FCP storage group.

The window display varies, depending on the storage group type.

- For a base volume in a FICON storage group, the only detail that is displayed in the new window is the volume device number (which is the same value as shown in the DEVICE NO. column of the **Storage Group details** window). The display includes a link through which you can copy that device number to the clipboard.
- For a volume in an FCP storage group, you must select a partition from the list of partitions to which the storage group is attached. After selecting a partition, the volume configuration details are displayed in table format. Use the details in each table row to configure access to the volume for the partition's operating system or installer. You can copy the details from one table row at a time; use the details from more than one row when you want to configure multipath access.

DEVICE NO.
Specifies the DPM-generated or user-supplied 4-digit hexadecimal device number of a host bus adapter (HBA) that provides a partition with access to the volume. Each HBA can provide more than one path to a volume, so the table might contain multiple rows for the same device number.

TARGET PORT WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a port in a storage subsystem that is connected to the system.

LUN NO.
Specifies the 16-character hexadecimal string (64-bit binary number) that identifies the logical unit (LUN) that represents the storage device on which the volume resides.

When you select **COPY TO CLIPBOARD** in the **ACTION** column, all three values are copied in the same sequence in which they appear in the table row, with values separated by a comma.

Map Volumes
Use the **Map Volumes** window to complete a creation request or a modification request for a FICON storage group. You can also add logical control units (LCUs) to the configured storage subsystems. This window is accessible only through the **Storage Details** page for a FICON group, and is accessible only to storage administrators who are using the default STORAGEADMIN user ID, or a user ID with equivalent permissions. Storage administrators access this page to fulfill a request that they receive from a system administrator.

About this task

To completely fulfill a creation request for a FICON storage group, a storage administrator must select predefined volumes in the storage subsystem to match the requested volumes. The requested volumes are listed in the request that is generated and sent when a system administrator uses the **Request Storage** task to create a new FICON storage group. A modification request can list volumes to be removed or modified, as well as volumes to be added to an existing FICON storage group.

Using the information in the request, DPM populates the two sections of the Map Volumes window: Predefined Volumes and Requested Volumes. The Predefined Volumes section contains information about the physical storage hardware that administrators defined through the **Configure FICON Connections** task. The Requested Volumes section contents visually represents the information in the request.

- For a creation request, DPM populates the Requested Volumes section with boxes that represent the volume size; each box is labeled with the model number or custom EAV size that the system administrator requested. Each box contains empty slots for the requested number of volumes.
- For a modification request, DPM populates the Requested Volumes section with boxes for the existing models and volumes. For volumes to be added, the volume slot is empty. For volumes to be modified, a message indicating the size change is shown below the volume slot, along with a **CONFIRM** button. Volumes to be deleted are not shown in the Requested Volumes section.

Procedure

1. Review the list of volumes under the Predefined Volumes heading.

   By default, the list contains the volumes in all configured storage subsystems that meet or exceed the requested number of paths per LCU. If the list is empty because the predefined volumes do not satisfy the requested number of paths, select the **Manage LCUs** link to open the **Configure FICON Connections** task.

   If necessary, you can filter the list by selecting one or more subsystems from the Select Subsystem drop-down list, or by using the search field to enter one or more LCU or volume numbers, or a range of numbers. You can also add LCUs by selecting the **Add LCUs** link, which opens the **Configure FICON Connections** task.

2. Review the volumes that are displayed in the Requested Volumes section. Make sure you note any volumes that are designated as boot volumes.

   Each volume slot is labeled with a partial description, if any, that the administrator provided in the storage request. If the administrator designated a volume as a boot volume, the slot label starts with Boot.

   For a modification request, the existing volume information is displayed in the slots within the model boxes. For volumes to be added, an empty volume slot indicates where you can add a predefined volume to fulfill the modification request. For volumes to be modified, a message indicating the size change is shown below the volume slot, along with a **CONFIRM** button. Empty slots in other model boxes indicate where you can move those volumes. In addition, a message at the bottom of the Requested Volumes section indicates the total number of volume size changes, along with a **CONFIRM ALL SIZE CHANGES** button.
3. When you decide which volumes to use to fulfill the FICON storage request, map them to open slots in the Requested Volumes section.

   You can map volumes through the following methods. For a size change request, as soon as you select a volume to be modified, DPM highlights the empty slot to which you can move the volume.

   - Drag and drop one or more volumes. For example, use your cursor to drag a predefined volume box from the list, and drop it into an empty slot in the Requested Volumes section. To select multiple volumes, click the check boxes of volumes in the Predefined list, and drag the group over to an empty slot.
   - Direct selection. For example, click the check box in one or more predefined volume boxes in the list, and click anywhere inside an open slot in the Requested Volumes section.
   - Keyboard controls. For example, use keyboard controls to select one or more volumes in the Predefined Volumes list, and move the focus over to the Requested Volumes section to select a target model or volume slot.

   Note that, for volume size changes, you can select **CONFIRM** or **CONFIRM ALL SIZE CHANGES** to have DPM automatically move them to the appropriate model box.

   If you selected more than one volume, DPM fills empty slots in sequence. If you selected too many volumes to fit in the empty slots, DPM fills only the available slots; the excess volumes remain in their original position, and remain as selected volumes. DPM uses the volume number to determine which volumes to place in empty slots, assigning the volumes in numerical order.

   If you change your mind about volume placement, you can use the same methods to move any volume out of a slot in the Requested Volumes section, and back to its original location (the Predefined Volumes list or a model box in the Requested Volumes section).
4. To make sure that you have satisfied the storage request, check the message at the bottom of the Requested Volumes section.

   This message indicates how many requested volumes are unmapped.
5. When you have finished mapping the requested volumes, select **SAVE** to save your changes and return to the Storage Group details page.

Results

DPM updates the fulfillment state, **VOLUMES** tab display, and other elements of the Storage Group details page to reflect your saved changes. DPM also uses an inline message to notify the system administrator who sent the creation or modification request. The message indicates whether any unmapped volumes remain or whether the request was fulfilled.

Modify an FCP or FICON storage group

To modify an FCP or FICON storage group, either select the **Modify Storage Group** action from the Storage Overview page, or open the Storage Group details page and select the **Modify** icon ( ). Either action opens the **Request Storage** task, which is populated with current information about the selected storage group. After you have modified the storage group, DPM automatically generates a request that you

can send to one or more storage administrators. You can edit the generated request to add your own greeting and more details, if necessary.

Before you begin

- For integrated requests and notifications, storage administrators (recipients) must have an email address associated with their user IDs, and Simple Mail Transfer Protocol (SMTP) settings must be defined. Users who send email through the **Request Storage** task do not require an assigned email address because DPM can generate one based on the user name, but the suggested practice is to assign email addresses for senders as well, so recipients know which person sent the email.
  - Email addresses for users are assigned through the **User Management** task.
  - The SMTP server and port settings are defined through the **Monitor System Events** task.

  If your installation does not have SMTP configured, you have the option of downloading or copying the generated request to send to one or more storage administrators.
- To modify a storage group, you can use the default SYSPROG or SERVICE user IDs, or any user IDs that an access administrator has authorized to the **Configure Storage** task through customization controls in the **User Management** task.

Procedure

1. On the **Modify Storage Attributes** page, review the current attributes and make changes, as necessary.

   You cannot change the type of an existing storage group. Depending on the type, you can change the following attributes (with some restrictions).

   Shareability
   Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.
   - If the storage group is currently defined as shared, you can change the number of partitions that share it. The minimum value is either two or the number of partitions that currently have attached the storage group.
   - If the storage group is currently defined as dedicated, you can change it to shared; in this case, the minimum number of partitions is set at the current number of partitions that have attached the storage group.
   - If you want to change a storage group from shared to dedicated, you can do so only when the storage group is attached to one partition, or no partitions.
   - For a FICON storage group, the Shareability attribute is disabled when more than one storage group is using the same logical control unit (LCU).

   Connectivity
   Specifies the number of paths that are available for use by each operating system with access to a FICON or FCP storage group.
   - For an FCP storage group only, you can change the number of paths on this page. Note that decreasing the number of paths can disrupt any running workload that is using this storage group.
   - For a FICON storage group, you cannot change the Connectivity attribute through this page. Instead, you must use the **Configure FICON Connections** task to modify the LCU paths.

   Optimized for 2nd level virtualization
   Specifies the number of additional connections (HBAs) that can be assigned directly to the operating system or its guests for access to a dedicated FCP storage group.

   Although the controls in the **Configure Storage** task allow you to select this attribute only for a dedicated (not shared) FCP storage group, you can optimize 2nd level virtualization for separate

partitions so they can share the same storage disks. For instructions, see “Optimize 2nd level virtualization and share the same FCP disks across partitions” on page 625.

When you select this option, DPM distributes additional HBAs as equally as possible, taking into account both fabrics and adapters that are currently assigned to this storage group. For example, assume that your system configuration has adapters 1001 and 2020 in fabric A, and adapter 4123 in fabric B. For an FCP storage group with a Connectivity attribute setting of 3, DPM assigned one HBA to each of those three adapters when the initial request for the storage group was submitted. If you modify that storage group by specifying 6 additional connections, DPM assigns the additional HBAs equally across the fabrics and adapters that are already in use: two HBAs to adapter 1001, two HBAs to adapter 2020, and two HBAs to adapter 4123.

- If you also modify the current Connectivity setting, DPM assigns new adapters as equally as possible across the currently configured fabrics, and distributes the additional HBAs as equally as possible among either the fabrics or adapters. For example, suppose you modify the Connectivity attribute setting from 3 to 4, and you specify 6 additional HBAs. In this case, DPM assigns two new adapters in fabric A, and two new adapters in fabric B to satisfy the Connectivity attribute change. Then DPM can assign the additional HBAs as described in the following sample configurations:
  - DPM can distribute the HBAs equally between the fabrics, with three HBAs assigned to the adapters in fabric A, and three HBAs assigned to the adapters in fabric B. In this case, each adapter would have one or two HBAs assigned to it.
  - DPM can distribute the HBAs among the four adapters, with two HBAs assigned to each adapter in fabric A (for a total of four), and one HBA to each adapter in fabric B (for a total of two).
- If you decrease the number of additional HBAs, DPM redistributes the remaining additional HBAs, if any, across the currently configured fabrics and adapters. Note that decreasing the number of additional HBAs can disrupt any running workload that is using this storage group.

Select **NEXT** to continue.

2. On the **Modify Volumes** page, review the currently defined volumes. You can add, modify, or delete volumes, as necessary.

   This page contains a table of the existing volumes for the storage group, followed by controls through which you can add more volumes. Volumes of the same size are grouped into one expandable and collapsible row, with the total number of volumes in the group shown to the left of the table row. Use the arrow next to the total number to expand or collapse the table row. The table footer indicates the total size of the storage group, as you add or delete volumes.

   To modify existing volumes

   To modify an existing volume, change any editable attributes in the table row for the volume. Editable attributes vary, depending on the type of storage group. After you modify a volume, a red dot is displayed at the start of the table row for that volume.

   For a volume in an FCP storage group

   You can modify the size, type, or description of a volume in an FCP storage group.

   For a volume in a FICON storage group

   You can modify the model, size, type, or description of a volume in a FICON storage group. However, if a boot volume is attached to an active partition, you cannot change the type.

   To delete existing volumes

   To delete a volume, select the trash can icon at the end of the table row. All volumes to be deleted are listed in another table at the bottom of the **Modify Volumes** page. If you change your mind and want to return the volume to the existing volumes list, you can select the recover icon () at the end of the row in the **Volumes to be deleted** table.

   To add new volumes

   To add a new volume, use the controls under the table of existing volumes. Specify the volume attributes and, optionally, the number of copies, and select the plus sign to add the volume. Volume attributes vary, depending on the type of storage group.

Select **NEXT** to continue.

3. On the **Name** page, modify the name or description, if necessary. Note that the name of the storage group must be unique.

   Select **NEXT** to continue.

4. On the **Confirm** page, review the changes to be made.

   Depending on the changes you requested, the page displays a summary of the storage group attributes, and separate tables that list the volumes to be added, volumes to be modified, and volumes to be deleted. The summary fields and table entries indicate not only the current information, but also the requested change. If necessary, click **EDIT** to change the attributes, name, description, or any volume information.

   Select **NEXT** to continue.

5. On the **Send Modification Request** page, review the automatically generated storage request.
6. Select **SEND** to send the modification request and return to the **Storage Overview** or the **Storage Group** details page (the location from which you initiated the modification request).

   If your installation does not have SMTP configured, you have the option of downloading or copying the generated request to send to one or more storage administrators.

Results

DPM displays an inline message that indicates whether the modification request was sent successfully, and changes the fulfillment state of the modified storage group accordingly.

- The fulfillment status of a FICON storage group changes to Pending only when you have edited or added volumes. If your modification request specified only volumes to be deleted, DPM unmaps those volumes immediately, and the fulfillment state remains Complete.
- The fulfillment status of an FCP storage group changes to Pending for any type of volume modification (add, modify, or delete). Note that, if the FCP storage group is already attached to a partition, the storage group is brought online automatically when the partition is started.

Modify an NVMe storage group

When you select the Modify action on the **Storage Overview** or Storage Group details page for an NVMe storage group, the Storage Group details page opens in Modification mode. Modification mode is indicated by a large blue bar that contains the Modification label, plus the **CANCEL** and **SAVE** buttons.

In this mode, you can add or delete volumes, as well as modify any editable fields directly through the Storage Group details page. Deleting an NVMe SSD volume, or changing its type or device number, can be either prohibited or disruptive, depending on the state of the partition to which the storage group is attached, as described in Table 13 on page 592. All modifications are allowed when the storage group is not attached to a partition.

Table 13. Considerations for modifying an NVMe storage group that is attached to a partition

Modification	**When the storage group is attached to a stopped partition**	**When the storage group is attached to an active partition**
Delete volumes	• You cannot delete the boot volume that is used for the operating system that the partition hosts.* • You can delete any data volume.	• You cannot delete the boot volume that is used for the operating system that the partition hosts.* • You can delete a data volume, but this action is disruptive to any running workloads.
Add volumes	You can add boot or data volumes.	You can add boot or data volumes.

Table 13. Considerations for modifying an NVMe storage group that is attached to a partition (continued)		
Modification	**When the storage group is attached to a stopped partition**	**When the storage group is attached to an active partition**
Change the volume type from Boot to Data	• You cannot delete the boot volume that is used for the operating system that the partition hosts. * • You can delete any data volume.	• You cannot delete the boot volume that is used for the operating system that the partition hosts. * • You can delete any data volume.
Change the volume type from Data to Boot	You can change the type of any volume from Data to Boot.	You can change the type of any volume from Data to Boot.
Change the volume device number	You can change the device number of any volume, without needing to make any manual configuration changes on the operating system after the partition starts.	• You cannot change the device number of the boot volume that is used for the operating system that the partition hosts. • You can delete a data volume, but this action is disruptive to any running workloads.

Table footnote: * Because storage groups can contain more than one boot volume, and a partition can attach more than one storage group that contains multiple boot volumes, you can use the **Partition Details** task to select a different boot volume to replace the one that you want to delete or change. Then you can delete or change the type of the original boot volume.

Change the adapters assigned to an FCP storage group
Use the **FCP adapter assignment** window to review the adapters assigned to a storage group and remove or replace them with other adapters that are available for use by a partition. You can access this window through the **PARTITIONS** tab on the Storage Group details page. Note that reassigning currently configured adapters can disrupt any running workload that is using this storage group.

The **FCP adapter assignment** window displays two tables: Assigned Adapters and Adapter Candidates. Each table contains the same columns and has a footer that indicates the total number of adapters in the table. You might need to scroll to see all table entries, or use the Search field to filter the table entries. The search string applies to both tables. Note that any incomplete adapters are indicated by an incomplete icon ( ).

If an FCP adapter is configured while the storage group is attached to an active partition, DPM cannot detect and list the new adapter as available for use by any partition. To make sure that you can choose from a complete list of available adapters, stop all active partitions to which the storage group is attached, and select the **Connection Report** icon to start a background check of the available connections for this storage group.

If you need to assign new adapters, the Assigned Adapters table contains a placeholder row for each required adapter. To fill those placeholders, use one of the following methods.

- Use the **Automatically assign** icon ( ) to have DPM automatically select redundant adapters across all fabrics. DPM selects the adapters with the lowest allocation percentage and the fastest card type.
- Use the buttons in the Action table column to manually change adapter assignments, one adapter at a time. The suggested practice is to assign at least two adapters from each fabric for redundancy.
  1. In the Assigned Adapters table, select **UNASSIGN** to remove individual adapters.
  2. In the Adapter Candidates table, select **ASSIGN** to assign different adapters. Newly assigned adapters are indicated by a blue dot next to the table row in the Assigned Adapters table.

If you need to change all of the currently assigned adapters, use the **Unassign all** icon ( ) to empty the Assigned Adapters table. Then use either the **Automatically assign** icon or the Action buttons to assign new adapters.

When you have finished, select **SAVE** to return to the Storage Group details page.

The following list describes the columns that are displayed in both of the tables on the **FCP adapter assignment** window.

Adapter Name
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

Adapter ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

Location
Specifies the physical location of the adapter in the I/O drawer of the system.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Allocation
Indicates the percentage of host bus adapters (HBAs) that are currently allocated to this adapter, shown in a bar graph and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. If the percentage is high (for example, 90%), consider assigning a different adapter.

Action
Contains one of the following buttons.

- In the Assigned Adapters table, **UNASSIGN** removes the adapter in the table row and moves the table row into the Adapter Candidates table.
- In the Adapter Candidates table, **ASSIGN** assigns the adapter in the table row and moves the table row into the Assigned Adapters table.

Connection Report for an FCP Storage Group
Use the **Connection Report** to view the system and storage connections (adapters, volumes, WWPNs, and so on) for an FCP storage group. You can also download the report contents in spreadsheet format. The report includes a 12-hour timestamp in the format `dd.mm.yyyy hh.mm` with AM or PM indicated. You can access the **Connection Report** page from the Actions list in the table entry for storage group on the **Storage Overview** page, or through the connections icon ( ) on the Storage Group details page.

On the **Connection Report** page, select the **Update report** icon ( ) to start a new background check of the available connections for the storage group. When the check is complete, the Report Date field is updated.

- For all FCP storage groups, DPM automatically runs a background check once every 24 hours.
- The **Update report** icon label changes to **Restart update** when a background check is in progress. If you select **Restart update**, DPM cancels the in-progress check and starts a new one.
- DPM stops any in-progress check under the following conditions.
  - When a user detaches this storage group from a partition.
  - When a user starts a partition to which this storage group is attached.
  - When a user reassigns adapters for this storage group.

  After the detachment, start, or reassignment process completes, DPM automatically starts a new background check.

The **Connection Report** page display contains three sections: System, SAN, and Storage. The sections are aligned horizontally, similar to columns in a row in table format. Each section contains an expandable box that displays specific information that is associated with one fabric in the storage configuration.

Each section heading has an icon that indicates the current status of connections.

- No errors were found:
- Errors exist:

To view the related information, expand each box in the row.

- The System section lists storage adapters for the fabric.
- The SAN section lists zoned worldwide port numbers (WWPNs) for the fabric.
- The Storage section lists the WWPNs that are mapped to a storage subsystem.

Each box has a heading, a control for expanding or collapsing the list, and total count of configured and sensed storage adapters or WWPNs. If errors exist, the error icon is displayed next to the box heading, and next to items in the expanded list.

The following list describes the contents of each expanded section.

System

The System section displays a list of storage adapters for each SAN fabric associated with the storage group. Each list has a heading (Storage Adapters) and a label that includes adapter counts in x/y format, where:

- x is the number of enabled adapters that sensed WWPNs in the fabric
- y is the requested number of paths divided by the number of sensed fabrics with enabled WWPNs

Each list contains the name of each sensed storage adapter. The name is the default name that DPM assigns, in the form *adapter_type adapter_ID partial_location*; for example, `FCP 0171Z22B-11`.

If errors exist for the system adapters, the adapters associated with an error are displayed at the top of the list. Errors are indicated when the number of sensed adapters is less than the total number of adapters that are defined for the fabric.

- The list indicates an unnamed missing adapter when the storage group is in Pending state and is not attached to an active partition.
- The list identifies the missing adapter by name when the storage group was successfully fulfilled and attached to a partition.

SAN

The SAN section displays a list of WWPNs for each SAN fabric associated with the storage group. Each list contains a heading (Fabric: *fabric_name*) and a label that includes WWPN counts in x/y format, where:

- x is the number of enabled WWPNs that were sensed by storage adapters
- y is the number of WWPNs that need to be zoned in all fabrics

The list contains both sensed and unsensed WWPNs for each fabric.

If errors exist for the WWPNs, the WWPNs associated with an error are displayed at the top of the list. Errors are indicated when the number of sensed WWPNs is less than the total number of zoned WWPNs, even if the connections are good but only some of the sensed WWPNs are being used.

Storage

The Storage section displays a list of WWPNs that are mapped to volumes. Each list contains a heading (Subsystem: *subsystem_name*) and a label that includes WWPN counts in x/y format, where:

- x is the number of WWPNs that sensed the requested volumes
- y is the number of WWPNs that sensed all of the sensed volumes

The list contains the mapped WWPNs, a count of sensed and requested volumes and, for error conditions only, a message in the VOLUME column. If errors exist for the WWPNs, the WWPNs associated with an error are displayed at the top of the list.

- If specific WWPNs were not sensed, the volume count for those WWPNs is zero.
- If a sensed WWPN is mapped to more volumes than the expected number of volumes, the volume count indicates the number of additional volumes. This WWPN is mapped incorrectly.
- If a sensed WWPN is mapped to different volumes than expected, the volume count indicates the number of different volumes. This WWPN is mapped incorrectly.

Connection Report for a FICON Storage Group

Use the **Connection Report** to view the logical paths that are in use for a FICON storage group. You can also download the report contents in spreadsheet format. You can access the **Connection Report** page from the Actions list in the table entry for storage group on the **Storage Overview** page, or through the connections icon () on the Storage Group details page.

The **Connection Report** page displays a table that contains a row for each logical control unit (LCU) for all storage subsystems that the storage group uses. The following list describes the table columns.

STORAGE SUBSYSTEM
Specifies the name of a storage subsystem that contains physical storage used to fulfill the requirements of this storage group.

LCU NO.
Specifies the two-digit hexadecimal number of an LCU that is defined for this storage subsystem.

PATHS
Specifies the number of logical paths defined for the LCU.

SWITCHES (PORTS)
Specifies the total number of outgoing switches to which the storage subsystem is connected, and the total number of connected ports for these switches. For example, if the storage subsystem is connected to two switches, each of which have four connected ports, the value shown in this column is 2 (8). This column contains a dash (-) if your environment uses point-to-point connections (that is, the storage subsystem is directly connected to the system, rather than to a switch).

SWITCHES
Specifies the total number of entry switches to which the DPM-enabled system is connected. This column contains a dash (-) if your environment uses point-to-point connections.

ADAPTERS
Specifies the total number of adapters used for this LCU.

You can expand each table row by selecting the **Details** link in the rightmost table column. The expanded section contains another table of information about the logical paths from the LCU to the DPM-enabled system. The following list describes the table columns. The expanded section also contains an **EDIT** link through which you can open the **Configure FICON Connections** task to define or modify LCUs and logical paths. For more information, see “Configure FICON Connections” on page 614.

SWITCH ID
Specifies the two-digit identifier of the outgoing switch to which the storage subsystem is connected. This column contains a dash (-) if your environment uses point-to-point connections.

PORT NO.
Specifies the two-digit hexadecimal number of the switch port that is used by this logical path.

SWITCH ID
Specifies the two-digit identifier of the entry switch to which the DPM-enabled system is connected. This column contains a dash (-) if your environment uses point-to-point connections, or if only one switch is on the path from the storage subsystem to the system (that is, your environment does not make use of cascaded switches).

ADAPTER ID
Specifies the four-character physical channel path identifier (PCHID) of the target adapter on the DPM-enabled system.

LOCATION
Specifies the location of the adapter in the I/O cage of the DPM-enabled system.

Tape Link details
Use the Tape Link details page to view or modify information about a specific tape link on a DPM-enabled system. The Tape Link details page consists of a summary, a set of action icons, and tabbed sections that you can select to change the lower portion of the page display. You also can use this page to delete a tape link, or to resend a zoning request.

For specific fulfillment states, note that various summary fields, tabbed sections, environment elements, and table entries have a pending, incomplete, warning, or error icon to alert you to details that might need your attention or action.

The heading on this page is the tape link name, which you can edit. If you modify the name, specify a value that is 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. The name must uniquely distinguish this tape link from all other tape links that are defined for this system.

You can also edit the description of the tape link. To modify any tape link attributes other than the name or description, select the **Modify** icon to display the Tape Link details page in Modification mode. Modification mode is indicated by a large blue bar that contains the Modification label, plus the **CANCEL** and **SAVE** buttons. For more information about this mode and the modifications that you can make, see “Modify an FCP tape link” on page 606.

For more information about the elements of the Tape Link details page, see the following topics.

- “Summary section of the Tape Link details page” on page 597
- “Action icons on the Tape Link details page” on page 598
- “Tabs on the Tape Link details page” on page 599

Summary section of the Tape Link details page

The summary fields display the attributes and current state of the tape link. Note that the following icons indicate details that might require your attention or action: pending icons (or), and incomplete icons ( ).

Type of tape link
Specifies the type of tape link: FCP.

Connectivity (Number of paths)
Specifies the number of physical system adapters that provide access to the tape library. These adapters are shared equally by any partitions that use this tape link.

Shareability
Specifies whether the tape link can be shared among partitions, or whether it is dedicated to only one partition. If the tape link can be shared, this field indicates how many partitions are using it currently, as well as the maximum number of partitions that can use it.

Description
Specifies the user-supplied description for this tape link. You can edit this description.

Fulfillment state
Specifies the current state of the tape link. DPM runs a background check of storage resources for FCP tape links and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours). In these background checks, DPM tries to detect the tape drives (logical units or LUNs) for the WWPNs that are assigned to this tape link. Users can manually start a background check by selecting the **Update tape link environment** icon ( ) on the **ENVIRONMENT** tab.

The following list provides a summary of each fulfillment state. For more details about fulfillment states and possible actions that you can take to correct errors or mismatches, see Table 14 on page 601.

Complete
All of the storage resources listed in a create or modify request are available, properly configured and zoned, and DPM detects only those resources.

Incomplete
One or more storage resources for the tape link are marked as incomplete because the resource is missing, or in an error or degraded condition. Because DPM periodically checks the availability of storage adapters, switches, and tape libraries that are in use for a tape link, resources that were functioning properly can become incomplete.

Pending
One or more requested storage resources are not yet available or zoned correctly, or the tape link is not yet attached to all partitions that were specified in the original create request or a modify request.

Pending with mismatches
DPM detects system adapters that do not match the original create request or a modify request. Either the number of system adapters does not match the number of connecting paths, or the detected adapters do not match specific adapters that were assigned to the tape link.

Tape library
Specifies the serial number of the tape library that partitions can access through this tape link. If the value is "Not specified", the storage administrator has not yet selected a tape library for this tape link.

Action icons on the Tape Link details page

The actions that are displayed depend on the fulfillment state of the tape link and the permissions that are associated with your user ID. Note that some actions produce an automatically generated request to send to a storage administrator. For integrated requests and notifications, storage administrators (recipients) must have an email address associated with their user IDs, and Simple Mail Transfer Protocol (SMTP) settings must be defined. If email support is not configured, users have the option of downloading storage requests to send them through other methods.

Resend Request
This action opens a window containing an automatically generated request that includes zoning instructions for incomplete or pending storage resources. You can select this action only when the tape link is in one of the following fulfillment states: Incomplete, Pending, or Pending with mismatches. If the tape link state is Incomplete because of adapter errors, or the state is Pending because tape link attachment operations are in progress, this action is disabled until the errors are resolved or the attachment operations are complete.

Modify
This action changes the page display to the **Tape Link details** page in modification mode. Modification mode is indicated by a large blue bar that contains the Modification label, plus the **CANCEL** and **SAVE** buttons. In this mode, the "Type of tape link" field is not displayed in the summary section, because the field value cannot change.

Use **Modify** whenever you need to change tape link attributes other than the name and description. In Modification mode, you can make changes on the **ADAPTERS** and **PARTITIONS** tabs only.

- If you are viewing the **ADAPTERS** tab when you select **Modify**, Modification mode opens to the **ADAPTERS** tab display.
- If you are viewing the **ENVIRONMENT**, **PARTITIONS**, **HISTORY**, or **WWPNS** tab when you select **Modify**, Modification mode opens to the **PARTITIONS** tab display.

For more details about Modification mode and the changes you can make to the tape link, see “Modify an FCP tape link” on page 606.

Delete

This action opens a window containing an automatically generated request to delete the selected tape link, along with attached instructions for deleting the tape link from the SAN configuration. You can delete a tape link that is in any fulfillment state; however, the **Delete** action is disabled if the tape link is attached to any active partitions, or when any asynchronous attachment or detachment operations are in progress. If the tape link is attached to any stopped partitions, you can either cancel or continue with the delete request through a confirmation dialog.

During the delete process, DPM detaches the tape link from each partition before deleting the tape link itself. Depending on the number of partitions, the delete request might take some time, during which one or more stopped partitions might be started. In this case, the delete operation is canceled, but you receive an error dialog that lists the partitions to which the tape link remains attached. Through this dialog, you can restart the delete operation.

Tabs on the Tape Link details page

The tabbed sections provide more details related to the tape link. Note that the following icons indicate details that might require your attention or action: pending icons (or), and incomplete icons ( ).

When you select a tab, the content of the Tape Link details page changes. For more details about each tab, see the following topics.

- “ENVIRONMENT” on page 599
- “PARTITIONS” on page 603
- “ADAPTERS” on page 604
- “WWPNS” on page 605
- “HISTORY” on page 605

ENVIRONMENT

The **ENVIRONMENT** tab displays the current zoning and other information about the system adapters, SAN fabrics and switches, the tape library and tape drives for an FCP tape link. You can update (or refresh) the display, which includes a 24-hour timestamp for the last update, in the format `yyyy.mm.dd hh:mm:ss`. You also can download a snapshot of the **ENVIRONMENT** tab contents.

DPM runs a background check of storage resources for FCP tape links and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours). DPM automatically refreshes the content of the **ENVIRONMENT** tab after each background check.

The **ENVIRONMENT** tab display contains three sections, System, SAN, and Tape subsystem, as shown in Figure 36 on page 600. Within each section, a summary is displayed under the heading, followed by connected boxes that represent the storage resources. If you hover your cursor over a system adapter or SAN fabric, the connections are highlighted with a blue background.

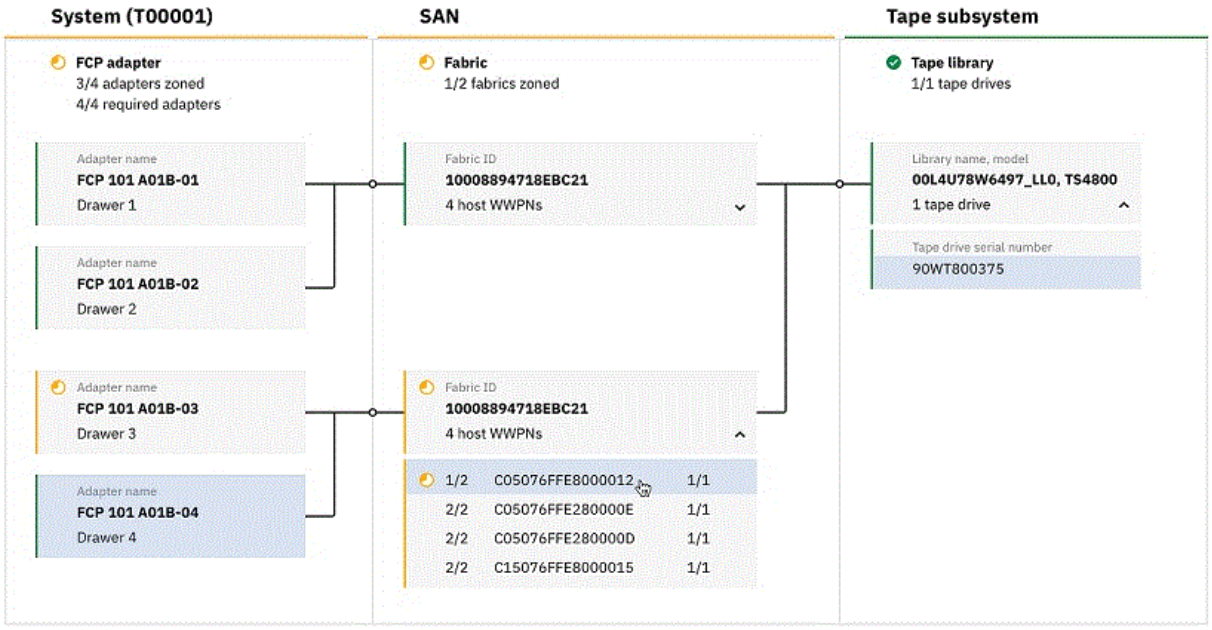


Figure 36. Sample ENVIRONMENT tab display for a tape link

Icons and connecting lines indicate the current status of tape link connections between the system adapters, SAN fabrics, and the tape library. For example, in Figure 36 on page 600:

- The System and SAN summary sections are marked as Pending ( ) because one adapter is not completely zoned.
- The Tape library section is marked as Complete ( ) because three of the four required adapters are properly zoned and can reach the tape library. A tape library is considered complete when at least one required adapter can reach it.

For more information about the display when DPM detects issues with tape link connections, see Table 14 on page 601.

The following list describes the content of each section in more detail.

System (*system name*)

The System section includes the system name and model, two summary counts of the system adapters, followed by a box for each FCP adapter that is assigned to the tape link through the original create request (or a later modification). Each box contains the system adapter name and the name of the drawer in which the adapter is installed.

- One summary count indicates how many of the required adapters are zoned in the SAN fabric. The number of required adapters is the same as the current Connectivity value (the number of connecting paths). For example, if the number of required adapters for the tape link is 4, but DPM detects the corresponding host WWPNs in the SAN fabric for only one adapter, the count is displayed as `1/4 adapters zoned`. In this example, the boxes for the remaining three adapters are marked with a Pending status icon, and the connection lines from the adapter box to the SAN fabric and the tape library are dashed orange lines because the connection is expected but not available yet.
- The second summary count indicates how many adapters DPM detected for this tape link and its tape library, along with the number of required adapters. For example:
  - If the number of required adapters for the tape link is 4, but DPM detects that one of these adapters is now in an error state, the count is displayed as `3/4 required adapters`. The box for the adapter in error is marked with an Incomplete status icon, and the connection line from the adapter box to the SAN fabric is solid red because the connection was in place previously, but is not available now.

– If the number of required adapters for the tape link is 4, but DPM detects that another adapter is connected to the tape library for this tape link, the count is displayed as `5/4 required adapters`. The box for the extra adapter is marked with the Pending with mismatches icon, and the connection lines from the adapter box to the SAN fabric and the tape library are solid black, because this unrequested adapter is completely zoned and can reach the tape library.

SAN

The SAN section includes a summary count of fabrics, followed by a box for each fabric that is assigned to the tape link through the original create request (or a later modification). Each box contains the fabric ID and a count of the required host WWPNs for the system adapters. The summary count displays the number of completely zoned fabrics and the number of currently available fabrics. For example, in Figure 36 on page 600, the summary count is `1/2 fabrics zoned` because only one of the two available fabrics is completely zoned.

You can expand each fabric box display to show the host WWPNs and counts that indicate their zoning status. The count on the left indicates whether each required host WWPN is zoned correctly with the system adapter ports that are connected to the fabric. For example, if two system adapters are connected to the fabric but the host WWPN is correctly zoned with only one adapter, the count is displayed as `1/2`; the connection is pending until the count is `2/2`. Similarly, the count on the right indicates whether each required host WWPN is zoned correctly with the total number of target WWPNs for tape drives in the tape library. Each tape drive contains two ports so two target WWPNs must be zoned. For example, if the storage administrator has selected six tape drives to be accessed through this tape link, each host WWPN must be zoned with the twelve target WWPNs. If a host WWPN is zoned with only two of the target WWPNs, the count is `2/12`.

Tape subsystem

This section includes a summary count of tape drives in the tape library, followed by a box for the tape library. The box contains the tape library name (serial number) and model, and the number of tape drives in the tape library. You can expand the box to display a box for each tape drive, along with its serial number.

- If the original create request for the tape link did not specify a particular tape library, the tape library name is not available until the storage administrator selects a tape library, configures at least one tape drive as a control path, and zones at least one target WWPN. Also, the summary count of tape drives is 0 until the storage administrator determines the tape drives that can partitions can access through the tape link, and starts zoning the host and target WWPNs.
- If DPM detects more than one tape library, the fulfillment state of the tape link is Incomplete. The tape link environment can include only one tape library. For tape libraries that were detected but not specified in the original create request for the tape link, the details shown are derived from the zoning that is currently in place for the tape library.

The **ENVIRONMENT** tab display varies depending on the current fulfillment state of the tape link. As shown in Figure 36 on page 600, different sections of the ENVIRONMENT tab can have elements in different states. The state of any resource directly influences the overall fulfillment state of the tape link itself. Table 14 on page 601 lists the fulfillment states, describes the table display, and provides possible actions you might take to resolve any issues. For actions that suggest modifying a tape link, see more information in “Modify an FCP tape link” on page 606.

Table 14. Interpreting the ENVIRONMENT tab display for different tape link fulfillment states

Fulfillment state	ENVIRONMENT tab display	Possible action
Complete All of the storage resources listed in a create or modify request are available, properly configured and zoned, and DPM detects only those resources.	The display contains complete icons (✓) next to the three section headings, and connections between the elements are shown as solid black lines.	None.

Table 14. Interpreting the ENVIRONMENT tab display for different tape link fulfillment states (continued)

Fulfillment state	ENVIRONMENT tab display	Possible action
Incomplete The following conditions cause the fulfillment state for a tape link to be Incomplete. • One or more system adapters are unreadable, in an error state, or no longer detected. • An error occurred, or an unrequested reconfiguration of storage resources in the SAN affects the requested resources. • The storage administrator has not configured a tape drive as the control path to the requested tape library. • The original tape link request included a specific library but a different library is detected, or more than one tape library is detected, through the current zoning. The tape link environment can include only one tape library. • The tape library can no longer be reached due to an error with cables or with the tape library itself.	The display contains incomplete icons () next to any section heading or individual elements (adapters, fabrics, or tape library) for which DPM detected an error. Also, connections between elements with errors are shown as solid red lines, with a slash (/) indicating where the connection is broken because of the error. If the errors are detected for system adapters or host WWPNs, an error icon is displayed next to the **ADAPTERS** or **WWPNS** tabs.	Hover your cursor over any incomplete icon to view more information about the specific error condition. • If an adapter is in error, go to the **ADAPTERS** tab and select the adapter name to open the Adapter Details page in the **Manage Adapters** task. The adapter details can determine how you can resolve the error. The simplest fix is replacing the adapter in error with a different available adapter, which you can do by selecting **Modify**. • If the errors are due to zoning in the SAN fabrics, cable or optic errors, multiple tape libraries, or errors with the tape library itself, select **Resend request** to notify one or more storage administrators so they can take the appropriate action.

Table 14. Interpreting the ENVIRONMENT tab display for different tape link fulfillment states (continued)

Fulfillment state	ENVIRONMENT tab display	Possible action
Pending One or more requested storage resources are not yet available or zoned correctly, or the tape link is not yet attached to all partitions that were specified in the original create request or a modify request. When the fulfillment state is Pending, DPM does not perform any dynamic I/O operations for partitions to which the tape link is attached.	The display contains pending icons ( ) next to any section heading or individual elements (adapters, fabrics, or tape library) when connections are expected but not yet available because of pending zoning or configuration tasks. • If zoning tasks are pending for system adapters or host WWPNs, a pending icon is displayed next to the **ADAPTERS** or **WWPNS** tab. • If the create or modify request included partitions to which the tape link is to be attached, and one or more asynchronous attachment processes are still in progress, a pending icon is displayed next to the **PARTITIONS** tab.	The Pending fulfillment state is generally a temporary state, but some tasks require time to complete. To determine whether those tasks are progressing, you can periodically select the **Update environment** button to refresh the tab display, and note the changes, if any. • If zoning tasks are pending for a longer time than you expect, you can select **Resend request** to remind one or more storage administrators of the pending tasks. • If tape link attachment operations are in progress, note that the attachment process might take some time, depending on the status and number of the selected partitions. The attachment to stopped partitions is relatively quick, but attachment to active partitions can take longer because these partitions might be busy. If further investigation seems necessary, go to the **PARTITIONS** tab, view the partitions that are marked as pending, and select the partition name to open the **Partition Details** task.
Pending with mismatches DPM detects system adapters that do not match the original create request or a modify request. Either the number of system adapters does not match the number of connecting paths, or the detected adapters do not match specific adapters that were assigned to the tape link. When the fulfillment state is Pending with mismatches, DPM does not perform any dynamic I/O operations for partitions to which the tape link is attached.	The display contains pending with mismatches icons ( ) next to the Systems section heading, on one or more adapters in this section, and on the **ADAPTERS** tab. Also, connections between the mismatched system adapters, the SAN fabrics, and the tape library are shown as solid black lines.	You must resolve all of the mismatched adapters before you can make any other modifications to the tape link. You can resolve mismatches by modifying the assigned adapters. To do so, select **Resolve adapter mismatches** or the **Modify** icon for the tape link to change the page display to Modification mode.

PARTITIONS

The **PARTITIONS** tab lists the partitions to which the tape link is attached in table format. If the tape link has not been attached yet to one of the listed partitions, the **PARTITIONS** tab has a pending icon ( ), and another pending icon marks the table row for the specific partition. To attach the tape link to more partitions, or to detach the tape link from one or more of the listed partitions, select the **Modify** icon for the tape link to change the page display to Modification mode. For more details about

partition modifications, see “Modify the partition maximum, add or delete selected partitions, or edit HBA device numbers” on page 609.

The following list describes the column values in the Partitions table.

NAME
Specifies the name of the partition. The name is a hyperlink through which you can open the **Partition Details** task.

STATUS
Specifies the operating status of the partition. For descriptions of possible status values, open the **Partition Details** task and view the online help for the Status section.

DESCRIPTION
The user-supplied description, if any, of the partition.

Each row in the Partitions table can be expanded to show details about the host bus adapters (HBAs) that the partition is using to access storage. If you want to modify the HBA device number, select the **Modify** icon for the tape link to change the page display to Modification mode.

- If an adapter that is assigned to an HBA becomes incomplete, the table entry for the HBA and the table entry for the partition are both marked with an incomplete icon ( ). If one or more adapters are incomplete, the fulfillment status of the tape link is Incomplete.
- If the tape link is in a pending fulfillment state, only the HBA name and device number are displayed in the Host Bus Adapters table.

The following list describes the column values in the Host Bus Adapters table.

NAME
Specifies the name of the HBA.

DEVICE NUMBER
Specifies the hexadecimal device number of the HBA.

WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a tape drive in the tape library.

FABRIC ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

ADAPTER ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

ASSIGNED ADAPTER
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

ADAPTERS

The **ADAPTERS** tab lists the system adapters that are either specified through the original create request for the tape link, or connected to the tape library for this tape link.

- If all adapters are not yet assigned, the **ADAPTERS** tab has a pending icon ( ) next to it, and the table entry for that adapter is marked with the same icon. The total at the foot of the Adapters table lists how many adapters are assigned to the tape link.
- If the adapters that are zoned do not match the adapters that were specified in the original create request, the **ADAPTERS** tab has a pending with mismatches icon ( ) and the tab display includes a table of Unrequested and zoned adapters, all of which are marked with the same pending with mismatches icon.

  Note: You must resolve all of the mismatched adapters before you can make any other modifications to the tape link. You can resolve mismatches by modifying the assigned adapters. To do so, select the **Modify** icon for the tape link to change the page display to Modification mode.

- If an existing adapter becomes incomplete, the **ADAPTERS** tab has an incomplete icon ( ) next to it, and the table entry for that adapter is marked with the same icon. You can replace such adapters through Modification mode.

For more details about adapter modifications, see "Modify the number of connecting paths and add, replace, or delete system adapters" on page 607.

The tables that can be displayed on the **ADAPTERS** tab contain the following information.

NAME
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

ADAPTER ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

TYPE
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

LOCATION
Specifies the physical location of the adapter in the I/O drawer of the system.

ALLOCATION
Indicates the percentage of host bus adapters (HBAs) that are currently allocated to this adapter, shown in a bar graph and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions.

WWPNS
The **WWPNS** tab lists the host worldwide port numbers (WWPNs) that are available for use. The tab display contains two tables: one table that lists each host WWPN that is in use by a partition, and one table that lists unused host WWPNs. The following list describes the column values that are displayed in each table.

WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a tape drive in the tape library.

STATE OF WWPN
Indicates the current state of the WWPN.

Validated
DPM detected the WWPN and found the logical unit number (LUN) that represents the tape drive that is configured in the fabric (switch).

Not validated
The storage administrator has not activated this WWPN.

Incomplete
DPM could not detect this WWPN on all required fabrics and the tape library. Incomplete WWPNs are marked with an incomplete icon ( ).

NAME (HBA)
Specifies the name of the host bus adapter (HBA) that provides a partition with access to external storage area networks (SANs) and devices that are connected to a system. This column is displayed only in the table of WWPNs that are in use.

PARTITION
Specifies the name of the partition that is using the WWPN. This column is displayed only in the table of WWPNs that are in use.

HISTORY
The **HISTORY** tab lists the actions that users have taken for this tape link. The most recent action is listed at the top of the History table. Information in the ACTION column not only briefly describes the activity, but also preserves details such as requests that were sent to storage administrators for fulfillment. If the tape link is deleted, you can access the history details only for the next 30 days, by using the HMC Web Services API for DPM.

The History table contains the following columns.

TIME
Specifies the date and time when the action was taken, in the format `yyyy-mm-dd hh:mm:ss`.

USER
Specifies the user ID of the person who initiated the action. If DPM initiated the action, "no user" is displayed in this column.

ACTION
Describes the action that was performed. Note that some words in the description are selectable links through which you can view details about the specific action. For example, for a modification request, you can use the link to open a new window that contains the updates that the user made, along with a link to download the email that DPM generated for that request. Depending on the action that was performed, the associated details can include instructions for additional user action; for example, changing a device number can require issuing a configuration command on the operating system. In these cases, a red dot is displayed next to the table row until a user selects the link to view the details.

FULFILLMENT STATE
Specifies the fulfillment state that resulted from the action.

Modify an FCP tape link
When you select **Modify** on the **Storage Overview** or Tape Link details page for an FCP tape link, the Tape Link details page opens in Modification mode. Modification mode is indicated by a large blue bar that contains the Modification label, plus the **CANCEL** and **SAVE** buttons. When you save your changes, the fulfillment state of the tape link changes to Pending, and DPM automatically generates a request that you can send to one or more storage administrators; this email includes zoning instructions for the storage administrators to follow to fulfill your request.

Use **Modify** whenever you need to change tape link attributes other than the name and description. In Modification mode, you can make changes on the **ADAPTERS** and **PARTITIONS** tabs only.

Notes:

- If the fulfillment state of the tape link is Pending with mismatches, you must resolve these mismatches before you can make any other modifications to the tape link.
- If the fulfillment state of the tape link is Pending because one or more asynchronous tape link attachment processes are still in progress, you can modify partitions but you cannot switch to the **ADAPTERS** tab until the attachment processes complete.

In Modification mode:

- The "Type of tape link" field is not displayed in the summary section, because the field value cannot change.
- Some fields in the summary section indicate not only the current tape link information, but also the changes you are making on the **ADAPTERS** or **PARTITIONS** tabs. For example, if the tape link currently has 2 connecting paths and a modification request will add two more paths, the Connectivity field in the summary lists both the current number of paths and the future number: `2 -> 4`
- The **Undo** and **Redo** buttons are available for you to revoke or restore changes on either tab, in the order that you made the changes.

For more information about the **ADAPTERS** or **PARTITIONS** tabs in Modification mode, see the following topics:

- “Modify the number of connecting paths and add, replace, or delete system adapters” on page 607
- “Modify the partition maximum, add or delete selected partitions, or edit HBA device numbers” on page 609

Modify the number of connecting paths and add, replace, or delete system adapters

Through the **ADAPTERS** tab in Modification mode, you can add or delete adapters only by changing the number of connecting paths. Remember that changes to this connectivity setting have an impact on bandwidth, performance, and redundancy. You also can replace currently assigned adapters with other available adapters, and resolve adapter mismatches when the fulfillment state of the tape link is Pending with mismatches.

Note: Deleting or replacing adapters can be disruptive when the tape link is attached to one or more active partitions. Inline messages and other visual cues indicate whether your changes might cause a problem.

Modify the number of connecting paths

Changes that you make through the **Number of connecting paths** slider, text entry field, or spin button are reflected in the adapters table. The changes vary, depending on whether you are decreasing the number of paths, increasing the number of paths, or both, during a single modification session.

Only decrease the number of connecting paths

When you decrease the number of paths, DPM automatically grays out the appropriate number of adapter rows from the table, selecting the adapters to remove in the following order.

1. Adapters to be selected by the storage administrator (placeholder rows) that DPM assigned or that you selected to replace assigned adapters.
2. Unzoned adapters that are already assigned to the tape link.
3. Zoned ("Matching") adapters that are already assigned to the tape link.
4. Unzoned adapters that you selected to replace assigned adapters.
5. Zoned ("Matching") adapters that you selected to replace assigned adapters.

Each adapter that DPM selects for removal is marked with a recover icon () to the right of the table row. If you prefer to remove different adapters, select the recover icon for any marked adapter, and the table display changes to show each adapter row with a trash can icon, so you can select which assigned adapters to delete. An inline message tells you how many adapters you need to select for deletion. When you click the trash can icon, DPM marks the adapter to be removed with one of the following marks, to the left of the table row:

- A red dot to indicate the adapter that was most recently selected for removal.
- A warning icon (), when this change is disruptive to active partitions that are using the tape link.

Only increase the number of connecting paths

When you increase the number of connecting paths, DPM adjusts the Adapters table by adding the corresponding number of table rows; for example, if you increase the number of paths by 2, the table contains two new table rows.

- DPM preselects adapters that are connected to the tape library already, and that provide optimal redundancy. Optimal redundancy for adapters is based on the following factors, which are listed in priority order from highest to lowest: on the location in the I/O drawers, on the drawer domain, on the current allocation, and on the connection to SAN fabrics.
- If the total number of preselected adapters is less than the number of connecting paths that you selected, placeholder rows represent the remaining number of adapters for the storage administrator to assign. If you do not supply a specific adapter for a placeholder row, the storage administrator selects the adapter for you, as part of fulfilling your modification request.

If more adapters are available for selection, you can select the exchange icon () to replace a preselected adapter.

Increase and decrease the number of paths in a single modification session

If you increase and decrease the number of connecting paths within a single modification session, DPM automatically adds or removes Adapter table rows in a specific order.

- When you increase the number of connecting paths, DPM automatically adds the appropriate number of adapters, preselecting them in the following order.
  1. Adapters that you already deleted in this modification session, if any.
  2. Zoned ("Matching") adapters that were not assigned previously to this tape link.
  3. Adapters that were previously assigned to this tape link, but were replaced through the exchange dialog.
  4. Adapters to be selected by the storage administrator (placeholder rows).
- When you decrease the number of connecting paths, DPM automatically removes the appropriate number of adapter rows from the table, selecting the adapters to remove in the following order.
  1. Adapters to be selected by the storage administrator (placeholder rows) if you increased the paths in this modification session.
  2. Zoned ("Matching") adapters that DPM preselected if you increased the paths in this modification session.
  3. Remaining placeholder rows, if any, including placeholder rows that DPM assigned or that you selected to replace assigned adapters.
  4. Unzoned adapters that are already assigned to the tape link.
  5. Zoned ("Matching") adapters that are already assigned to the tape link.
  6. Unzoned adapters that you selected to replace assigned adapters.
  7. Zoned ("Matching") adapters that you selected to replace assigned adapters.

Replace assigned adapters

To replace an assigned adapter (or add an adapter to a placeholder row), complete the following steps. For the best results, try to assign adapters that reside in different system I/O drawers and in different domains; that are not on the same card; and that are connected to different fabrics. Inline messages provide warnings if the selected adapters do not meet these criteria.

1. Select the exchange icon (). A dialog opens and displays information about the assigned adapter or placeholder row that you want to exchange, and available adapters to replace it.
2. If you want a storage administrator to select an adapter for you, select **Adapter to be assigned by the storage administrator** under the Available adapters heading. Otherwise, use the information in the Available adapters table to select a replacement adapter. Note that any adapter with an existing error condition is marked with an incomplete icon (). The suggested practice is to avoid selecting such adapters.

   MATCH
   If an adapter is already connected to the tape library that you are using for this tape link, this column contains the label "Matching" in the adapter row. Otherwise, this column is empty.

   NAME
   Specifies the name of the FCP adapter. DPM assigns a default adapter name in the form *adapter_type pchid partial_location*, which can help you determine whether you are selecting adapters that, for optimal redundancy, reside in different drawers and different domains. For example, in the sample default name `FCP 0171 Z22B-11`:

   - FCP is the type.
   - `0171` is the physical channel path identifier (PCHID).
   - `Z22B` is the plug location of the I/O drawer, with the first letter denoting the frame in which the drawer resides.
   - `11` is the slot in the drawer in which the adapter is plugged.

   FABRIC ID
   Displays the worldwide name (WWN) of the uplink Fibre Channel switch. For optimal redundancy, use this value to select adapters that are connected to different fabrics.

ADAPTER ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

TYPE
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names

LOCATION
Specifies the physical location of the adapter in the I/O drawer of the system.

ALLOCATION
Indicates the percentage of host bus adapters (HBAs) that are currently allocated to this adapter, shown in a bar graph and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. If the percentage is high (for example, 90%), consider assigning a different adapter.

3. Select **Replace** to save your selection and close the dialog window. On the **ADAPTERS** tab, the table row for the adapter that you just selected is marked with one of the following icons.
   - A pending icon ( ) indicates that zoning is required before the fulfillment state of the tape link can change to Complete.
   - An incomplete icon ( ) indicates an existing error condition for the adapter. The suggested practice is to replace such an adapters with different ones.
   - A warning icon ( ), when this change is disruptive to active partitions that are using the tape link.
4. Repeat these steps, as necessary, to replace any more assigned adapters.

Resolve pending mismatches
When the fulfillment state of the tape link is Pending with mismatches, the **ADAPTERS** tab display contains three separate sections through which you can change the number of connecting paths, view and delete unrequested and zoned adapters, or view and replace assigned adapters. You can use any one of those three actions, or a combination of them, to resolve the pending mismatches.

For example, suppose that you requested a tape link with two connecting paths, and you selected two specific, available adapters for your tape link. If a third adapter is already zoned for the tape library that is selected for your tape link, the fulfillment state of the tape link is Pending with mismatches because three zoned adapters exceeds the requested number of two connecting paths. On the **ADAPTERS** tab, the third adapter is listed in the table of Unrequested and zoned adapters, which is displayed above the assigned adapters table. Through Modification mode, you can resolve this mismatch through one of the following actions.

- Increase the number of connecting paths to 3. In this case, the unrequested adapter becomes an assigned adapter, and no zoning changes are required.
- Select the unrequested adapter for deletion. In this case, when you save your changes, the storage administrator receives zoning instructions to remove the host WWPN for this unrequested adapter.
- Replace one of the assigned adapters with the unrequested adapter. This action can be useful if one of the assigned adapters is pending (not zoned yet).

Modify the partition maximum, add or delete selected partitions, or edit HBA device numbers

Through the **PARTITIONS** tab in Modification mode, you can change the maximum number of partitions to use the tape link, or add or remove partitions from the Partitions table, which, in effect, starts tape link attachment or detachment operations when you save your changes. You also have the option of changing the device numbers of host bus adapters (HBAs) that a partition uses to access the tape library.

Notes:

- Removing a partition from the Partitions table does not delete the partition from the system; this action only detaches the tape link from the selected partition. Removing partitions from this table is the same as removing a tape link through the **Storage** section of the **Partition Details** task.
- Detaching a tape link from an active partition, changing an HBA device number for an active partition, and deleting an active partition are all disruptive changes. The suggested practice is to stop the partition before making any of these modifications.

Modify the maximum number of partitions to use the tape link
Use the "Maximum number of partitions" spinner or text field to set the maximum number of partitions to which the tape link can be attached. If you select partitions to attach the tape link, this number adjusts to match the number of selected partitions. You can either leave this adjusted value in place, or set the maximum manually: use the spinner or type the number that you want to set as the maximum.

The maximum value can exceed the number of selected partitions; however, the maximum value cannot exceed the system limit for concurrently active partitions. The text for this field indicates the limit for concurrently active partitions on your system.

Add or delete selected partitions (initiate attachment or detachment operations)
The Partitions table lists the partitions to which the tape link is attached. To remove a partition from the table, select the delete icon (trash can) in the corresponding table row. To add partitions, complete the following steps.

1. Select **SELECT PARTITIONS** to open a dialog through which you can view details about available partitions on the system: the partition name; its current status (Active, Stopped, and so on); and the user-supplied description, if any.
2. Use the check box to select each partition, then select **ADD** to close the dialog and populate the partitions table.

When you select **SAVE** to save your changes, DPM asynchronously detaches the tape link from any partitions that you deleted, or attaches the tape link to the partitions that you added. The tape link fulfillment state is Pending until these asynchronous processes complete.

Change the device number of a host bus adapter (HBA)
To view the HBAs that a partition uses to access the tape library, select **Details** in the corresponding table row. The Details view contains the Host Bus Adapter table, which includes the editable **DEVICE NUMBER** field. If you want to change the device number, specify a four-character hexadecimal device number in the editable device number field.

Configure Storage Cards
Use the **Configure Storage Cards** task to modify the currently configured FCP or FICON adapter cards installed in a DPM-enabled system. You can access the **Configure Storage Cards** task by selecting **STORAGE CARDS** in the **Configure Storage** task. Note that you cannot reconfigure NVMe adapters through this task; reconfiguration requires properly removing the carrier card and its SSD from the drawer and reinstalling them in a different physical location, as instructed by a service representative.

Before you begin

- To open this task, you can use the default SYSPROG or SERVICE user IDs, or any user IDs that an access administrator has authorized to the **Configure Storage** task through customization controls in the **User Management** task. Also, you must have access permission to all storage adapters.
- Note that DPM does not allow the reconfiguration of any adapter card that is already in use. For more details about in-use FCP and FICON adapter cards, see step “2.a” on page 612.

About this task

Through the **Configure Storage Cards** task, you define the protocol of theFICON Express adapters that are installed in the system I/O drawers. DPM automatically detects the installed adapters, which you can define as either FICON or FCP devices. If you change the number of cards that are already specified, DPM

automatically selects a combination of the unconfigured cards, but you can override these selections, if necessary.

When you have finished making changes, DPM provides an updated exportable file of an FCP and FICON adapter cabling plan that you can use to physically connect the system to SAN hardware. The file is in Comma Separated Values (CSV) format that you can view in a spreadsheet application.

Procedure

1. Open the **Configure Storage** task, and select **STORAGE CARDS** to open the **Configure Storage Cards** page.

   The **Configure Storage Cards** page opens to a visual abstraction of each physical I/O drawer in the system. Each drawer has a front and rear display, each with two domains, as well as adapter-card slots. An I/O drawer can contain different types of adapter cards, so DPM highlights only the slots containing an adapter card that you can use for connections to storage devices.

   Depending on the configuration of the system, you might need to use navigation controls to view all of the frames, drawers, and cards. For systems with only one frame, use the scroll bar or expand/collapse controls to view adapters in the frame drawers. For multiple-frame systems, use the overview map to change the viewport display, as shown in Figure 37 on page 611.

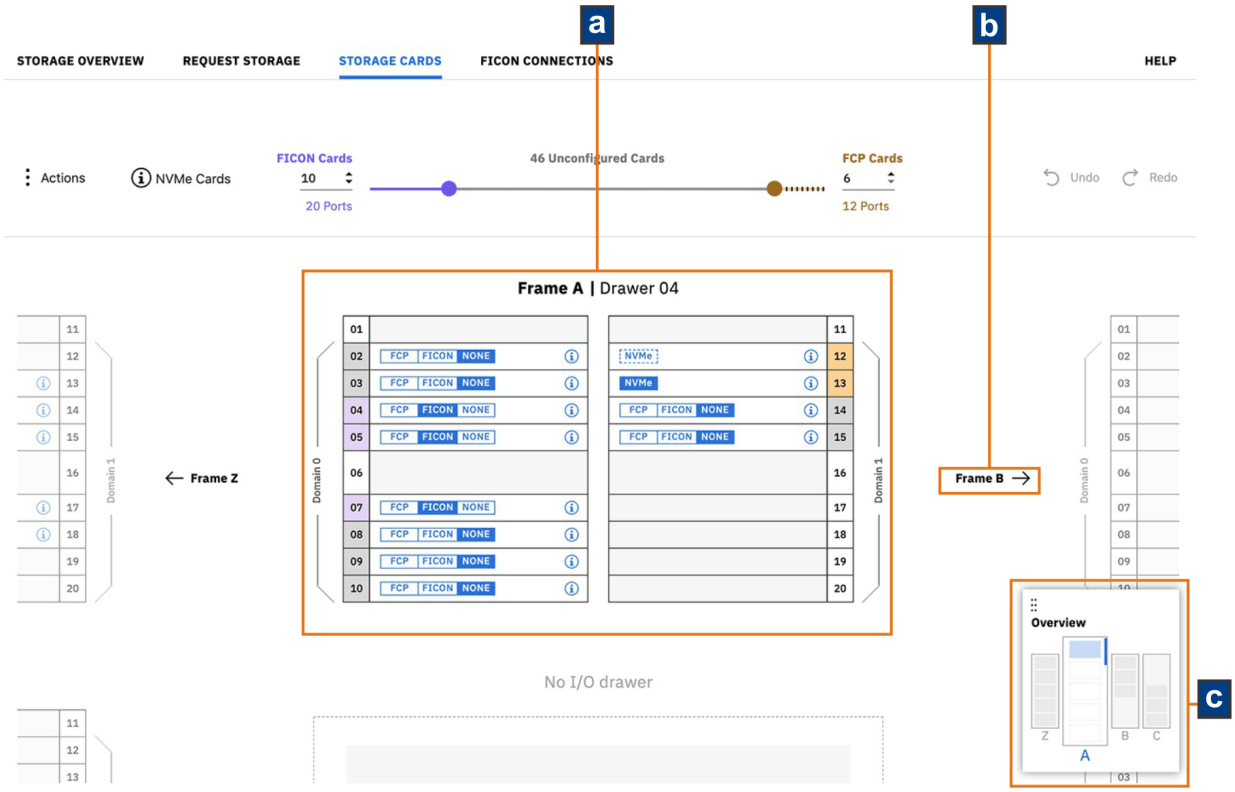


Figure 37. Overview map and other viewport navigational controls

a. This screen capture shows Frame A centered in the viewport.

b. Selectable frame buttons on either side of Frame A provide a way to change the viewport to either the previous or next frame in the system. These buttons are displayed only when the system is configured with additional frames to the left or right of the current frame.

c. The overview map shows not only how many frames are in the system, but also which frame and which I/O drawer within that frame are currently displayed in the viewport. In this example, Frame A has only one I/O drawer installed, which is shown as a solid blue rectangle. When another frame with multiple I/O drawers becomes the current frame in the viewport, any additional I/O drawers that are not currently in the viewport are shown as white rectangles with blue outlines. To change

the display in the viewport, select a different frame in the overview map or use the frame buttons. Scroll up or down to view different I/O drawers within the current frame, if any.

If the system has one or more IBM Adapter for NVMe1.1 features, the frame display also indicates the current location of any installed NVMe carrier card. For an overview of any NVMe adapters that are installed in the system, hover your cursor over the information icon (ⓘ) to the left of the **NVMe Cards** label. To download a CSV file of details about the NVMe storage adapters, use the **Actions** menu to select **Export NVMe Plan**.

Each NVMe adapter consists of two pieces of hardware: an IBM-supplied carrier card installed in a system I/O drawer, and the solid state drive (SSD) that customers purchase. The page display identifies which hardware is installed and whether the adapter is in use.

- When an NVMe carrier card is installed but does not contain an SSD, the NVMe adapter label is shown as a white rectangle with a dotted blue outline. When the carrier card is empty, selecting the information icon opens a window that contains the adapter location; the card type; the adapter ID; and a control to toggle the LED light on the physical card on or off.
- When an SSD is installed in the carrier card, the NVMe adapter label is a solid blue rectangle. When an SSD is installed, selecting the information icon opens a window that contains the adapter location; the card type; the adapter ID; the size and serial number of the SSD; the toggle for the LED light; and a link to the **Adapter Details** task.
- When an NVMe SSD is defined as a volume of a storage group, the NVMe adapter is considered in use, whether or not the storage group is attached to a partition. In this case, a lock icon is displayed next to the NVMe adapter label. To determine which storage group is using a locked NVMe adapter, record the serial number of the SSD and select **Storage Overview** to view a list of NVMe storage groups. For each NVMe storage group, open the Storage Group details page and look for the matching serial number in the table on the **VOLUMES** tab.
- A red dot indicates that DPM recently detected the NVMe adapter.

2. On the **Configure Storage Cards** page, set unconfigured adapter cards as either FICON or FCP, or modify the protocol of configured cards, as necessary.
   a) If you want to change the total number of FICON or FCP adapter cards, use the slider or input fields to specify the number of each type of adapter.

   Figure 38 on page 612 shows the UI controls for specifying the number of each adapter type.

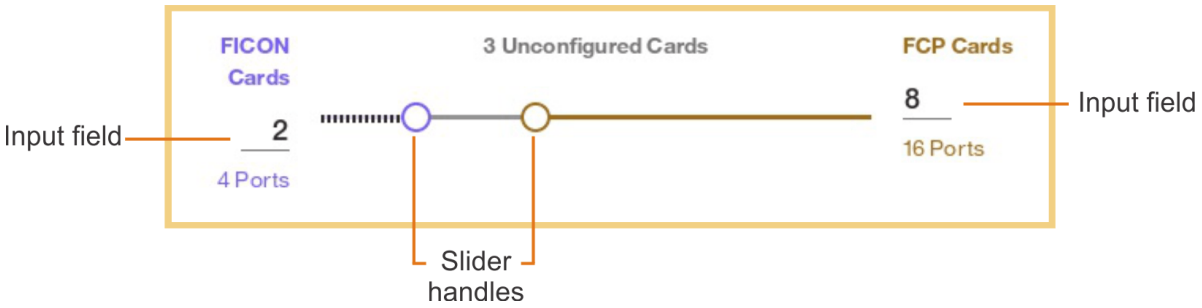


Figure 38. Slider and input fields for FICON or FCP adapter cards

   - When you use the sliders or input fields to enter the number of FICON or FCP cards, DPM automatically selects a combination of the unconfigured cards to satisfy your request. This combination is *redundant*; that is, the configured cards of each type are spread across domains and drawers to ensure availability, in case of a card or drawer failure. You can override these selections by selecting the appropriate protocol label in each card: FICON or FCP. Selecting NONE resets the adapter card to the unconfigured state. Depending on the type of adapter card and its cabling, you might not be able to change the protocol through these labels. For these adapter card types, the protocol labels are disabled.
   - To display more information about a particular FICON or FCP adapter, select the information icon (ⓘ) to open a display that contains details such as the adapter location and card type, the

adapter ID, and physical worldwide port numbers (WWPN) for each port on the adapter. This display also includes a link to open the **Adapter Details** page of the **Manage Adapters** task.

- Note that DPM does not allow the reconfiguration of any adapter card that is already in use. FCP and FICON adapter cards that are in use are shown with disabled (gray) label selections for changing the current configuration. For example, if an adapter card is currently configured as a FICON card and is in use, its labels for FCP and NONE are disabled (shown in gray). FCP cards also are marked with a lock icon when they are in use for access to a disk or tape storage device.
  - An FCP adapter card cannot be reconfigured when it is in use by a storage group that is attached to a partition, regardless of the partition state; when it is in use by a tape link; or when it is used to reach a tape library. For an FCP adapter that cannot be reconfigured, you can determine which storage groups are using the adapter by completing the following steps:
    1) Select the information icon to open a display that contains a link to open the Adapter Details page.
    2) Select the link and review the Connections section to determine which storage groups or tape links are using the adapter.
  - A FICON adapter cannot be reconfigured when it provides a logical control unit (LCU) path to a switch or storage subsystem. For a FICON adapter that cannot be reconfigured, you can determine which switch or storage subsystem is using that adapter by completing the following steps:
    1) Select the information icon to open a display that contains the adapter ID that you need, and make a note of it.
    2) Go to the FICON Connections page, and select the **Connect Adapter Ports** link in the System box.
    3) On the Connect System to Switches page or Connect System to Subsystem page, use the search to find the adapter ID in the frame display. Enter the adapter ID into the search field, and select the name of the matching adapter port in the drop-down list. The adapter port name in the search field is outlined with gray, which denotes that the adapter port is in use. When you hover your cursor over the adapter port name in the search field, the adapter port label in the frame display shows the ID of the switch or storage subsystem that is using the port. When you hover your cursor over the adapter port in the frame display, the adapter details include a message indicating that the adapter port is in use and cannot be disconnected.

b) Review the updates that you have made.

Figure 39 on page 614 shows a sample portion of the frame display on the **Configure Storage Cards** page, with the most recently configured adapter cards marked with a red dot.

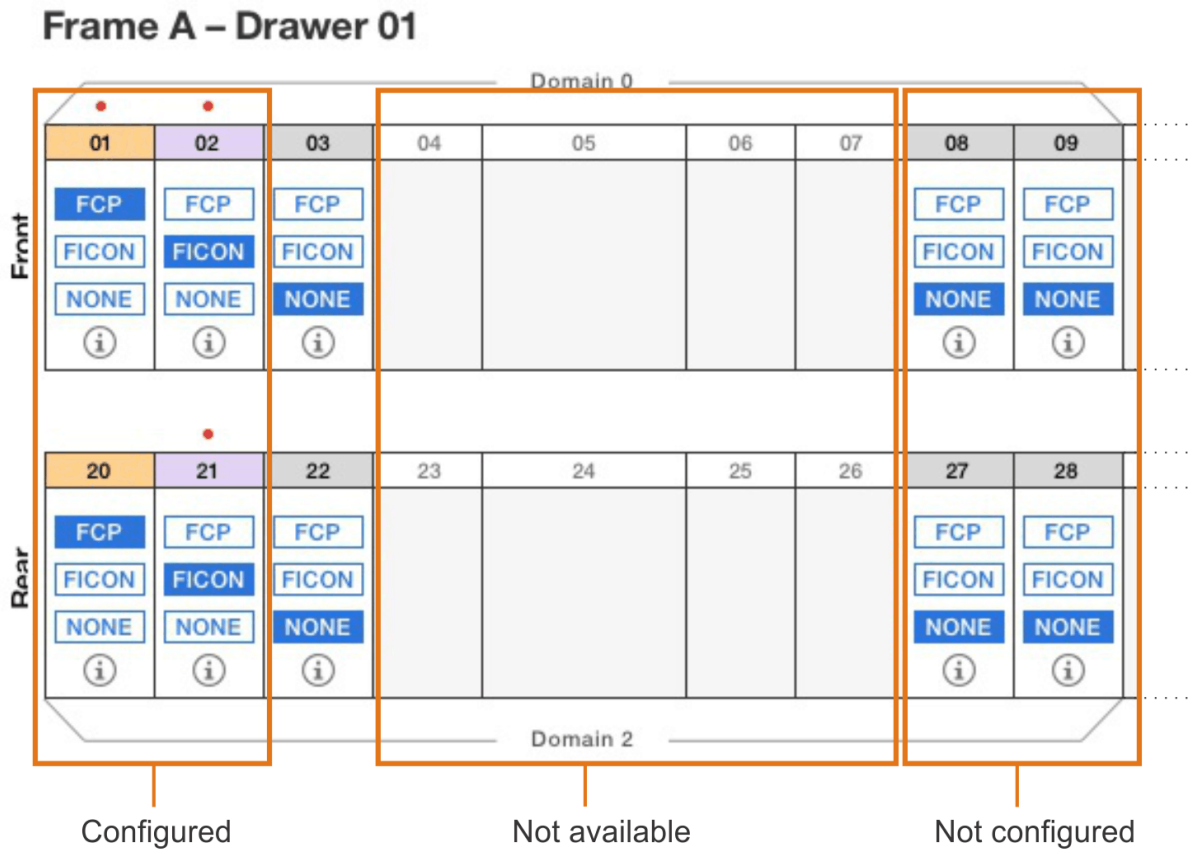


Figure 39. Sample display of a partial frame drawer, with domains and adapter cards

3. When you have finished defining or modifying the FICON or FCP adapter cards, select **SAVE** to apply your changes.

Results

You have fully configured adapter cards on the DPM-enabled system. You can download an updated copy of the cabling details file and view it through a spreadsheet application. Note that physical storage hardware (subsystems, switches, and so on) must be connected by cables, and storage cards must be configured through the **Request Storage** task.

Configure FICON Connections

Use the **Configure FICON Connections** task to complete the initial configuration, or to modify the current configuration, of the FICON-based, external storage hardware devices that are connected to a DPM-enabled system through FICON or FCP adapters. These hardware devices include disk storage subsystems, fabrics, and switches.

Before you begin

- To open this task, you can use the default SYSPROG, STORAGEADMIN, or SERVICE user IDs, or any user IDs that an access administrator has authorized to this task through customization controls in the **User Management** task. Also, you must have access permission to all FICON adapters.
- If you need help to complete this configuration, you can use the **Invite** link on the **Configure FICON Connections** page to notify a co-worker about the remaining configuration tasks. DPM automatically generates an invitation that you can send, to which you can add your own greeting and more details, if necessary. For integrated invitations and notifications, users must have an email address associated with their user IDs, and Simple Mail Transfer Protocol (SMTP) settings must be defined.
  - Email addresses for users are assigned through the **User Management** task.

  - The SMTP server and port settings are defined through the **Monitor System Events** task.
- If you plan to request or create tape links to provide partitions with access to tape libraries in the SAN, you need to configure some storage cards to use the FCP protocol, as described in "Configure Storage Cards" on page 610. However, do not define tape libraries as part of the FICON connections in this procedure. Instead, follow the procedure in "Request or create a tape link" on page 567.

About this task

Through this task, system and storage administrators collaborate to connect a system to devices in the storage area network (SAN) through a simplified, visual, and automated process that does not require extensive knowledge of mainframes or Linux systems. This process does, however, require administrators to know high-level information about the physical elements of the SAN, such as the names of storage subsystems, the types of devices and communication protocols, intended use, and so on. This information is usually available through a system plan for the company's physical IT site.

Through the **Configure FICON Connections** task, you can build or modify a visual copy of the storage hardware devices in the SAN and their FICON connections to this system. This configuration can contain at most two physical sites where storage devices are located. The primary site is always where the DPM-enabled system is physically located. System administrators can define physical elements, such as switches, fabrics, and disk storage subsystems, but storage administrators are required to define port connections and logical control units (LCUs). The same authorizations are required to modify any of the physical elements that have been defined for the current storage configuration.

If the DPM-enabled system is not yet physically attached to SAN hardware through cables, DPM provides several automated options for this configuration process; for example, storage administrators have the option of having DPM select port connections. However, if the system is already cabled, you need to supply information that reflects the physical connections that are already in use.

Depending on the configuration that has been done already, you might need to only modify existing elements, or you might be starting from scratch. For completeness, the steps in this procedure describe how to configure physical elements from scratch, but also include advice for modifications. Note that, if you are modifying a configuration that is currently in use, DPM provides messages to help you avoid making changes that might disrupt running workloads. When you have finished, DPM provides a summary of running partitions and storage groups, if any, that were affected as a result of your dynamic reconfiguration changes. DPM also provides an updated exportable file of an FCP and FICON adapter cabling plan that you can use to physically connect the system to SAN hardware. The file is in Comma Separated Values (CSV) format that you can view in a spreadsheet application.

Procedure

1. Open the **Configure Storage** task.
   - If you accessed the **Configure Storage** task through a link in an invitation, select **START** to open the **Configure FICON Connections** page.
   - Otherwise, select **FICON CONNECTIONS** to open the **Configure FICON Connections** page.
2. On the **Configure FICON Connections** page, define or modify the storage hardware that is or will be connected to this DPM-enabled system.

   This page provides a basic visual layout of the storage configuration, along with hover help to guide you through the process of defining a replica of the storage hardware that is or will be connected to the system. The replica must match the planned or actual configuration of storage subsystems and switches. Your SAN configuration can consist of point-to-point (direct) connections or switch connections, but not both.

   The page content varies, depending on what physical elements have already been defined. You can look for check marks (to identify fully configured elements, or for warning indicators ( ) or highlighted red text, which indicate partially configured elements that require attention. Figure 40 on page 616 shows a sample display of a partial configuration.

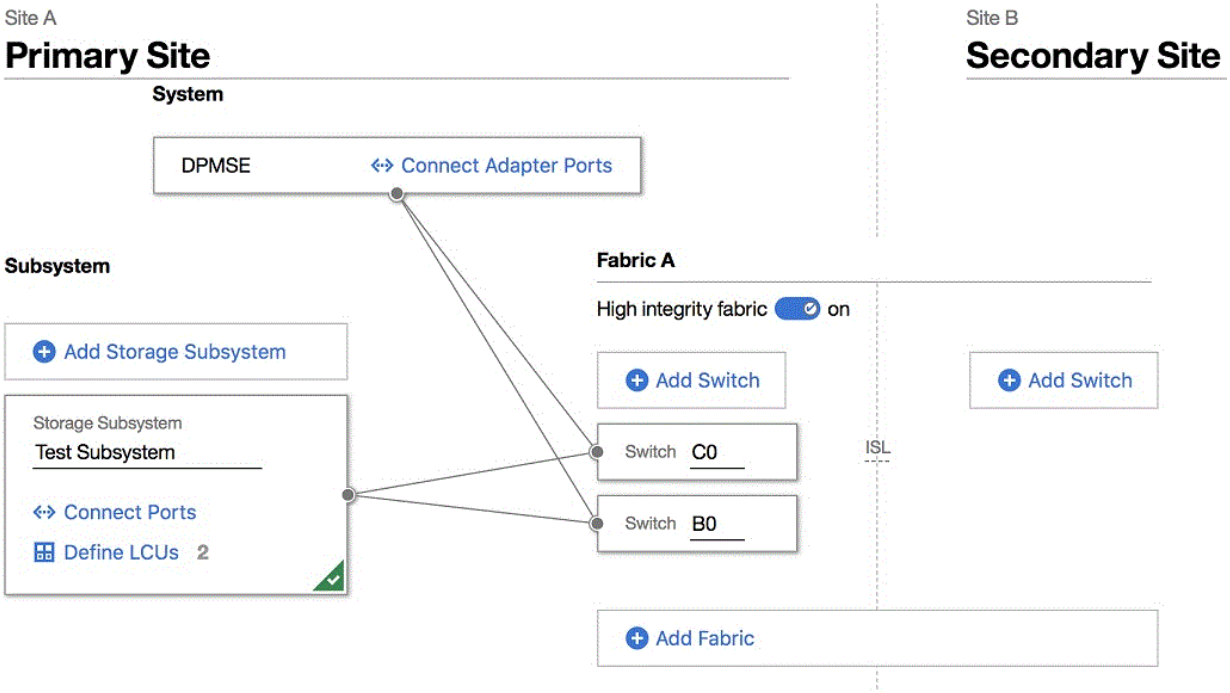


Figure 40. Sample display of a partially configured primary site

You can define or modify elements for the primary site and the secondary site, if one has been defined already. If you want to define a secondary site, you can select **Add empty site** to add headings and controls for manually defining that site, or select **Add and clone to the secondary site** to clone the elements that you have already defined for the primary site. The name of the secondary site must be different from the name of the primary site, and the same length and supported-character rules apply to both names.

You can clone the primary site any time after the first storage subsystem or switch is added to the primary site. DPM duplicates the primary site subsystems, fabrics, and switches, along with adapter ports and LCUs, but you must provide unique names and IDs for the storage subsystems and switches.

- For a configuration with point-to-point (direct) connections, DPM automatically replicates the physical paths between the system and all cloned storage subsystems.
- For a configuration with fabrics and switches, DPM automatically replicates physical paths as you provide a unique switch ID for each cloned switch.

If a secondary site already exists, you can delete that site only when it does not contain any switches or subsystems.

As you work through the following steps, you open different subtask windows to make selections or perform actions, then select **DONE** to save your changes or **CANCEL** to discard them; either button selection returns you to the **Configure FICON Connections** page. Note that, while you are working in a specific subtask window, the **Undo** and **Redo** buttons revoke or restore changes only within that window. On the **Configure FICON Connections** page, however, the Undo/Redo history includes the changes that you saved in a subtask window, as well as any selections you made on the **Configure FICON Connections** page itself. For example, suppose that you select the **Connect Adapter Ports** link in the System box and, on the **Connect System** window, you select two or more configured adapter ports in the system I/O drawers, and select **DONE** to save those changes. Back on the **Configure FICON Connections** page, you can use **Undo** and **Redo** to delete those two connections or restore them, without having to reopen the **Connect System** window.

a) If the primary site does not have a name, start by adding one.

   The name can be 1 - 32 characters in length. supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters.

b) Add or modify physical elements for the primary site. If you need to add new elements, select the plus sign to add a box that represents a specific physical element in the SAN.

   As you provide names for new elements, note that supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters.

   1) If your SAN configuration consists of point-to-point (direct) connections rather than switches, skip to the next step to add storage subsystems. Otherwise, select the plus sign to add and name a fabric, and then add one or more FICON switches. Fabric names must be unique among fabrics, and cannot exceed 32 characters. Switch IDs must be unique within a fabric, and consist of hexadecimal values in the range 01 - EF. If necessary, repeat this process to add more fabrics and switches. You can create a maximum of 256 fabrics per site, and a maximum of 239 switches per fabric.

      If you are modifying existing fabrics and switches, the following rules apply.

      - You cannot modify the high integrity fabric setting when LCUs are in use for switches in the fabric. If you need to modify the high integrity fabric setting, you must first remove all of the paths from the LCUs that are using that fabric, and then modify the high integrity fabric setting. After modifying the setting, you can restore the paths by adding them back to the LCUs.
      - You can delete a fabric from a site only when the fabric does not contain any switches.
      - You can delete a switch only when all of its existing connections (to an adapter port or to a storage subsystem) are not configured in any storage group.
      - You can disconnect a switch only when both of the following conditions are true.
        - No storage groups are using the switch port.
        - All LCUs that are using the switch port are not being used to fulfill a storage group.

   2) Under the Subsystems label, select the plus sign to add a storage subsystem, and provide a name for it. If necessary, repeat this process to add and name more subsystems, specifying a unique name for each. Storage subsystem names must be unique among storage subsystems, and cannot exceed 64 characters. You can create a maximum of 256 storage subsystems per site. You can delete a storage subsystem from a site only when that storage subsystem does not contain any LCUs.

c) Select the **Connect Adapter Ports** link in the System box.

   The **Connect System** window opens to a visual display of the configured adapters with their ports (typically two ports per adapter), along with either the storage subsystems (for direct connections without switches) or switches that are defined for the primary site. If you have defined storage subsystems or switches for the secondary site, you need to select **Show** to display them.

   Adapters are displayed by frame; for multiple-frame systems, a viewport indicator is displayed so that you can easily switch to view a different frame. The indicator shows how many frames are in the system, and which frame is currently displayed in the viewport. To change the display, select a different frame in the viewport indicator or use the frame buttons.

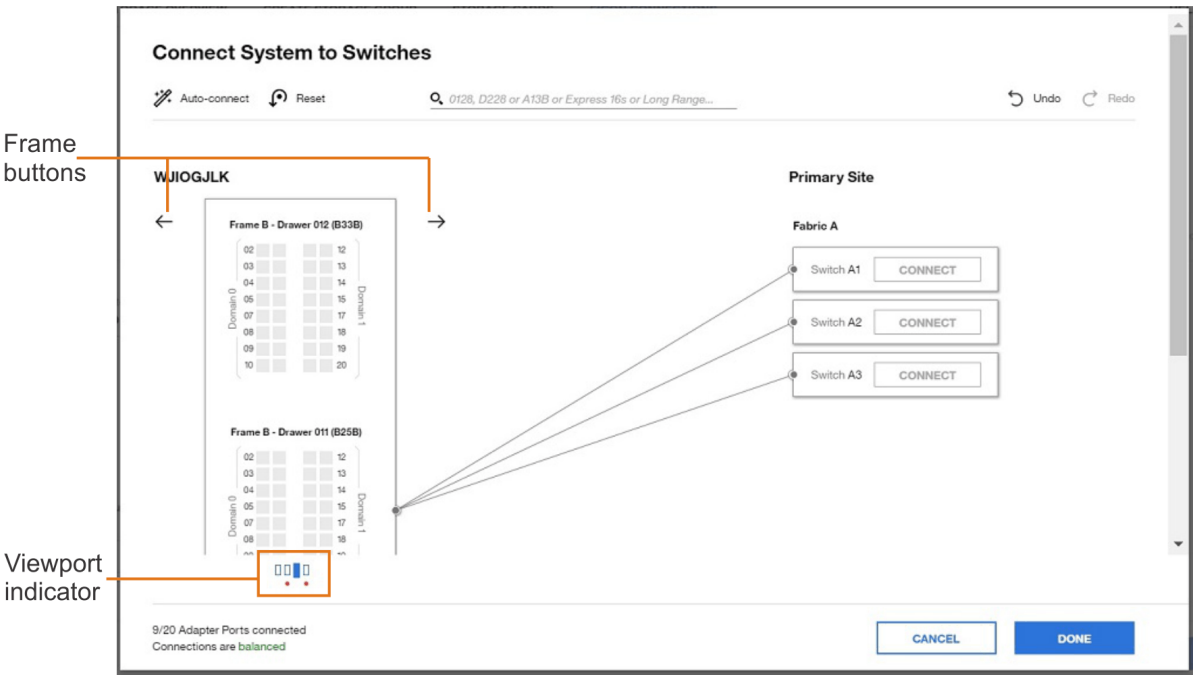


Figure 41. Viewport indicator and frame buttons

If you are modifying existing adapter ports, note that you can disconnect an adapter port only when both of the following conditions are true.

- No storage groups are using the adapter port.
- All LCUs that are using the adapter port are not being used to fulfill a storage group.

If the system is not cabled yet, the suggested practice is to select the **Auto-connect** icon ( ) to have DPM automatically connect all unconnected ports, but you can select each port yourself. You cannot select unconfigured adapter ports, which are shown in gray. For availability, connect each storage subsystem or switch to at least two adapter ports, each of which resides in a different frame and domain of the system. If the automatic updates from **Auto-connect** span more than the current frame of a multiple-frame system, a red dot is displayed under the updated frames in the viewport indicator, and a message is displayed next to the appropriate frame button.

1) Select two or more configured adapter ports in the system I/O drawers. While making your selections, you can hover over each adapter port to display more details, including the adapter name, location, ID, card type, and cable type. You can also use the search field to highlight one or more adapter ports, using a search string for any of these adapter port properties. Available adapter ports with properties that match the search string are highlighted with a blue outline.
   - The search provides an auto-suggest function to help you more quickly select an adapter port with properties matching the search string that you enter.
   - If adapter ports that match the search string are not in the currently displayed frame of a multiple-frame system, the display automatically changes to show the closest frame containing search results. If more adapter ports that match the search string reside in other frames, a text label that indicates the number of those matching adapter ports is displayed above one or both frame buttons, depending on the location of the additional adapter ports.
   - If an adapter port in the search results is already in use and cannot be configured, DPM does not highlight that adapter port unless you hover your cursor over a search tag containing the adapter port in the search field. If you hover your cursor over the box for the in-use adapter port in the frame display, a message in the adapter details window indicates that the adapter port cannot be changed.
   - The search field can expand to multiple lines, if you require more space to enter search strings or adapter names.

2) Select **CONNECT** in a specific storage subsystem or switch to connect it to the selected adapter ports. Note that the box for each adapter port now displays the storage subsystem or switch ID, and a line now connects the system to the storage subsystem or switch. Line numbers indicate the total number of adapter ports connected to the storage subsystem or switch.

   For storage subsystems, the ID consists of the letter A to indicate the primary site (B indicates the secondary site, if any) and a sequential number, starting with 1 (one). This ID is also appended to the storage subsystem box label in this display.

3) Repeat as necessary until all storage subsystems or switches are connected to the system. For the best results, make sure that the indicator (at the foot of the window, under the adapter port display) identifies the connections as balanced. You are not required to do so but, if **BALANCE CONNECTIONS** is enabled, you can select that button to have DPM modify the port connections such that all connected switches have as close to the same number of port connections as possible. If the automatic updates from **BALANCE CONNECTIONS** span more than the current frame of a multiple-frame system, a red dot is displayed under the updated frames in the viewport indicator, and a message is displayed next to the appropriate frame button.

   For example, suppose that you have connected the system to four switches: three in one fabric, and one in another fabric. One switch, switch B4, has six port connections, and the other switches have fewer connections (five, four, and three).

   - If you select **BALANCE CONNECTIONS**, DPM adds available port connections so that each of the four switches have as many connections as the switch with the highest number of six port connections.
   - If the number of available port connections does not allow each switch to have six connections, DPM removes connections from switch B4 and adds them to the other switches, to distribute the number of port connections as evenly as possible among the four switches. If DPM cannot remove port connections on the switch because they are in use, **BALANCE CONNECTIONS** is disabled.

   Note that using **Auto-connect** and **BALANCE CONNECTIONS** are similar in that DPM attempts to evenly balance connections across subsystems or switches, but the two connection methods differ in the following ways.

   - **Auto-connect** connects all available ports, while **BALANCE CONNECTIONS** uses only enough ports to ensure that each connected switch has as many port connections as the switch with the most port connections.
   - **Auto-connect** does not reconfigure any already connected ports, while **BALANCE CONNECTIONS** can reconfigure already connected ports, if necessary.

4) When you have finished, select **DONE** to return to the **Configure FICON Connections** page. Note that lines connect each storage subsystem or switch to the system, with each line indicating the number of connections.

d) If you are using direct connections without switches, skip to step "2.f" on page 620 to define LCUs; otherwise, continue to the next step.

e) For each storage subsystem in the display, select the **Connect Ports** link. Complete this step only if you are using fabrics and switches in your configuration.

   The **Connect Subsystem to Switches** window opens to a visual display of the ports on each switch that is defined on the same site as the storage subsystem. (To see all defined fabrics and switches, you might need to scroll down or use the expand or collapse controls.) For availability, the suggested practice is to connect each storage subsystem to at least one switch per fabric, and at least two ports on each switch. You can define a maximum of 64 connections to switches on each subsystem. For the best results, make sure that the redundancy indicator (at the foot of the window) identifies the connections as redundant.

   1) In the box for the first switch, select whether you want to view the switch port numbers in decimal or hexadecimal notation. You can also specify the switch size, by typing an integer from 1 - 256 in the input field, which is part of the port counter at the bottom of the switch box. Note

that you can reduce the size of an existing switch only when the reduction would not result in the removal of ports that have existing connections.

2) Select one or more ports in the switch. Note that a line displays the connection between the storage subsystem and the switch, with a number that indicates the total of selected ports for that switch.

   If necessary, use the search field to locate one or more switch ports, using a two-digit number for each port, in the notation that you have chosen to view the switch ports (decimal or hexadecimal). If you enter a number in a notation that does not match the notation that you have selected for viewing switch ports, DPM indicates that the search value is invalid. You can select **Connect all** to connect the valid switch ports that are listed in the search field to the storage subsystem. If the result of this action will cause the total number of switch connections to the storage subsystem to exceed the maximum of 64, **Connect all** is disabled.

3) Select one or more ports in other switches that are displayed, either manually or by selecting **Clone to** and selecting one or more target switches.

   - If the result of cloning will cause the total number of switch connections to the storage subsystem to exceed the maximum of 64, **Clone to** is disabled.
   - If the target switch is smaller than the switch you are cloning, DPM automatically increases the size of the target switch to match the cloned switch.
   - The cloned switch port numbers match the source port numbers. For example, suppose that you select ports 0, 8, 21, and 28 on Switch 10, and clone those ports to Switch 20. When you expand the display of Switch 20, ports 0, 8, 21, and 28 are selected.
   - If the ports on the target switch are not free, DPM overwrites the target switch configuration unless a storage group is already using the target switch port. In this case, you cannot select the target switch for the cloning operation.

4) When you have finished, select **DONE** to return to the **Configure FICON Connections** page. Note that lines now connect the subsystem to the switches on which you selected ports.

5) Repeat this process as necessary, for each subsystem.

f) For each storage subsystem in the display, select the **Define LCUs** link.

The **Define LCUs and Logical Paths** window opens.

1) Select the plus sign to add one or more LCUs for the storage subsystem. The Add LCUs window opens.

2) On the Add LCUs window, type one or more LCU numbers in the LCU Numbers field, or select the table icon () to open the LCU input matrix. You can specify a range of LCU numbers, or individual numbers, or both. LCU numbers must be unique within the storage subsystem; valid values are in the range 00 - FF. You can specify a maximum of 256 LCUs per storage subsystem. The suggested method to use is the matrix because it shows which LCUs are already configured; configured LCUs are gray, as shown in Figure 42 on page 621.

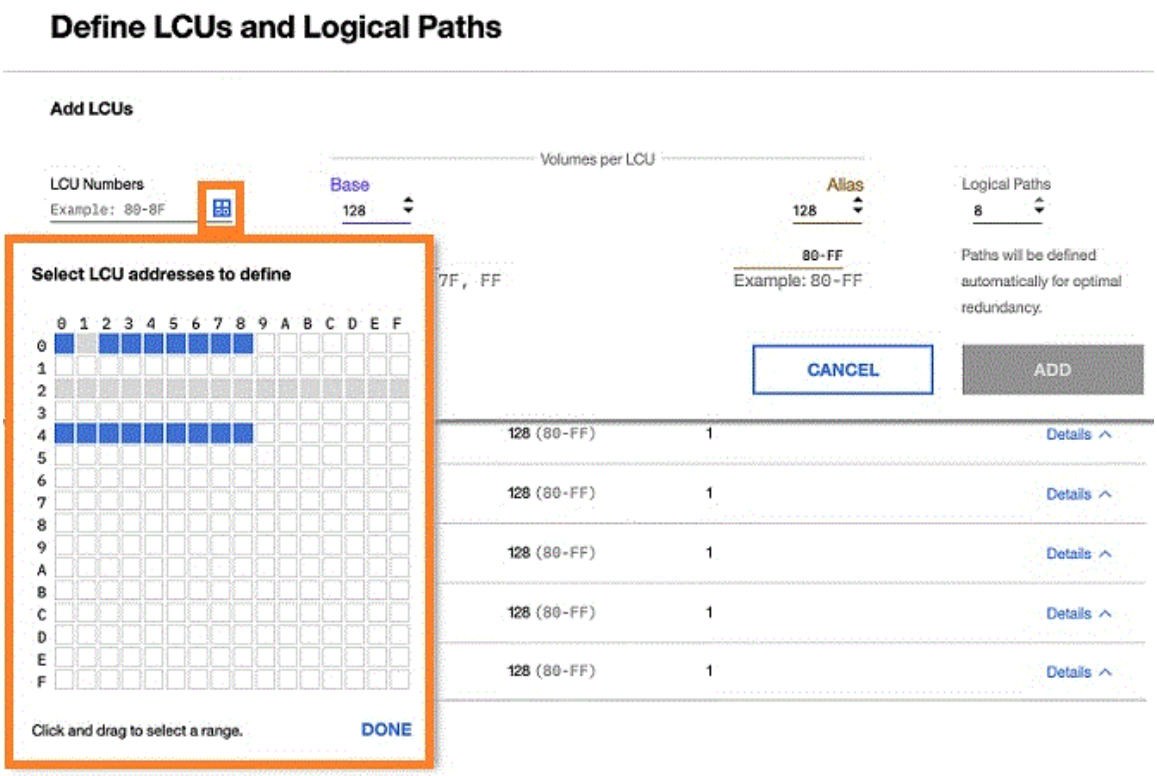


*Figure 42. Sample display of the LCU input matrix (highlighted) on the **Define LCUs and Logical Paths** window*

3) Use the **Base** and **Alias** fields to specify the number of base and alias volumes to define for each LCU. Either type the number or click the up or down arrows increase or decrease the number. You can specify up to a combined total of 256 base and alias volumes for one LCU. Note that you cannot add an alias volume if any base volume is being used to fulfill a storage group.
4) If necessary, change the value specified in the **Logical Paths** field, which represents the requested number of paths. The maximum value for an LCU is 8 logical paths. If you are modifying the paths for an existing LCU, the following rules apply.
   - Although you can add a path to or delete a path from an LCU that is being used by a storage group while it is attached to a partition, you cannot delete the last remaining path from an LCU that is in use.
   - You cannot add a path to an LCU in the primary site if doing so requires the use of a cascaded switch. Only the secondary site can have cascaded switches.
5) Select **ADD** to add the LCUs. DPM automatically selects paths to maximize redundancy and to reduce common points of failure. The **Define LCUs and Logical Paths** window now contains a table that lists each LCU or group of LCUs, along with the number of base volumes, the number of alias volumes, and the number of logical paths for each LCU. DPM groups LCUs that have the same number of base volumes, the same number of alias volumes, and the same configured paths. To view all of the LCU numbers (addresses) in the group, select the information icon in the LCU column (the resulting display is similar to the LCU input matrix, but it is read-only). The table entry for a group lists the total number of LCUs in the left margin of the table row, which you can select to expand the group entry.

   By selecting **Details**, you can expand the LCU table entry to view or edit details about the logical paths to the system. The expanded view is another table that contains a row for each path. If you have already connected the system to one or more switches, this table lists the assigned switch, switch port, adapter ID, and adapter location. If the logical path goes through cascaded switches, this table includes another SWITCH column between the SWITCH PORT and ADAPTER ID columns.

If necessary, you can select **EDIT** to modify or delete any of the information on the **Define LCUs and Logical Paths** window. To prevent a path from being changed or deleted, you can select the lock icon. If you edit a path statement, it is locked by default. If you are modifying or deleting elements, the following rules apply.

- You cannot delete an LCU when a storage group is using it.
- You cannot delete a base volume or alias volume when it is being used to fulfill a storage group.

Note that some changes that you make through the edit function might result in the LCU being removed from a group.

When you have finished, select **SAVE** to exit edit mode.

6) Optional: To copy one or more of the defined LCUs to another subsystem, select **Clone to**. The cloned LCU numbers match the source LCU numbers. If any LCUs with matching numbers are already defined for the target subsystem, DPM prompts you to confirm the cloning operation before overwriting the target subsystem's LCU configuration.
   - If a storage group is already using an LCU with a matching number on the target subsystem, you cannot select that storage subsystem for the cloning operation.
   - You can also use the search field to locate an LCU or range of LCUs, using two-digit hexadecimal search strings, separated by a comma when you specify more than one string.
7) Select **DONE** to return to the **Configure FICON Connections** page. Note that the box for the storage subsystem now lists the total number of defined LCUs.

When you have finished adding LCUs, note that the box for each subsystem contains a check mark ( ).

g) Check the display for warning indicators ( ) or highlighted red text to make sure that you have supplied names and connections as required.

3. If storage cards must be configured, use the **Invite** link on the **Configure FICON Connections** page to notify a co-worker about the remaining configuration tasks.
4. Select **SAVE** or **SAVE & FINISH** to save the configuration data that you have supplied.

   If storage cards are already configured, and you have completed the FICON configuration, DPM automatically changes the button label to **SAVE & FINISH**.

Results

Depending on the configuration activities you completed in step “2” on page 615, you have either fully or partially configured storage for the DPM-enabled system. If you have invited one or more storage administrators to complete the configuration, they can log in to the HMC and open the **Configure Storage** task through a link in the invitation, and complete the configuration. If you modified a configuration that is currently in use, DPM provides a summary of running partitions and storage groups, if any, that were affected as a result of your dynamic reconfiguration changes.

What to do next

- Use the **Request Storage** task to define storage resources, known as storage groups, for partitions to use. For more information, see “Request or create a FICON or FCP storage group” on page 560 or “Request or create an NVMe storage group” on page 565.
- If you exported the cabling details file before the FICON configuration was completed, you can download an updated copy. Note that physical storage hardware (subsystems, switches, and so on) must be connected by cables, and storage cards must be configured before you can use the **Request Storage** task.

Create and manage templates for FICON or FCP storage groups

To make storage requests even easier to complete, administrators can create a template for requesting a FICON or FCP storage group. Templates can reflect typical usage patterns (production, staging, test);

standardize storage for specific user groups; or document company requirements or restrictions that might be in place for storage use. Users can select an available template and, with minimal changes, quickly submit a request for a new storage group. Note that you cannot use a template to define an NVMe storage group.

Before you begin

To create and manage storage templates through the **Configure Storage** task, you can use the default SYSPROG, STORAGEADMIN, or SERVICE user IDs, or any user IDs that an access administrator has authorized to this task through customization controls in the **User Management** task.

Procedure

1. Open the **Configure Storage** task. The options displayed on the Configure Storage page depend on the authorization of your user ID. To work with templates, select **REQUEST STORAGE GROUP**, **CREATE STORAGE GROUP**, or **MANAGE TEMPLATES**.
2. Select the **Create Template** (plus) icon.
3. On the **Name Template** page, specify the name of the new template and, optionally, provide a description.
   - For the name of the template, specify a value that is 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters.
   - For the optional description, use up to the maximum of 200 characters.
4. On the **Specify Storage Attributes** page, specify the attributes that you want for any storage groups that are created from this template.
   a) For Type, select the type of storage: FICON or FCP.

      This setting represents the type of storage devices that the storage group can use, and also controls the other attributes or default settings that are displayed on this page.

   b) For Shareability, select either **Dedicated** or **Shared**.

      If you select **Dedicated**, then only one partition is able to use this storage group. If you select **Shared**, specify the number of partitions that can share this storage group by moving the **Partitions** slider, typing a number in the input field, or clicking the up or down arrows to increase or decrease the number. The maximum number of partitions is set automatically to the system limit.

   c) For Connectivity, specify the number of paths to be available for use by each operating system with access to this storage group.

      The number of paths that you can define varies, depending on the storage group type. For FCP, the limit is the total number of adapters that are configured as FCP on the system; for FICON, the limit is the number of adapters that are configured as FICON on the system, up to a maximum of eight. The number that you select affects overall bandwidth, performance, and redundancy. Specify the number by moving the **Paths** or **Paths per Operating System** slider, typing a number in the input field, or clicking the up or down arrows to increase or decrease the number.

      FCP
      The suggested practice is to define at least two paths.

      FICON
      The suggested practice is to set the number of paths to the standard eight.

   d) For a dedicated FCP storage group only, select **Optimized for 2nd level virtualization** when you want to enable the direct assignment of host bus adapters (HBAs) so an operating system or its guests can access the storage group.

      Although the controls in the **Configure Storage** task allow you to select this attribute only for a dedicated (not shared) FCP storage group, you can optimize 2nd level virtualization for separate partitions so they can share the same storage disks. For instructions, see “Optimize 2nd level virtualization and share the same FCP disks across partitions” on page 625.

If you select this check box, specify the number of additional connections (HBAs) that can be assigned directly to the operating system or its guests. Specify the number by moving the **Additional HBAs** slider, typing a number in the input field, or clicking the up or down arrows to increase or decrease the number.

DPM distributes additional HBAs as equally as possible, taking into account both fabrics and adapters that will be assigned to this storage group, as indicated through the Connectivity attribute setting. For example, suppose that your storage configuration has two fabrics (A and B), the Connectivity attribute is set to 2, and you specify 7 additional HBAs. In this case, DPM creates a total of nine HBAs: one HBA for an adapter on fabric A and one for an adapter on fabric B to satisfy the Connectivity attribute setting, plus the seven additional HBAs. DPM assigns the seven additional HBAs as equally as possible, with four assigned to the adapter on fabric A, and the remaining three assigned to the adapter on fabric B.

e) Select **NEXT** to continue.

5. Optional: On the **Add Storage Volumes** page, specify the size and type of each volume to be added to any storage groups that are created through this template.

   This page initially contains a table heading with controls for defining a volume. The table columns vary, depending on the type of storage group (FCP or FICON) that you are creating. As you add volumes, the table is populated with a table row for each volume. Volumes of the same size are grouped into one expandable and collapsible row, with the total number of volumes in the group shown to the left of the table row. Use the arrow next to the total number to expand or collapse the table row. The table footer indicates the total size of the storage group, as you add or delete volumes.

   Steps to define volumes for an FCP storage group

   a. To specify the capacity of the volume, enter a number in the **Gibibytes** field or click the up or down arrows to increase or decrease the amount of gibibytes (GiBs).

   b. For Type, select either **Data** or **Boot**. Select **Boot** only if this volume is to contain bootable programs, such as the image of the operating system to be installed in a partition. You can specify only one type for each volume, but you can define more than one volume of each type for the storage group.

   c. Optional: Enter a description of this volume.

   d. Optional: If you want to duplicate this volume definition, specify the number of copies by typing a number in the **Copies** field or clicking the up or down arrows to increase or decrease the number.

   e. Select **ADD** to add this volume and its copies, if any. Details about the newly added volumes are displayed in a scrollable table, along with a footer that indicates the total number of volumes added and total amount of GiBs. If you added multiple volumes of the same size and type, they are grouped in a collapsible row. You can edit any of the table entries.

   f. Repeat this process, as necessary, to define all of the volumes that you want to add to the storage group. If necessary, you can delete any volume from the table by selecting the trash can icon.

   g. When you have finished defining volumes, select **NEXT** to continue.

   Steps to define volumes for a FICON storage group

   a. For Model, select one of the predefined models or Custom (EAV), depending on the size of volume that you want for the storage group. If you select a model, DPM automatically fills in the appropriate value for the Gibibyte and Cylinders fields.

   b. If you selected Custom (EAV) for the model, enter one of the following amounts:

      - The amount of GiBs in the Gibibyte field (DPM automatically calculates and displays the corresponding cylinder amount in the Cylinders field).
      - The amount of cylinders in the Cylinders field (DPM automatically calculates and displays the corresponding GiBs amount in the Gibibyte field).

c. For Type, select either **Data** or **Boot**. Select **Boot** only if this volume is to contain bootable programs, such as the image of the operating system to be installed in a partition. You can specify only one type for each volume, but you can define more than one volume of each type for the storage group.

d. Optional: Enter a unique, four-digit hexadecimal device number in the range 0000 - ffff for this volume; otherwise, DPM automatically assigns a device number when the storage group is first attached to a partition. The suggested practice is to have DPM automatically assign device numbers to avoid conflicts.

e. Optional: Enter a description of this volume.

f. Optional: If you want to duplicate this volume definition, specify the number of copies by typing a number in the **Copies** field or clicking the up or down arrows to increase or decrease the number.

g. Select **ADD** to add this volume and its copies, if any. Details about the newly added volumes are displayed in a scrollable table, along with a footer that indicates the total number of volumes added and total amount of GiBs. If you added multiple volumes of the same size and type, they are grouped in a collapsible row. You can edit any of the table entries.

- If you selected Custom (EAV) but you change the Gibibytes or Cylinders field to a value that exactly matches the size of a predefined model, Custom (EAV) remains the Model value unless you explicitly change it.
- If you requested copies of this volume, DPM assigns device numbers in sequential order. For example, if you entered 1057 for the volume and requested four copies, the assigned device numbers are 1057, 1058, 1059, 105A, and 105B. You can edit these values, if necessary. Note that, to avoid any numbering conflicts, DPM might change these device numbers later, when the storage group is attached to a partition.

h. Repeat this process, as necessary, to define all of the volumes that you want to add to the storage group. If necessary, you can delete any volume from the table by selecting the trash can icon.

i. When you have finished defining volumes, select **NEXT** to continue.

6. On the **Confirm Template** page, review the summary of your template.

   If necessary, select **EDIT** to change the attributes, name, description, or volumes. When you have finished, select **FINISH**.

Results

DPM creates the template, which is displayed in tile format on the **Request Storage**, **Create Storage Group**, or **Manage Templates** pages. The selectable template tile includes the name, description (if any), attributes, size in GiB, and the date on which the template was created.

What to do next

- Select the **Create Template** (plus) icon to create more templates. When the display includes multiple templates, you can sort them by name and by date (on which the template was created or modified). Users with system administrator authority also have the option of sorting templates by frequency of use.
- To modify a template, select the template menu (three vertical dots on the template tile), and select **Edit Template**.
- To delete a template, select the template menu (three vertical dots on the template tile), and select **Delete Template**.
- To use a template to create and submit a storage request, see the instructions in "Request or create a FICON or FCP storage group" on page 560.

Optimize 2nd level virtualization and share the same FCP disks across partitions

When you request storage for partitions to use, you can select the **Optimized for 2nd level virtualization** attribute when you want to enable the direct assignment of host bus adapters (HBAs) so an operating system or its guests can access an FCP storage group. Although the controls in the **Configure Storage**

task allow you to select this attribute only for a dedicated (not shared) FCP storage group, you can optimize 2nd level virtualization for separate partitions so they can share the same storage disks.

For example, suppose that you have created two partitions, ZVM1 and ZVM2, in which you plan to install z/VM to host multiple Linux images, and you want both of these partitions to share the same set of 10 storage volumes. To accomplish this goal, you need to request two different FCP storage groups, and request that your storage administrator configure the same logical unit numbers (LUNs) in the storage controller for the two storage groups. To do so, perform the following steps.

1. Open the **Configure Storage** task and, depending on your user ID authorization, select either **REQUEST STORAGE** or **CREATE STORAGE GROUP**.
2. On the **Specify Storage Attributes** page, define the attributes for the storage group.
   - For **Type**, select FCP.
   - For **Shareability**, select Dedicated.
   - For **Connectivity**, specify the number of paths to be available for use by each operating system with access to this storage group.
   - Select **Optimized for 2nd level virtualization**, and specify the number of additional connections (HBAs) that can be assigned directly to the operating system or its guests.

   Select **NEXT** to continue.
3. On the **Add Storage Volumes** page, specify the capacity and type of volumes that you require. For this example, define 10 storage volumes. When you have finished defining the volumes, select **NEXT** to continue.
4. On the **Name and Duplicate** page:
   a. Provide a name for the first storage group; for example, FCP-STORAGE-1.
   b. Enter 1 as the number of duplicates and select **DUPLICATE**.
   c. Provide a unique name for the second storage group; for example, FCP-STORAGE-2.
   d. Select **NEXT** to continue.
5. On the **Confirm** page, review the summary of your storage request; then select **NEXT** to continue.
6. Review the automatically generated storage request, and add instructions for the storage administrator to configure the same logical unit numbers (LUNs) in the storage controller for both storage groups. Then send it to one or more storage administrators for fulfillment.

   For FCP storage groups, DPM periodically checks for the requested volumes, and updates their fulfillment status on the **Storage Overview** tab of the **Configure Storage** task. When the storage administrator completes the configuration through tools for managing storage subsystems, DPM changes the storage group status to Complete.
7. Attach the storage groups and start the partitions. Note that you can perform these tasks before the storage groups are fulfilled.
   a. Open the **Partition Details** task for partition ZVM1, and go to the **Storage** section to attach FCP storage group FCP-STORAGE-1. Save your changes and close the task.
   b. Open the **Partition Details** task for partition ZVM2, and go to the **Storage** section to attach FCP storage group FCP-STORAGE-2. Save your changes and close the task.
8. Use the **Start** task to start the ZVM1 and ZVM2 partitions.

Manage tape libraries
Use **REQUEST TAPE LINK** or **CREATE TAPE LINK** to view information about the tape libraries that are connected to this system. You can also use this task to send zoning instructions to storage administrators to start initial zoning, to update zoning, or to remove FCP tape libraries from the DPM environment. To manage tape libraries, you can use the default SYSPROG, STORAGEADMIN, or SERVICE user IDs, or any user IDs that an access administrator has authorized to this task through customization controls in the **User Management** task.

The **Request tape link** or **Create tape link** page displays the FCP tape libraries table, which lists any tape libraries that DPM has discovered in the SAN. Above this table, the display includes either descriptive text or a time stamp indicating the last time, if any, that DPM discovered any correctly zoned FCP tape libraries. For discovered tape libraries, the table includes the tape library name (serial number), model, and state.

To display the table actions, select the ellipsis (•••) in the table header.

Start initial zoning
If the Tape libraries table is empty, select **Start initial zoning**, which causes DPM to generate an email with initial zoning instructions for a storage administrator. The instructions include the system management world wide port name (WWPN), which is a dedicated host WWPN that does not enable access to data in the tape library; its sole purpose is to enable DPM to discover (or detect) tape libraries in the SAN.

The instructions tell the storage administrator to complete the following zoning tasks in fabrics (switches) for *each* tape library to be connected to the system.

- Zone the system management WWPN with the target WWPN of at least one tape drive in the tape library.
- Configure the tape drive associated with the target WWPN as a control path.

When the initial zoning is complete, the time stamp and table content are updated.

Discover libraries
If the Tape libraries table has entries but does not list a specific tape library that you want find, or the time stamp is not recent, select **Discover libraries** to cause DPM to perform a one-time check of the current connections to tape libraries in the SAN. Depending on the number of system adapters that are defined as FCP storage adapters, and the number of target ports that are currently zoned, this discovery check could take some time.

Discover libraries is not available for selection until an administrator either requests initial zoning or requests a new tape link. When the **Discover libraries** check completes, the time stamp and table content are updated.

Available
At least one physical path reaches the tape library. (Note that you cannot delete a tape library that is in this state.)

Not available
No physical path, including the system management WWPN path, reaches the library. This state usually indicates a tape library that was correctly zoned and used for one or more tape links, but is no longer connected.

Remove libraries
To delete a tape library that you no longer want to use in your environment, use the following suggested procedure.

1. Delete all of the tape links that use the specific tape library. To delete tape links, you must use the default SYSPROG user ID or an equivalent user ID with the same permissions.
   a. To quickly find a list of the tape links that you need to delete, go to **STORAGE OVERVIEW**, and sort the Tape links table rows by the value in the LIBRARY column.
   b. For each tape link to be deleted, check the **Tape Link details** page to determine whether any active partitions have attached the tape link. If so, use the **Stop** task to stop the active partitions.
   c. Select the **Delete** icon on the **Tape Link details** page to delete the tape link. The time required to successfully delete the tape link depends on the number of partitions that have attached the tape link.
   d. Return to **STORAGE OVERVIEW**.

2. Select **REQUEST TAPE LINK** or **CREATE TAPE LINK** and use the **Remove libraries** action in the FCP tape libraries table to switch into table-edit mode. In this mode, a trash can icon is added to each table row.
3. Select the appropriate trash can icon to remove one or more tape libraries, and select **Save**. This action not only removes the table rows for the deleted tape libraries, but also results in an automatically generated email that contains instructions for a storage administrator to unzone the deleted libraries, including the system management WWPN.

Console Default User Settings

Accessing the User Settings task

Notes:

- If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the **Configure Data Replication** task.
- Only a user ID assigned access administrator roles sets the defaults of the Hardware Management Console settings by using the **Console Default User Settings** task.
- Because there are many main users interfaces (one for each logged on user), the Hardware Management Console provides each user the ability to change settings. In other words, if you change confirmation settings or controls, this does not cause that same change for other logged-on users.

This task enables you to customize settings that control how the Hardware Management Console operates. You can choose settings such as: single object selection, show tips, or choose when to display or not display confirmation windows.

User Settings

Use the **User Settings** task to customize settings that control how you want the console to operate for your user ID.

User Settings tabs

Use these tabs to control how you want the console to operate for your user ID.

“Confirmations” on page 629
To customize your preferences for using confirmation windows for a subset of console workplace tasks, select the **Confirmations** tab.

“Controls” on page 630
To select the object controls that you prefer, select the **Controls** tab.

Additional options are available from these pages:

Apply
To save the settings currently displayed on this tab, click **Apply**.

Reset
To discard any changes you made to the settings on this tab, and display again the current settings for this window, click **Reset**. If changes have been saved by clicking **Apply**, you can no longer discard the changes.

Defaults
To return to the preferences on this tab to the settings that are the default for the current user, click **Defaults**.

Note: If you are using this option from the **Console Default User Settings** task, then you are returning to the preferences on this tab to the settings that are the system default for all users.

OK
To save the settings on all tabs, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Confirmations

Use this page to customize preferences for using confirmation windows for a subset of tasks.

The preferences you set for using confirmation windows apply to the following subset of tasks:

- Activate
- Deactivate
- Load
- PSW Restart
- Reboot Support Element
- Remove Object Definition
- Reset Clear
- Reset Normal
- Single Object Operations
- Start All Processors
- Stop All Processors

You can customize the console for displaying a confirmation window upon starting any of the tasks listed above. A confirmation window identifies the task and, optionally, lists the task's target objects. The console operator must use a confirmation window either to confirm starting the task or to cancel it instead.

Confirmation windows reduce the possibility of inadvertently performing tasks, particularly tasks that may disrupt the operation of the Central Processor Complex (CPC) or its images.

Customize the settings to indicate your preferences, then click **Apply**.

Enabled with object list
To display a confirmation window upon starting any of the tasks listed above and to list the task's target objects, select **Enabled with object list**.

Note: The **Load** task does not support this option.

Enabled without object list
To display a confirmation window upon starting any of the tasks listed above, but without listing the task's target objects, select **Enabled without object list**.

Do not show confirmations
To start the tasks listed above without displaying confirmation windows, select **Do not show confirmations**.

Use 'No' as the default action
To set the confirmation window's default action to 'No' upon starting any of the tasks listed above, select **Use 'No' as the default action**.

- If this is selected (a check mark appears) it indicates the default action for the confirmation window is to cancel the task. That is, the **No** button is preselected on the confirmation window, click **No** to cancel the task.

- If this is not selected (a check mark does not appear) it indicates the default action for the confirmation window is to confirm starting the task. That is, the **Yes** button is preselected on the confirmation window, click **Yes** to confirm starting the task.

Controls

Use this page to select the object controls to use on the console.

Single object selection
To select only one object at a time while working on a task, select **Single object selection**. Otherwise, more than one object can be selected while working on a task.

Show tips each time you logon
To display different console facts or tips each time you log on, select **Show tips each time you logon**.

Accept Console Messenger messages
To allow your console sessions to receive Console Messenger chat and broadcast messages, select **Accept Console Messenger messages**. Otherwise, your sessions will not receive these messages, and other sessions attempting to initiate chats with your session will be told that you have elected not to participate in chats.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task.

Bring Chat Window to foreground on new message
The initial chat message window is always displayed in the foreground to notify you of the incoming chat message.

To have the Console Messenger task continue to bring an open chat message window to the foreground after the initial message is received, select **Bring Chat Window to foreground on new message**.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task.

Display timestamps using
To define the time zone that is used to localize timestamps, for those tasks that use timestamps. Select the drop-down arrow to choose your preference.

Notes:

- This is only available for those tasks that are enabled to respect this timestamp setting.
- From the **User Settings** task, if you change your preference and apply this change, a message appears indicating you must restart your login session before the change appears.

Client Time Zone
To display timestamps localized to the time zone of the client browser, select **Client Time Zone**. If you are on a local session, this is the same as the Console Time Zone.

Console Time Zone
To display timestamps localized to the time zone of the Hardware Management Console, select **Console Time Zone**. This is the default. If you are on a local session, this is the same as the Client Time Zone.

UTC Time Zone
To display timestamps localized to the UTC time zone, select **UTC Time Zone**.

Console Default User Settings

Use the **Console Default User Settings** task to set the default settings for operating the console.

Only the ACSADMIN default user ID or a user ID with access administrator roles can access this task.

This task will not affect currently logged on users until they log off then log back on.

Console Default User Settings tabs

Use these tabs to set the defaults for controlling how the console operates for all users.

"Confirmations" on page 629
To set preferences for using confirmation windows for a subset of console workplace tasks, select the **Confirmations** tab.

"Controls" on page 630
To set the object controls, select the **Controls** tab.

Additional options are available from these pages:

Apply
To save the settings currently displayed on this window, click **Apply**.

Reset
To discard any changes you made to the settings on this window, and display again the current settings for this window, click **Reset**.

Defaults
To return to the preferences that are the default for the current user, click **Defaults**.

OK
To save the settings, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Console Messenger

Accessing the Console Messenger task

Note: To send messages using this task, you must enable **Console messenger** from the **Customize Console Services** task. Enabling **Console messenger** also allows you to receive messages. The **Accept Console Messenger messages** and **Bring Chat Window to foreground on new message** options become available from the **Controls** tab of the **User Settings** task to allow you to customize the way that this task operates for your user ID.

This task is used to provide a simple person-to-person message communication facility between users of the Hardware Management Console and the Support Element.

You can send a broadcast message or you can initiate a two-way chat.

Sending a broadcast message

This function allows you to send the same information to all the users on a console at the same time. To send a broadcast message:

1. Open the **Console Messenger** task. The Console Messenger window is displayed. This window allows you to choose the console or user that you want to send a message to and whether or not you want to send a two-way chat or send a broadcast message.
2. To send a broadcast message, select a top level console from the ***Reachable Consoles*** tree view list section of the window and make sure **Broadcast** is displayed in the ***Message Type*** section of the window.

   If you select a top level console from ***Reachable Consoles*** that is a Support Element, the ***Message Type*** displays **Broadcast** and an additional option, **In addition, send the message to all managing consoles.**, is displayed. This option controls the distribution of the message. Broadcast messages are always sent to all of the users on the selected console. However, if you select this option the broadcast message is also sent to all users on all Hardware Management Consoles that are acting as managing

consoles of the Support Element. This option is not available when the selected console is a Hardware Management Console.

3. Click **OK**. The Send Broadcast Message window is displayed.

   This window indicates who the recipient of your message will be and includes a message area for you to provide information that will be sent to all other user sessions (logged on and disconnected) of the selected console.
4. Specify a message in the **Message** input field, then click **Send**. The Broadcast Message Sent window is displayed indicating whether or not your message was received successfully.
5. Click **Close** to return to the Hardware Management Console workplace.

If you are receiving a broadcast message, the Broadcast Message Received window is immediately displayed on your Hardware Management Console screen. This window identifies the user that sent the message and displays the message sent by the user.

From this window you can:

- View more information about where the message came from, click **view more info**.
- Begin a two-way chat session with the user session that sent the broadcast message, click **Initiate® Chat**.
- End the task and return to the Hardware Management Console workplace, click **Close**.

Initiating a two-way chat

This function allows you to send a message to an individual user. To initiate a two-way chat:

1. Open the **Console Messenger** task. The Console Messenger window is displayed. This window allows you to choose the console or user you want to send the message to and whether or not you want to send a two-way chat or send a broadcast message.
2. To send a two-way chat, select an individual user session located below the reachable console. This automatically changes the ***Message Type*** area to **Two-way Chat**, then click **OK**. The Console Messenger Chat window is displayed.

   This window indicates who you will be sending messages to, a history of the dialogue you will be having with your chat partner, and a message area for you to provide information that will be sent to your chat partner.
3. Specify a message in the **Message** input field, then click **Send**. The Console Messenger Chat window is refreshed with the message you entered now appearing in the **History** area of the window with the prefix **Me**.

   The message is sent to the partner and their Console Messenger Chat window is also refreshed, with the message text appearing in the **History** area with the prefix **Partner** added to it.
4. If both partners need to continue sending messages to each other, specify a message in the **Message** input field and click **Send**.

   Note: To ensure the chat window comes to the foreground in your Hardware Management Console sessions when partners send you messages, select **Bring chat window to foreground on message arrival.** (a check mark appears).
5. When you are done conversing with your chat partner, click **Close**.

   Note: The **Status** for your chat partner changes to **Closed by partner** and the **Send** option is no longer enabled, indicating that you have closed the Console Messenger Chat window.

There are other Hardware Management Console tasks, such as the **Users and Tasks** task, that offer an ability to open the **Console Messenger** task to start a two-way chat or send a broadcast message. The steps necessary to open the **Console Messenger** task from these other tasks is mentioned in the description of those tasks. Once the **Console Messenger** task has been opened, continue with the steps described in this section for information on the procedure for sending a broadcast message or conducting a two-way chat.

Console Messenger

This task is used to provide a simple person-to-person message communication facility between users of the Hardware Management Console and Support Element.

Note: To initiate this task you must enable **Console messenger** from the **Customize Console Services** task and **Accept Console Messenger messages** must be selected from the **Controls** tab of the **User Settings** task to be able to receive messages.

Instances of this task will also be started automatically in a user's session in order to participate in a two-way chat requested by another user, or to display a broadcast message sent by another user.

Use this window to select the console and user session you want to interact with and what type of interaction is appropriate: a two-way chat or a one time broadcast message.

A console user is able to send messages to users on:

- The same console
- Any console that is known to the **Configure Data Replication** task
- Any console that is acting as this console's call-home server
- Any console that this console has discovered and that is in the same domain
- Any Support Element that is being managed by this console.

Reachable Consoles and Message Type

The list of reachable consoles is displayed in a two-level tree view format. The top level of the tree (indicated by the +/- expansion box) contains an entry for each of the reachable consoles (console nodes) that have been identified by this task. The next level in the tree view displays the list of user sessions (either logged on or disconnected) that were running on the console at the time this window was displayed.

Note: A disconnected session is displayed in red and a logged on user is displayed in green. Messages can be sent to disconnected users.

Current Console
Represents the console from where the task is being initiated. It is always displayed at the top of the tree view.

User Session
Appears below the console node and consists of the user's user ID followed by the location from which they initiated the console session.

Selecting from the reachable consoles list determines whether a two-way chat or broadcast message will be initiated. The **Message Type** area changes dynamically according to the selection you have made in the **Reachable Consoles** tree view.

Two-way Chat
Selecting a user session begins a two-way chat with the selected logged on user.

Broadcast
Selecting a console node sends a broadcast message to all of the logged on users of the selected console.

To send a broadcast message to all of the users on any other console that also acts as a managing console for the selected console, select **In addition, send the message to all managing consoles.** Otherwise, the broadcast message is just sent to the users on the selected console node. This option may not be available if the selected console entry does not represent a console that is not managed by others.

Note: There is a possibility that some of the managing consoles may not receive the broadcast message. When you send the broadcast message the **Omitted Consoles** window is displayed. This window lists the managers of the selected consoles that do not have the console messenger facility enabled, therefore those consoles would not receive the message. You can decide whether or not to

proceed with the message. **Yes** continues with the message, otherwise **No** cancels sending the message.

Note: The data for the list of available console nodes is obtained when this window is first displayed and is not refreshed. To refresh this data you must cancel the task and re-open it. Also, if the console node is expanded you can refresh that node by collapsing and then re-expanding the node.

Additional options on this window include the following:

OK
To initiate the two-way chat or broadcast message, click **OK**.

Cancel
To exit this task without sending any messages, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Console Messenger Chat

Use this window to engage in a two-way chat with a selected partner, sending messages to the partner and seeing the messages sent by the partner.

Chat Partner
This area of the window displays your chat partner's user ID and the current chat partner session status. The session status information is updated dynamically as it changes. Session status information can be one of the following:

Logged on
Chat session is open and your chat partner is currently logged on.

Disconnected
Chat session is open but your chat partner has disconnected their browser from the console session. The chat session is available for use and your chat partner will see the new messages when they reconnect to the console session.

Closed by partner
Chat partner has closed the chat session. This window remains open for you but new messages cannot be sent.

Partner is no longer reachable
Chat session has been closed because some communication interruption has made message delivery to the chat partner unavailable. This window remains open but new messages cannot be sent.

To see additional information about your chat partner, click **view more info**. The **Chat Partner** area is expanded to display the full user ID and additional console session information, such as start time and the internal session ID. You can restore this area to its original display by clicking **close**.

History
This area of the window is a scrollable text output area that provides a running transcript of the chat session. It displays the messages that you sent, along with the messages that have been received from your chat partner.

The entries in the history area are prefixed with an indication as to who sent the message and the local time the message was sent or received. The prefix is one of the following:

Me
Represents messages that you sent and initiated.

Partner
Represents messages that are received from your chat partner.

The messages are displayed in different colors to allow for easy identification.

In addition to message entries, this area includes marker lines that associate dates with the entries in the history. A date (and time) marker line is placed at the top of this area to record the date on which the chat session started. Additional marker lines are placed in this area any time the history spans a date change boundary, such as crossing midnight.

Message
This area of the window is the input area where you specify the message you want sent to your chat partner.

To send the message to your chat partner you can either, click **Send** or press **Enter**.

Note: The Message area is disabled if the status of your chat partner changes to **Chat Closed** or **Partner Not Reachable**.

Bring chat window to foreground on message arrival.
To bring this window into the foreground when a new message from your chat partner arrives, select **Bring chat window to foreground on message arrival.**

Send
To send the message that you specified in the **Message** input area to your chat partner, and to clear the input area for the next message, click **Send**.

Close
To close the chat and end this task click **Close**. A message is sent to your chat partner indicating the chat session has closed.

Help
To display help for the current window, click **Help**.

Send Broadcast Message

Use this window to send a message to the selected console node.

Recipient
This area of the window lists the console or consoles that the broadcast message is going to be sent. It will always list the name of the console node that you selected from the **Reachable Consoles** list. Also, if you selected the option to send the message to all managing consoles then those consoles would also be included.

Message

This area of the window is the input area where you specify the message you want sent to all of the user sessions on the consoles listed in the **Recipient** area.

To send the broadcast message, click **Send**.

Send
To send the broadcast message that you specified in the **Message** input area to all of the user sessions on the consoles listed in the **Recipient** area, click **Send**.

Once you have sent the message, the **Broadcast Message Sent** window is displayed. This window summarizes the results of sending the broadcast message. It lists the console names that successfully received the broadcast message and those consoles that did not (if applicable). This is an informational window, click **Close** when you have finished reviewing this information.

Cancel
To cancel sending the broadcast message and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Broadcast Message Received

You can use this window to view the message sent to your console or to respond to the message sent to your console.

From
This area of the window displays information about the user session that sent the broadcast message.

To see additional information about your user that sent the message, click **view more info**. The **From** area is expanded to display the location and additional console session information, such as start time and the internal session ID. You can restore this area to its original display by clicking **close**.

Message
This area of the window displays the contents of the broadcast message and the date and time the message was sent.

Initiate Chat
To begin a two-way chat session with the user session that sent the broadcast message, click **Initiate Chat**.

The **Console Messenger Chat** window is displayed.

Close
To close the window and end the task, click **Close**.

Help
To display help for the current window, click **Help**.

Copy Console Logs to Media

Accessing the Copy Console Logs to Media task

Note: You cannot perform this task remotely.

This task copies the Hardware Management Console log file (**IQYYLOG.LOG**) to a media device. You may want to do this for saving or archiving the log file.

To copy the log file to a media device:

1. Open the **Copy Console Logs to Media** task. Insert the media device that you want to copy the console logs to. The Select Media Device window is displayed.
2. Select the media device, then click **OK**.
3. Follow the instructions on the subsequent windows to complete the task.

Select Media Device

Use this window to select the device to which the Hardware Management Console log file will be copied to.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

OK
To continue the task with the selected media, click **OK**.

Refresh
To update the device list, click **Refresh**.

Cancel
To exit this task without making any device selections, click **Cancel**.

Help
To display help for the current window, click **Help**.

Create Welcome Text

Accessing the Create Welcome Text task

This task, used by an access administrator or a user ID that is assigned access administrator roles, allows you to customize the welcome message or display a warning message that appears on the Welcome window before you log onto the Hardware Management Console.

To create a message:

1. Open the **Create Welcome Text** task. The Create Welcome Text window is displayed.
2. Enter a message in the input field to be displayed in the Welcome window. You can also specify a label name in the **Classification** input field that will be displayed as the background on the Welcome and Logon windows.
3. Click **OK** to apply the change.
4. The next time you log on to the Hardware Management Console your message is displayed.

Create Welcome Text

This window is used to customize the welcome message or display a warning message that appears before users log onto the console.

The text that you enter in the message input area for this task will appear on the **Welcome** window after you initially access the console. You can, therefore, use this text to notify users of certain corporate policies or security restrictions applying to the system.

Automatically reflow text
To have the text formatted in the **Welcome** window in order to fit the width of the user's browser window, select **Automatically reflow text**. If you do not select this option the text is shown on the **Welcome** window just as you entered it in the message input area.

Message input area
Use this area to specify the text you want displayed in the **Welcome** window. You can specify a message or warning up to 8192 characters.

Clear
To remove the text that is currently appearing in the message input area, click **Clear**.

Classification:
You can, optionally, specify a short label describing the security classification of this system. For example, *Business Use Only*, *Top Secret*, or *Unclassified*. This label appears as part of the background on the **Welcome** and **Logon** windows.

OK
To proceed with the message or warning you specified in the message input area, click **OK**.

Reset
To return to the original text that appeared in the message input area, click **Reset**.

Cancel
To exit this task without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Cryptographic Configuration

Accessing the Cryptographic Configuration task

The Crypto Express are orderable features.

- The Crypto Express (CCA Coprocessor, EP11 Coprocessor, and Accelerator) features work with the Integrated Cryptographic Service Facility (ICSF) and the Resource Access Control Facility (RACF®) (or equivalent software products) in an z/OS or OS/390® operating environment to provide data privacy,

data integrity, cryptographic key installation and generation, electronic cryptographic key distribution, and personal identification number (PIN) processing.

- The cryptographic functions of the Crypto Express Accelerators provide:
  - SSL acceleration of modular arithmetic operations; mainly clear-key RSA private key decryption.
  - A function reduced, but performance enhanced alternative to the CCA Coprocessor and EP11 Coprocessor.
- The cryptographic functions of the Crypto Express Coprocessors provide:
  - Support for CCA (Common Cryptographic Architecture) APIs.
  - Support for AES, DES, and RSA cryptographic operations for data confidentiality, and data integrity and distributed key management.
- Using the cryptographic functions of the Crypto Express EP11 Coprocessor provides:
  - Support for Enterprise PKCS #11 (EP11) APIs.
  - Support secure PKCS #11 keys, keys that never leave the secure boundary of the coprocessor unless encrypted.

This task allows you to monitor the installed Crypto Express features by loading their configuration data during CPC activation. Upon completing the configuration and initialization of the installed Crypto Express features, you can monitor and manage it by:

- Checking the status and details of the Crypto Express features.
- Testing the random number (RN) generators of the Crypto Express CCA Coprocessor.
- Run Customer Initiated Selftest of the Crypto Express EP11 Coprocessor.
- Manually clear the cryptographic keys from the Coprocessor or Accelerator.
- Manually clear the cryptographic keys within the given usage domain(s).
- Import and activate a UDX file configuration.
- Indicate whether to permit TKE commands for processing on the selected Crypto Express CCA Coprocessor.
- Select the crypto configuration type for your system.

To work with the Crypto Express features:

Note: Depending on your user task role, you may only be able to view this task.

1. The Crypto Express features must be installed, and the CPC must be powered-on.
2. Open the **Cryptographic Configuration** task.

The Cryptographic Configuration window lists the Crypto Express features installed in the CPC and provides controls for working with them.

Cryptographic Configuration

Use this window to configure and monitor the Crypto Express features installed in your system. The Crypto Express features can be configured to operate as CCA Coprocessor, EP11 Coprocessor, or Accelerator.

Note: Depending on your user task role, you may only be able to view this task.

The Crypto Express features are secure, integrated hardware that perform high-speed cryptographic functions. Each Cryptographic adapter is identified by a cryptographic number, starting at 0. The cryptographic numbers that can be configured on the system can have an upper limit of 60, but could be smaller depending on your model.

Using the cryptographic functions of the Crypto Express Accelerators provide:

- SSL Acceleration of modular arithmetic operations; mainly, clear-key RSA private key decryption.

- A function reduced, but performance enhanced alternative to the CCA Coprocessor and EP11 Coprocessor.

Using the cryptographic functions of the Crypto Express CCA Coprocessors provide:

- Support for Common Cryptographic Architecture (CCA) APIs.
- Support for AES, DES, and RSA cryptographic operations for data confidentiality, and data integrity and distributed key management in a secure environment.

Using the cryptographic functions of the Crypto Express EP11 Coprocessors provide:

- Support for Enterprise PKCS #11 (EP11) APIs.
- Support secure PKCS #11 keys, keys that never leave the secure boundary of the coprocessor unless encrypted.

Using the cryptographic functions of the Crypto Express features require either:

- Activation of the partition with the crypto settings in your activation profile using the **Customize/Delete Activation Profile** task.
- Changing the crypto settings on the logical partition using the **Change LPAR Cryptographic Controls** task.

Use the Cryptographic Configuration window to start these tasks. You can use this window to perform tasks for configuring and monitoring the Crypto Express features:

- Checking the status and details of the Crypto Express features by clicking View Details....
- Testing the Random Number (RN) generator of the Crypto Express CCA Coprocessors by clicking “Test RNG/CIS” on page 641.
- Run Customer Initiated Selftest of the Crypto Express EP11 Coprocessor by clicking “Test RNG/CIS” on page 641.
- Manually clear the cryptographic keys from the Coprocessor or Accelerator by clicking Zeroize.
- Manually clear the cryptographic keys within the given usage domain(s) by clicking “Domain Management” on page 644.
- Indicate whether to permit TKE commands for processing on the selected Crypto Express CCA Coprocessors by clicking TKE Commands.
- Indicate the crypto type configuration for the Crypto Express features by clicking Crypto Type Configuration.
- Import and activate a UDX file configuration by clicking UDX Configuration.

Number
Displays the ID number assigned by the system to identify the Crypto Express features.

Status
Indicates the status of the Crypto Express feature card; such as, operating or deconfigured.

Crypto Serial Number
Displays the serial number of the crypto adapter contained in the Crypto Express features.

Type
Indicates whether the Crypto Express cryptographic card is configured to operate as a CCA coprocessor, EP11 coprocessor, or an accelerator.

Operating Mode
Displays the operating mode for the Crypto Express features.

TKE Commands
Indicates whether TKE commands are permitted or denied for the Crypto Express features

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Refresh
To update the displayed cryptographic configuration information with the current configuration, click **Refresh**.

Cancel
To exit the current task, click **Cancel**.

Help
To display help for the current window, click **Help**.

View cryptographic details

You can use the Support Element workplace to monitor the status of the Crypto Express features.

To view the status of the Crypto Express features:

1. Open the **Cryptographic Configuration** task in system programmer or service representative role..

   The Cryptographic Configuration window lists the Crypto Express features installed in the CPC and provides controls for working with them.

   Note: The Crypto Express features have completed its initialization when the status indicates *Configured*. After initialization is complete, you need to refresh the Cryptographic Configuration window. If initialization is ongoing, you may need to refresh the Cryptographic Configuration window to see the current status until *Configured* is indicated.
2. Select from the list the Crypto Express features that you want more information for.
3. Click **View Details**.

The Cryptographic Details window displays information on the selected Crypto Express features.

Test RNG/CIS

Use this task to:

- Verify whether the Random Number (RN) generated of the Crypto Express CCA Coprocessor are sufficiently random. Ordinarily, a RN generator is tested automatically when it is initialized, but you can use this task to manually test an RN generator. You can select to run a RN generator test on individually selected Crypto Express CCA Coprocessors or run a test on all Crypto Express CCA Coprocessors.
- Run a Customer Initiated Selftest of the Crypto Express EP11 Coprocessors.

To test a Crypto Express CCA Coprocessor or EP11 Coprocessors:

1. The Crypto Express CCA Coprocessors or EP11 Coprocessors must be online and assigned to a logical partition.
2. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   The Cryptographic Configuration window lists the Crypto Express features installed in the CPC, and provides buttons for working with them.

   To manually test specific Crypto Express CCA Coprocessors or EP11 Coprocessors:

   - Select from the list a configured Crypto Express CCA Coprocessors or EP11 Coprocessors that you want to test.
   - Click **Test RNG/CIS** to test them.

     A message is displayed to indicate the results of the test.

   To manually run the test on **all** Crypto Express CCA Coprocessors or EP11 Coprocessors:

   - Use the **Select All** function from the table icons or **Select Action** list from the table tool bar and to test all.

     A message is displayed to indicate the results of the test.

Zeroize Coprocessors or Accelerators manually

Zeroizing a Coprocessor or Accelerator for the Crypto Express features clear all configuration data and cryptographic keys by resetting them to binary zeroes.

Attention: Zeroizing one or all Coprocessors or Accelerators clears its configuration data and clears all cryptographic keys. Zeroizing all also erases configuration data from the Support Element hard drive (for example, UDX files). The selected Coprocessor or Accelerator should be zeroized manually only when absolutely necessary, typically when the Coprocessor or Accelerator configuration data must be erased completely.

For example:

- You must zeroize selected Coprocessors or Accelerators prior to selling or transferring ownership of the CPC.
- A service representative may zeroize Coprocessors or Accelerator prior to upgrading the CPC, if required.
- You may want to zeroize selected Coprocessors or Accelerators if, in an emergency, it is the only way to maintain the security of encrypted data.

To manually zeroize Crypto Express CCA Coprocessors or EP11 Coprocessors:

1. A power-on reset of the CPC must be complete.
2. The Crypto Express CCA Coprocessor or Crypto Express EP11 Coprocessor must be online and assigned to a logical partition.
3. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   This displays the Cryptographic Configuration window. The window lists the Coprocessors and Accelerators installed on the CPC, and provides controls for working with them.

To manually zeroize a specific :

- Select from the list the configured Coprocessor or Accelerator you want to zeroize.
- Click **Zeroize** to zeroize the selected Coprocessor or Accelerator.

  A Zeroize Warning window is displayed to notify you of the consequences for clearing the configuration data.
- Click **Zeroize** to confirm your request to zeroize the selected Coprocessor or Accelerator.

To manually run zeroize on all Coprocessors or Accelerators:

- Click **Zeroize All** to zeroize all the Coprocessors and Accelerators and erase configuration data from the Support Element hard drive.

  A Zeroize Warning window is displayed to notify you of the consequences for zeroizing all the Coprocessors and Accelerators.
- Click **Zeroize All** to confirm your request to zeroize them.

A message is displayed to indicate the results of the function.

Domain Management

Zeroizing a usage domain clears the cryptographic keys for a selected logical partition by resetting them to binary zeroes.

To zeroize a logical partition usage domain:

1. A power-on reset of the CPC must be complete.
2. The Crypto Express CCA Coprocessor or EP11 Coprocessor must be online and assigned to a logical partition.
3. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   This displays the Cryptographic Configuration window. The window lists the Crypto Express CCA Coprocessors or EP11 Coprocessor installed in the CPC, and provides controls for working with them.

   To zeroize a usage domain:

   - Select from the list the configured Coprocessor you want to zeroize.
   - Click **Domain Management**.

     A Domain Management window is displayed
   - Select the usage domain index(es) to zeroize.
   - Click **Zeroize** to confirm your request to zeroize the selected usage domain indexes.

   A message is displayed to indicate the results of the function.

TKE commands

The TKE workstation can manage secure functions of a specific Crypto Express CCA Coprocessors only if permission is given. If permission is denied, all requests for information or commands to a specific Crypto Express CCA Coprocessors from the TKE workstation will not be allowed. You can use the Support Element to dynamically permit or deny TKE commands to the Crypto Express CCA Coprocessors from the TKE workstation.

Note: Permitting TKE access with the default TKE communication keys set can allow unauthorized access. For security reasons you should immediately change the default value of the keys from the TKE.

To permit or deny TKE commands:

1. The Crypto Express CCA Coprocessors must be online and assigned to a logical partition.
2. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   The Cryptographic Configuration window lists the Crypto Express CCA Coprocessors installed in the CPC and provides controls for working with them.

3. Select from the list the Crypto Express CCA Coprocessors that you want to view or modify TKE command permission.
4. Click **TKE Commands**.

   The TKE Commands Configuration window displays information on the TKE commands for the selected Crypto Express CCA Coprocessors.
5. Select the Crypto Express CCA Coprocessors to permit or deny TKE commands. The check box displays a check mark when you mark it.
6. **Permit**
   To permit TKE commands, click **Permit**.

   Deny
   To deny TKE commands, click **Deny**.

Crypto type configuration

The selected Crypto Express (CCA Coprocessors, EP11 Coprocessors, and Accelerators) features can be configured to run as an accelerator or coprocessor. The selected Crypto Express features must be deconfigured prior to changing the crypto configuration type.

Note: The TKE Workstation is required for key management of the Crypto Express EP11 Coprocessors.

If you select **Accelerator**, you can zeroize the selected Crypto Express CCA Coprocessors by indicating **Zeroize the Coprocessor** on the Crypto Type Configuration window.

To select a crypto type configuration:

1. A power-on reset of the CPC must be complete.
2. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   The Cryptographic Configuration window lists the Crypto Expres features installed on the CPC and provides controls for working with them.
3. Select from the list the Crypto Express features that you want to change the crypto type configuration.
4. Click **Crypto Type Configuration**.

   The Crypto Type Configuration window displays information on the selected Crypto Express features.
5. Select a configuration type for the Crypto Express features.
6. Zeroize the Crypto Express CCA Coprocessors when selecting an Crypto Express Accelerator crypto type.
7. Click **Apply** to change the crypto type configuration.

UDX configuration

Use the UDX Configuration to add customized operations to the selected Coprocessor installed on your system. The UDX configuration provides the capability to develop your own UDX Segment 3 image file and load your custom Segment 3 image file onto one or more Coprocessors. To view the Segment 3 details, click **View Details** on the Cryptographic Configuration window. The Segment 3 image file is built and loaded onto a removable media using a xSeries server workstation. For more information on building a UDX Segment 3 image file go to the following website at:

- Crypto cards (www.ibm.com/security.cryptocards)
- Click on Library on the navigation bar.

Note: The recognized file name for the UDX file is *.CCA.UDX.

To configure for User Defined Extension (UDX):

1. The selected coprocessors must be installed, and the CPC must be power-on reset to activate the UDX configuration. Otherwise, to import a UDX file:
2. Open the **Cryptographic Configuration** task.

The Cryptographic Configuration window lists the coprocessors installed on the CPC and provides controls for working with them.

3. Select the Coprocessor to configure for UDX.
4. Click **UDX Configuration** to configure the coprocessor for UDX configuration.

   The UDX Configuration window displays detailed information for the coprocessor configured for UDX capability and provides controls for working with them.
5. Click **Import From Media** to import the UDX configuration file from the removable media to the Support Element hard drive.
6. Click **Import From FTP Server** to import a secure FTP location.
7. Click **Activate** to load the UDX configuration data to the selected Coprocessor.

Zeroize

This window cautions that you are about to clear the cryptographic keys from the selected Coprocessor(s) or Accelerator(s). Use the window's controls to confirm or cancel your request to zeroize the Coprocessor(s) or Accelerator(s).

Important: When **Zeroize** is selected on this window, you must re-enter the selected Coprocessor(s) or Accelerator(s) key data to re-enable cryptographic operations.

Zeroizing the selected Coprocessor(s) or Accelerator(s) clears the cryptographic keys from the Coprocessor(s) or Accelerator(s) hardware data by resetting it to binary zeros.

Note: The selected Coprocessor(s) or Accelerator(s) should be zeroized manually only when absolutely necessary, typically the Coprocessor(s) or Accelerator(s) must be cleared immediately.

- You must zeroize selected Coprocessor(s) or Accelerator(s) prior to transferring ownership of the Coprocessor(s) or Accelerator(s) hardware.
- In an emergency, you may want to zeroize selected Coprocessor(s) or Accelerator(s) to maintain the security of encrypted data.

Additional functions on this window include:

Zeroize
To only clear cryptographic keys from the cards specified, click **Zeroize**.

Cancel
To exit the current task, click **Cancel**.

Domain Management

This window allows you to clear the cryptographic keys within the given usage domain(s). When a crypto with the given associated usage domains are removed from a partition, this partition no longer has access to the cryptographic keys. If this crypto is assigned to a different partition utilizing the same usage domains as before, this new partition has access, possibly unintentional access, to the cryptographic keys. Therefore, when a crypto is removed from an active partition, the Usage Domain Zeroize window displays, providing the opportunity to clear the cryptographic keys within the given usage domain(s).

Cryptographic number
Displays the crypto umber assigned to the selected crypto

Cryptographic status
Displays the current state for the selected crypto

Cryptographic type
Displays the Crypto Express feature type.

Usage domain index table

Usage domain index
Displays the number associated with the usage domain

Partition Name
Displays the partition name the crypto is in

Crypto State
Displays the cryptos current state in the partition

Compliance mode
Displays the current standard compliance of the cryptos. Compliance mode returns to default after zeroize of card, zeroize of domain, activation of UDX, and removal of UDX from Segment3.

CCA compliance levels (Crypto Express6S)
Non-compliant (default)

PCI-HSM 2016

PCI-HSM (migration)

EP11 compliance levels (Crypto Express6S and 5S)
FIPS, 2009

BSI, 2009

FIPS, 2011

BSI, 2011

BSI, 2017 (Crypto Express6S only)

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Zeroize
To clear cryptographic keys within the given usage domain(s), click **Zeroize**.

Cancel
To exit the current task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Zeroize All

This window cautions that you are about to clear the cryptographic keys from all Coprocessors or Accelerators and delete the UDX file. Use the window's controls to confirm or cancel your request to clear the cryptographic keys from all Coprocessors or Accelerators.

Note: When **Zeroize All** is selected on this window, you must re-enter the Coprocessors or Accelerators key data to re-enable cryptographic operations.

Zeroizing All Coprocessors or Accelerators deletes the configuration data and clears the cryptographic keys for all Coprocessors or Accelerators by resetting it to binary zeroes. This includes clearing cryptographic secure keys, configuration data, and any other secure hardware data.

Note: The Coprocessors or Accelerators should be zeroized manually only when absolutely necessary, typically when coprocessor configuration data must be erased immediately. For example:

- You must clear the cryptographic keys for all Coprocessors or Accelerators prior to selling or transferring ownership of the Coprocessors or hardware.
- You may want to clear the cryptographic keys for all the Coprocessors or Accelerators to maintain the security of encrypted data.

Additional functions on this window include:

Zeroize All
To clear all cryptographic keys from the cards and delete configuration data from the system, click **Zeroize All**.

Cancel
o close the window without clearing cryptographic keys from all Coprocessors or Accelerators, click **Cancel**.

Cryptographic Details

This window displays detailed information about an installed Crypto Express feature.

Number
Displays the ID number assigned by the system to identify the Crypto Express features.

PCHID
Displays the Physical Channel Identifier (PCHID) assigned to the Crypto Express features.

Status
Indicates the status of the Crypto Express feature card; such as, operating, deconfigured, or installed.

Type
Indicates whether the Crypto Express cryptographic card is configured to operate as a CCA coprocessor, EP11 coprocessor, or an accelerator.

TKE commands
Indicates whether TKE commands are permitted or denied for the selected Crypto Express CCA Coprocessors.

Card location
Displays the physical location of the card in the frame.

Card serial number
Displays the serial number of the Crypto Express features plugged into the specified card location.

Crypto serial number
Displays the serial number of the crypto adapter contained in the Crypto Express features.

Crypto part number
Indicates the crypto part number for the crypto adapter contained in the Crypto Express features.

FPGA version
Indicates the crypto Field Programmable Gate Array (FPGA) version for the crypto adapter contained in the Crypto Express features. The version is programmable and can be changed by firmware updates.

ASIC version
Indicates the crypto ASIC version for the selected Crypto Express features. The version is programmable and can be changed by firmware updates.

Card version
Indicates the crypto card version for the crypto adapter contained in the Crypto Express features. The card version is programmable and can be changed by firmware updates.

Segment 1 image information

Segment 1 is an area of the selected Crypto Express feature that holds self-testing code (POST) which ensures the card is operating properly, and code that supports the secure update of firmware in Segments 1, 2, and 3.

Name
Displays the name that was specified when the image was built.

Hash Data
Uniquely identifies the image in Segment 1.

Segment 2 image information

Segment 2 is an area of the selected Crypto Express feature that holds the operating system for the card, as well as a small amount of self-testing code (POST) code which ensures the card is operating properly.

Name
Displays the name that was specified when the image was built.

Hash Data
Uniquely identifies the image in Segment 2.

Segment 3 image information

Segment 3 is an area of the Crypto Express feature that holds the Common Cryptographic Architecture (CCA) application code. This is also the area where a User-Defined Extension (UDX) image would reside, if a UDX Image was activated. If a UDX image is not activated, then the Default image resides in the Segment area. A UDX is a customized version of the CCA code containing specialized functions.

Operating Mode
Describes the type of image activated in the Segment 3, either UDX or the Default. If the selected Crypto Express features are deconfigured, the UDX status indicates *Not available*. This UDX image is imported from a USB flash memory drive or DVD using the UDX Configuration option.

Timestamp
Indicates the time stamp indicating when the UDX image or default image in Segment 3 was created.

Name
Displays the name that was specified when the image was built.

Hash Data
Uniquely identifies the image in Segment 3.

Number of concurrent internal code changes since last hardware reset
Displays the number of concurrent internal code changes for the selected Crypto Express feature since the last hardware reset.

Additional functions on this window include:

Close
To close the window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

TKE Commands Configuration

Use this window to indicate whether you want TKE commands permitted or denied for the selected Crypto Express CCA Coprocessors. The TKE workstation manages secure functions of the selected Crypto Express CCA Coprocessors only when permission is given. If permission is denied, all requests for information or commands to the selected Crypto Express CCA Coprocessors from the TKE workstation is denied.

Note: Permitting TKE access with the default TKE communication keys set can allow unauthorized access. For security reasons the user should immediately change the default value of the keys from the TKE.

Cryptographic number
Indicates the cryptographic number for the selected Crypto Express CCA Coprocessors to permit or deny TKE commands.

Status
Indicates the status of the selected Crypto Express CCA Coprocessors. (Operating, Deconfigured)

Type
Indicates the type of selected Crypto Express CCA Coprocessors.

TKE Commands
Indicates if the TKE commands are permitted or denied for the Crypto Express CCA Coprocessors.

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Permit
To permit TKE commands, click **Permit**.

Deny
To deny TKE commands, click **Deny**.

Cancel
To close the window without changed the selected coprocessor current settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

UDX Configuration

Use this window to import and activate a UDX for the selected Coprocessor installed on your system and to reset the Segment 3 area to the Default image. This window also indicates the imported Coprocessor UDX files on your system.

Note: The recognized file name for the UDX file is: *.CCA.UDX.

Use the **UDX Configuration** window to:

- **Import** a new UDX image from a removable media or FTP location
- **Delete** or zeroize a UDX image from the hard disk
- **Activate** the UDX image into Segment 3 area
- **Reset to Default** the Default image into the Segment 3 area.

Select a Cryptographic Number, then select an action for the Segment 3 area.

Import or delete a UDX file

You can copy a UDX file to the Support Element hard drive hard drive from a removable media and use for subsequent UDX activation.

Import from FTP
To import the UDX file from a secure FTP location, click **Import from FTP**.

Import from Media
To import the UDX file from a removable media to store on the Support Element hard disk, click **Import from Media**.

Delete
To delete the UDX file from the Support Element hard disk, click **Delete**.

UDX Configuration table

The UDX configuration describes the Segment 3 area of the selected Coprocessor which holds the Common Cryptographic Architecture (CCA) application code. This window displays exactly what is located into Segment 3. You can find more detailed help on the following elements of this window:

Number
Displays a number assigned by the system to identify the selected coprocessor.

Type
Indicates if the selected Crypto Express features are operating as a coprocessor or accelerator.

Status
Displays the status of the selected coprocessor; such as, operating, deconfigured, or installed.

Image Activated
Indicates whether the UDX image is activated or the Default image is activated.

Image Timestamp
Displays the time stamp indicating when the UDX image or default image in Segment 3 was created.

Image Name
Displays the name that was specified when the image was built.

Pending Reset to Default
Displays the status if a reset to default is forced the next time the Coprocessor is operating online.

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Close
To close the window without changed the selected coprocessor current settings, click **Close**.

Help
To display help for the current window, click **Help**.

Import UDX from FTP

Use this window to import a UDX configuration file to a specified FTP destination. Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import the UDX file from the specified secure FTP location , click **Import**.

Cancel
To close the window without performing the selected operation, click **Cancel**.

Help
To display help for the current window, click **Help**.

Crypto Type Configuration

This window displays what configuration type for the selected Crypto Express features currently operating on your system. The Crypto Express features must be deconfigured prior to changing the crypto configuration type.

Cryptographic Number
Displays the number assigned by the system to identify the Crypto Express feature.

Status
Displays the status of the Crypto Express; such as, operating, deconfigured, or installed.

Select a configuration for the Crypto

Specify the crypto configuration type for the Crypto Express features installed in your system. If changing from a CCA Coprocessor to an Accelerator, you can zeroize the cryptographic keys in the CCA Coprocessor when the crypto is operating online.

For a Crypto Express features select:

- CCA Coprocessor
- EP11 Coprocessor

  Note: The TKE Workstation is required for key management of the Crypto Express EP11 Coprocessor.
- Accelerator

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Apply
To perform the selected operation, click **Apply**.

Refresh
To update the displayed crypto type configuration information with the current configuration, click **Refresh**.

Cancel
To close the window without changing the crypto type configuration, click **Cancel**.

Help
To display help for the current window, click **Help**.

Cryptographic Management

Accessing the Cryptographic Management task

Use this task to release the cryptographic number from the card serial number that it is associated with. This is necessary because the cryptographic number assigned to that card continues to be associated with the card's serial number, unless the card is released, preventing reuse of the cryptographic number. Releasing the cryptographic number permits the cryptographic number to be assigned to a new card serial number.

Each Crypto Express features is assigned a serial number (0-15) as part of the configuration process. This assignment is made when the card is installed in your system.

Use the Cryptographic Management window to view all:

- Installed cards with cryptographic number assignments
- Fenced cards that still maintain a cryptographic number assignment.

To release a cryptographic number from the card serial number:

Note: Depending on your user task role, you may only be able to view this task.

1. Open the **Cryptographic Management** task.

   The Cryptographic Management window list the cryptographic number assignments in the current system configuration.
2. Select the cryptographic number to be released from the card serial number list.
3. Click **Release**.

   The Cryptographic Management window confirms the cryptographic number you selected to be released.
4. Click **Confirm**.

   A message is displayed to indicate the release was successful.

Cryptographic Management

Use the **Cryptographic Management** task to release the cryptographic number from the card serial number that it is associated with. The Crypto Express (CCA Coprocessor, EP11 Coprocessor, and Accelerator) feature is a secure, integrated hardware that perform high-speed cryptographic functions. Each Crypto adapter is assigned a cryptographic number (0-15) as part of the configuration process. This assignment is made when the card is installed in your system.

Note: Depending on your user task role, you may only be able to view this task.

Releasing the cryptographic number permits the cryptographic number to be assigned to a new card serial number. You should release the cryptographic number when a cryptographic feature is permanently removed from the system. The cryptographic feature must have a status of fenced before it can be released.

The cryptographic functions of the Crypto Express Accelerators provide:

- SSL acceleration of modular arithmetic operations; mainly clear-key RSA private key decryption.
- A function reduced, but performance enhanced alternative to the CCA Coprocessors and EP11 Coprocessors.

The cryptographic functions of the Crypto Express Coprocessors provide:

- Support for Common Cryptographic Architecture (CCA) APIs.
- Support for AES, DES, and RSA cryptographic operations for data confidentiality, and data integrity and distributed key management.

Using the cryptographic functions of the Crypto Express EP11Coprocessor provides:

- Support for Enterprise PKCS #11 (EP11) APIs.
- Support secure PKCS #11 keys, keys that never leave the secure boundary of the coprocessor unless encrypted.

Use the Cryptographic Management window to view all:

- Installed cards with cryptographic number assignments
- Fenced cards that still maintain a cryptographic number assignment

To start the task to release a cryptographic number from the configuration, select a cryptographic number from the list box, then click **Release**.

Note: When you select a cryptographic number from the list box, all numbers associated with the card serial number are selected automatically.

Additional functions on this window include:

Release
To release the cryptographic number from the card serial number that it is associated with, click **Release**.

Cancel
To close the window without releasing the cryptographic number assigned to the cryptographic card, click **Cancel.**

Help
To display help for the current window, click **Help**.

Cryptographic Management List

Use this window to manage the release of the cryptographic numbers from the system configuration.

Number
The number assigned to the Crypto Express feature for identification purposes.

PCHID
The Physical Channel Path Identifier (PCHID) associated with the cryptographic number.

Card Location
The physical location of the cryptographic card in the frame.

Status
The status of the cryptographic card; installed, fenced, etc.

Card Serial Number
The serial number of the Crypto Express feature plugged into the specified card location.

Cryptographic Card Data

Use this window to review cryptographic card data.

Card Location
The physical location of the card in the frame.

Status
The status of the cryptographic card; installed, fenced, etc.

Card Serial Number
The serial number of the Crypto Express features plugged into the specified card location.

Type
Description of the type of cryptographic card, either a Crypto Express7S, Crypto Express6S, or Crypto Express5S feature.

Number
The number assigned to the Crypto Express7S, Crypto Express6S, or Crypto Express5S feature for identification purposes.

PCHID
The Physical Channel Path Identifier (PCHID) associated with the cryptographic number.

Cryptographic Management Confirmation

Use this window to confirm the selected cryptographic numbers to be released from the system configuration.

You can find more detailed help on the following elements of this window:

Customer Information

Accessing the Customer Information task

This task enables you to customize the customer information for a CPC or a group of CPCs.

To customize your customer information:

1. Select one or more CPCs (servers).
2. Open the **Customer Information** task. The Customize Customer Information window is displayed
3. Select one of the following tabs from the Customize Customer Information window:
   - Administrator
   - System
   - Account
4. Supply the appropriate information in the fields provided.

   If the selected objects do not all have the same customer information, the information displayed on the Customer Information window will be the information that applies to the first selected object. The information for the other objects will be displayed by tabs on the right.
5. Click **OK** when you have completed the task.

Customer Information

Use this window to specify customer information settings for individual CPCs or a group of CPCs. Each targeted CPC is represented by a read-only tab that allows its current customer information to be viewed. In addition, an editable Working Copy tab provides customer information that can be updated and applied to all targeted CPCs.

Customer Information tabs

The following tabs are provided for CPCs for contact information:

- Select **Administrator** to set up your administrator information for this CPC.
- Select **System** to set up information about this CPC.
- Select **Account** to set up customer account information for this CPC.

The following tabs are provided for CPCs prior to IBM Z® (Z) for contact information:

- Select **Company** to set up your company information for this CPC.
- Select **Account** to set up customer account information for this CPC.

The following functions are available from these pages:

Reset
To set the editable Working Copy customer information fields back to their original values, click **Reset**.

Use As Working Copy
To set the editable Working Copy customer information fields to the values of the selected CPC, click **Use As Working Copy**.

OK
After providing the appropriate information in the fields, click **OK**.

Cancel
To exit this page without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Administrator

Use this page to specify the appropriate administrator information in the provided fields. This data is used to set up your customer contact information for this CPC.

Company name
Specify your company name in this required field, up to 36 characters.

Administrator name
Specify the name of an individual within the company to contact about the CPC in this required field, up to 36 characters.

Email address
Specify an email address of a company contact, up to 256 characters.

Telephone number
Specify a telephone number for a company contact in this required field, up to 20 numeric characters including left and right parentheses ( ), hyphen (-), and comma (,).

Note: Modem support is available only for zEnterprise Systems 196 and 114 and earlier.

Alternate telephone number
Specify an alternate telephone number for a company contact, up to 20 numeric characters including left and right parentheses ( ), hyphen (-), and comma (,).

Fax number
Specify a fax telephone number for a company contact, up to 20 numeric characters including left and right parentheses ( ), hyphen (-), and comma (,).

Alternate fax number
Specify an alternate fax telephone number for a company contact, up to 20 numeric characters including left and right parentheses ( ), hyphen (-), and comma (,).

Street address
Specify the street address where the administrator resides in this required field. Include the building, floor, or room number, up to 34 characters.

Street address 2
Specify the second line of the street address where the administrator resides. Include the building, floor, or room number, up to 34 characters.

City or locality
Specify the city or locality where the administrator resides in this required field, up to 36 characters.

Country or region
Select the country or region where the administrator resides in this required field.

State or province
Select the state or province where the administrator resides in this required field.

Postal code
Specify the postal or zip code where the administrator resides in this required field, up to 12 characters.

System

Use this page to specify the appropriate system information in the fields provided. This data is used to set up your customer account information for this system.

Use the administrator mailing address
Selecting this causes the administrator's mailing address to also be used as the system location.

Street address
Specify the street address where the system resides in this required field. Include the building, floor, or room number, up to 34 characters.

Street address 2
Specify the second line of the street address where the system resides. Include the building, floor, or room number, up to 34 characters.

City or locality
Specify the city or locality where the system resides in this required field, up to 36 characters.

Country or region
Select the country or region where the system resides in this required field.

State or province
Select the state or province where the system resides in this required field.

Postal code
Specify the postal or zip code where the system resides in this required field, up to 12 characters.

Modem telephone number
Specify the modem telephone number of the Hardware Management Console that is the call-home server for the system, up to 34 characters.

This is the telephone number a remote, automated service support system must dial to establish a remote connection with the call-home server.

Note: The modem telephone number can only be specified for a zEnterprise 196 (z196), zEnterprise 114 (z114), and earlier systems.

Account

Use this page to specify the appropriate information in the customer account fields provided. This data is used to set up your customer account information for this system.

If you do not know or are unsure of this information, contact your support structure for assistance.

Customer number
Specify the number assigned to your account for this purchase, up to 10 characters.

Enterprise number
Specify the number assigned to your account as your single enterprise number, up to 10 characters.

Sales branch office
Specify the three-digit sales branch office number that services this system.

Service branch office
Specify the three-digit service branch office number that services this system.

Area
Specify the three-digit area number that services this system.

Company

Use this page to specify the appropriate company information in the provided fields. This data is used to set up your customer contact information for this CPC.

Company name
Specify your company name in this required field, up to 35 characters.

Street address
Specify the company mailing address in this required field. Include the building, floor, or room number, up to 35 characters.

Street address 2
Specify the second line of the company mailing address. Include the building, floor, or room number, up to 35 characters.

Street address 3
Specify the third line of the company mailing address. Include the building, floor, or room number, up to 35 characters.

System location
Specify the physical location where the CPC resides in this required field. Include the building, floor, or room number, up to 35 characters.

System location 2
Specify the second line of the physical location where the CPC resides. Include the building, floor, or room number, up to 35 characters.

Person name
Specify the name of an individual within the company to contact about the CPC in this required field, up to 30 characters.

Voice telephone number
Specify a telephone number for a company contact in this required field, up to 34 numeric characters including left and right parentheses ( ), hyphen (-), and comma (,).

Modem telephone number
Specify the modem telephone number of the Hardware Management Console that is the call-home server for the CPC in this required field, up to 34 characters.

This is the telephone number a remote, automated service support system must dial to establish a remote connection with the call-home server.

Account

Use this page to specify the appropriate account information in the fields provided. This data is used to set up your customer account information for this CPC.

If you do not know or are unsure of this information, contact your support structure for assistance.

Customer number
Specify the number assigned to your account for this purchase, up to 10 characters.

Sales branch office
Specify the three-digit sales branch office number that services this CPC.

Service branch office
Specify the three-digit service branch office number that services this CPC.

Area
Specify the three-digit area number that services this CPC.

Country
Specify the two or three-digit country code where the CPC resides.

Customizable Data Replication Warning

Customizable Data Replication Warning

The customizable data types listed in this window are currently not configured to be replicated from any replication data sources. The changes that are about to be made will result in these data types to start being replicated. This will result in the complete replacement of the data for these types that is currently maintained on this Hardware Management Console.

Continue with the configuration, and commit the changes if this is the desired result. If this is not the desired result, make sure to cancel or alter these changes.

Note: Allowing the replication of some types of customizable data such as user profiles, object instance data, and customized dial information can result in changes that change the operating characteristics of this Hardware Management Console.

Type of data
Specifies the data type that was just manually changed.

Select an Action
Select one of the following actions that you want to be taken in response to this customizable data replication warning.

- Request reset of this data to prior settings
- Unconfigure all data sources for this data
- Ignore this warning

OK
To proceed with the action you have selected, click **OK**.

Help
To display help for the current window, click **Help**.

Customize API Settings

Accessing the Customize API Settings task

This task, used by an access administrator or a user ID that is assigned access administrator roles, allows you to control Hardware Management Console Application Programming Interfaces (APIs) access. This access permits applications that were not supplied as part of the Hardware Management Console Application (HWMCA) to communicate with the objects defined to this Hardware Management Console.

This task allows you to enable or disable an SNMP agent and set up a community name file and event notification information for an SNMP agent from the **SNMP** tab. You can enable or disable the Web Services Application Programming Interface (API) from the **WEB Services** tab.

For more information on SNMP and Web Services, see *SNMP Application Programming Interfaces*, SB10-7171, and *Hardware Management Console Web Services API*, SC27-2637, respectively.

To customize API settings:

1. Open the **Customize API Settings** task. The Customize API Settings window is displayed.
2. From the **SNMP** tab you can enable SNMP APIs and add, change, or delete community names, SNMPv3 users, and event notification information. From the **WEB Services** tab you can enable or disable the Web Services Application Programming Interface (API) and control the IP address and user access.
3. Click **OK** to save the SNMP or WEB Services configurations and continue.

Customize API Settings

Use this task to customize the settings that support using Application Programming Interfaces (APIs) to the Hardware Management Console Application.

SNMP
Use this tab to enable and customize the SNMP settings.

WEB Services
Use this tab to enable and customize the Web Services Application Programming Interface (API).

Additional functions for this window include the following:

OK
To save the configuration, click **OK**.

Cancel
To exit this window and discard any changes made, click **Cancel**.

Help
To display help for the current window, click **Help**.

SNMP

Use this page to customize the settings that support using Management Application Programming Interfaces (APIs) to the Hardware Management Console Application.

You can find more detailed help on the following elements of this window:

Enable SNMP APIs

Enable
To allow other system management applications to use Management APIs to the Hardware Management Console Application, select **Enable**.

The Management APIs include:

Data exchange APIs
Allow applications to exchange information about objects managed by the console Application.

Command APIs
Allow applications to send commands to objects managed by the Hardware Management Console Application.

SNMP agent parameters
Specify the parameters to use to start the Simple Network Management Protocol (SNMP) agent when the console Application starts.

Community Names

Specifies the community name(s) the Hardware Management Console Application must use to request SNMP information from the SNMP agent.

The Community Names table displays the following information:

Name
Specifies the community name used to verify that a request for SNMP information is valid when a manager makes an SNMP request.

Address
Specifies the IPv4 or IPv6 internet address.

Network Mask
Specifies a network mask that is logically ANDed with the IP address of the manager making an SNMP request.

Access Type
Specifies the access you want to allow SNMP requests.

The following options are available from this section of the window:

Add...
To add a new community names entry, click **Add...**.

Change...
To change the community name entry information for the selected entry, click **Change...**.

Delete
To delete the community name entry information for the selected entry, click **Delete**.

Community Name Information

Specify the community name the Hardware Management Console Application must use to request SNMP information from the SNMP agent.

A community name is similar to a password. It is used by an SNMP agent to validate requests for information received from system management applications.

The SNMP agent provides SNMP information to system applications authorized to manage another application and its objects.

Note: The community name is case sensitive and cannot exceed 16 characters.

The community name you specify must match exactly the community name in the SNMP information for this console for its SNMP agent to validate and accept requests from the Hardware Management Console Application for SNMP information.

Name
This field contains the community name. Specify a unique string of characters (up to 16 characters), which is used to verify that a request for SNMP information is valid when a manager makes an SNMP request. The community name it is using must match the community names specified in this field. If it does not match, the SNMP request is not processed. The community name is similar to a password.

Address
Specify an IPv4 or IPv6 internet address (IP address).

The IPv4 address is written as four decimal numbers, representing the four bytes of the IP address, separated by periods (for example, `9.60.12.123`). The IPv6 address can be written as eight groups of four hexadecimal digits, separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

Note: For IPv6 simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or you can use a double colon in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

When a manager makes an SNMP request, a logical AND is performed on its address and the value specified in the network mask field. If the result of the logical AND matches the value specified in the address field, the request is processed.

If you specify a specific IPv4 address in this field, only the host using that IP address can use the community name specified in the name field. Enter a network mask of 255.255.255.255 if you specify a specific IPv4 IP address in this field.

If you specify a specific IPv6 address in this field, only the host using that IP address can use the community name specified in the name field. Enter a network mask of 128 if you specify a specific IPv6 IP address in this field.

To allow any host with the correct community name to make SNMP requests:

- For IPV6, specify : : in the address field and 0 in the network mask field.
- For IPV4, specify 0.0.0.0 in the address field and 0 in the network mask.

Network mask / Prefix
This field contains a network mask that is logically ANDed with the IP address of the manager making an SNMP request. If the result of the logical AND is equal to the address specified in the address field and the community name matches, the request is processed.

To allow SNMP requests only from the host specified in the address entry field, specify a network mask of 255.255.255.255 for an IPv4 address or specify a network mask of 128 for an IPv6 address.

To allow any host with the correct community name to make SNMP requests:

- For IPV6, specify a network mask of 0 and an address of : :.
- For IPV4, specify a network mask of 0 and an address of 0.0.0.0.

Read only
If you want to allow SNMP requests with valid community names to have only read access to the SNMP agent information on this system, select **Read only**.

Read/write
If you want to allow SNMP requests with valid community names to have write access to the SNMP agent information on this system, select **Read/write**.

OK
To save the current settings in this window, click **OK**.

Cancel
To exit this window, discard any changes made, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

SNMPv3 Users

Specifies the SNMPv3 user(s) the Hardware Management Console Application uses. SNMPv3 provides enhanced security via password based authentication and encryption.

The SNMPv3 Users table displays the following information:

User Name
Specifies the SNMPv3 user name.

Access Type
Specifies the access allowed to the SNMPv3 user.

The following options are available from this section of the window:

Add..
To add a new SNMPv3 user entry, click **Add...**.

Change...
To change the SNMPv3 user name information for the selected entry, click **Change...**.

Delete
To delete the selected SNMPv3 user entry, click **Delete**.

SNMPv3 User Information

Use this window to provide an SNMPv3 user name, password, and access type.

User Name
Specify an SNMPv3 user name. The user name must be at least 8 characters in length and cannot exceed 32.

Password
Specify a valid password for the SNMPv3 user. The password must be at least 8 characters in length and cannot exceed 32.

Read only
To allow only read access to the specified user name, select **Read only**.

Read/write
To allow read and write access to the specified user name, select **Read/write**.

OK
To save the current settings in this window, click **OK**.

Cancel
To exit this window, discard any changes made, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Event Notification Information

This information controls the distribution of messages about events that affect objects managed by the Hardware Management Console Application.

The following options are available from this section of the window:

Add...
To add a new event notification information entry, click **Add...**.

Change...
To change the event notification entry information for the selected entry, click **Change...**.

Delete
To delete the selected event notification information entry, click **Delete**.

Event Notification Information

Use this window to add or change information that controls the distribution of trap messages about events that affect objects managed by the Hardware Management Console Application.

Trap messages are unsolicited notifications of significant system events sent by an SNMP agent to an SNMP client.

TCP/IP address
Specify the host name or IPv4 or IPv6 TCP/IP address of the location where you want SNMP trap messages sent when selected events occur.

The IPv4 address is written as four decimal numbers, representing the four bytes of the IP address, separated by periods (for example, `9.60.12.123`). The IPv6 address can be written as eight groups of four hexadecimal digits, separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

Note: For IPv6 simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or you can use a double colon in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

Port number
Specify the TCP/IP port number when defining SNMP trap recipients, if it's something other than the default SNMP trap port of `162`.

Events
Select one or more events for which trap messages are sent to the specified location. The events affect objects managed by the Hardware Management Console Application.

Activation Profile Change
To send a message when the activation profile for an object has changed, select **Activation Profile Change**.

Capacity Change
To send a message when a hardware object's temporary capacity has changed, select **Capacity Change**.

Capacity Record Change
To send a message when a temporary capacity record for a hardware object has changed, select **Capacity Record Change**.

Disabled Wait
To send a message when an operating system object enters a disabled wait, select **Disabled Wait**.

Exception State
To send a message when the status of an object changes from an acceptable status to an unacceptable status, or from an unacceptable status to an acceptable status, select **Exception State**.

Exclude Refresh Messages
To disable the sending of a message when an object receives a refresh message, select **Exclude Refresh Messages**.

Console Application Ended
To send a message when the Hardware Management Console Application ends, select **Console Application Ended**.

Console Application Started
To send a message when the Hardware Management Console Application starts, select **Console Application Started**.

Hardware Message Deletion
To send a message when a message for a hardware object is deleted, select **Hardware Message Deletion**.

Hardware Messages
To send a message when a hardware object receives a new or refresh message, select **Hardware Messages**.

Messages
To send a message when a Hardware Message or Operating System Message occurs on an object, select **Messages**.

Name Change
To send a message when the name of an object changes, select **Name Change**.

Object Creation
To send a message when an object definition is added, select **Object Creation**.

Object Destruction
To send a message when an object definition is removed, select **Object Destruction**.

Operating System Messages
To send a message when an operating system object receives a new or refresh message, select **Operating System Messages**.

Security Events
To send a message when a security event occurs for an object (such as logons or object definitions), select **Security Events**.

Status Change
To send a message when the status of an object changes, select **Status Change**.

OK
To save the current settings in this window, click **OK**.

Cancel
To exit this window, discard any changes made, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

WEB Services

Use this page to customize the settings that supports the use of the Web Services Application Programming Interface (API) to the console.

Enable
To allow other system management applications to use Web Services API functions, select **Enable**.

Allow all IP Addresses
To allow connections from any IP address, select **Allow all IP Addresses**.

Note: When you select this option the ability to add, edit, or remove an IP address is disabled.

IP Addresses
To allow a specific IP address connection to the Web Services API functions, select **IP Addresses**. Then, select the IP address from the "IP Addresses table" on page 664 that is allowed connection to the Web Services API functions.

IP Addresses table
This table displays the IP addresses that allow connections to the Web Services API functions for a specific TCP/IP address.

Add
To add an IP address to the IP Addresses table that allows connections to the API ports, click **Add**. The Define IP address and mask window is displayed.

1. Choose how you want to define the IP address and mask.
2. Provide a valid IP address (and mask) that is appropriate for that selection.
3. Click **Add** to include this information in the IP Addresses table.

To return to the previous window without adding this information, click **Cancel**.

Edit
To change an existing IP address that allows connections to the API ports, select an IP address from the list, then click **Edit**. The Define IP address and mask window is displayed. Make appropriate changes, then click **Update** to include this information in the IP Addresses table. To return to the previous window without making changes, click **Cancel**.

Remove
To remove an IP address, select an IP address from the IP Addresses table, then click **Remove**. The IP address is removed from the IP Addresses table.

Access Control table
From this table, you can select one or more user IDs that might have access to the Web Services API functions. The table contains the following information:

Name
Specifies the user ID.

Type
Specifies the type of user ID that was set up using the **User Management** (users or user templates) task.

Maximum Sessions
Specifies the number of times a single user can be logged in to a Web Services API session simultaneously without disconnecting. The default value is 100. This value is set in the **User Management** (users) task.

Customize Automatic Logon

Accessing the Customize Automatic Logon task

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables or disables the automatic logon feature.

When enabled, the automatic logon feature will log on the Hardware Management Console automatically using the user ID you specified whenever the Hardware Management Console is powered on.

To customize automatic logon:

1. Open the **Customize Automatic Logon** task. The Customize Automatic Logon window is displayed.
2. Select **Enable automatic logon feature**, then select a user ID.
3. Click **OK** to save the setting and exit the task.

Customize Automatic Logon

Use this window to verify or change the setting of the automatic logon feature.

Automatic logon automatically logs on the Hardware Management Console Application when the Hardware Management Console is initialized. The console is initialized whenever it is turned on or rebooted.

When automatic logon is enabled, the **Hardware Management Console Workplace** window is displayed when console initialization is completed, providing immediate access to application tasks. The level of access is determined by the user identification selected when automatic logon was enabled.

Attention: When automatic logon is enabled, a user does not need a user identification and password to log on the application.

Otherwise, when automatic logon is disabled, the logon window is displayed when console initialization is completed. A user must specify a user identification and password to log on the application manually.

Enable automatic logon feature
To change the setting for automatically logging on the Hardware Management Console Application, select **Enable automatic logon feature**.

When automatic logon is enabled (a check mark appears), select the user identification to logon to from the list of user IDs.

Select a User ID
Select the user identification to logon to from the list of user IDs.

OK
To save the new setting, click **OK**.

Apply
To save the automatic logon information customized for this Hardware Management Console and continue customization, click **Apply**.

Cancel
To leave this task without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Console Date/Time

Accessing the Customize Console Date/Time task

This task is used to configure the date, time, and time zone of the battery operated clock on the console. You can also set up a Network Time Protocol (NTP) client.

The battery operated clock keeps the date and time for the Hardware Management Console. You can change the settings of the battery operated clock under the following conditions:

- The battery is replaced in the Hardware Management Console.
- Your system is physically moved to a different time zone.

If a CPC Support Element is enabled for time synchronization (by selecting **Selected CPCs...** from the Date and Time window), this task causes the Hardware Management Console to update its clock with the time that is set on the CPC Support Element and keyboard entries will be ignored.

The following list shows the zone correction for some major cities around the world:

City	Direction	Number of Hours Standard Time	Number of Hours Daylight Time
Amsterdam	East	1	2
Anchorage	West	9	8
Berlin	East	1	2
Buenos Aires	West	3	-
Chicago	West	6	5
Denver	West	7	6
London	East	0	1
Los Angeles	West	8	7
New York City	West	5	4
Madrid	East	1	2
Oklahoma City	West	6	5
Paris	East	1	2
Pittsburgh	West	5	4
Rio de Janeiro	West	3	2
Rome	East	1	2
Stockholm	East	1	2
Sydney	East	10	11
Tel Aviv	East	2	3
Tokyo	West	9	-
Toronto	West	5	4
Vienna	East	1	2

For the procedure for changing the Hardware Management Console date and time, see the "Changing your time-of-day" topic in the **Introduction**.

This task also allows you to set up a Network Time Protocol (NTP) client.

Note: When the Hardware Management Console is configured to have an NTP client running, the Hardware Management Console is continuously synchronized to an NTP server instead of synchronizing to a CPC Support Element. If a Hardware Management Console is set up to synchronize to a CPC Support Element, the synchronization is requested immediately when the NTP client has stopped and then the Hardware Management Console will continuously synchronize with the Support Element at the designated time.

To set up the date and time:

1. Open the **Customize Console Date/Time** task. The Date and Time window is displayed. You can change the date and time of the battery operated clock on the console if **None** is selected as the time source. The time zone can be changed at any time.
2. Select the **Network Time Protocol (NTP)...** time source to set up the configuration of the NTP client.
   - From the Select Action drop-down, click **Add Server...** to add a server to the NTP configuration file. The Add Network Time Server window is displayed.
     – Specify a time server host name or IP address and select the authentication, then click **OK**.

       Note: To locate an external NTP server, you can:

       - Use the Internet to search for Network Time Protocol.
       - See the Network Time Protocol website (www.ntp.org) for a list of public servers as well as a list of NTP pools that allows the console to get the NTP time from a server that is in the pool. For example, in the United States, you can specify the following addresses:
         - 0.us.pool.ntp.org
         - 1.us.pool.ntp.org
         - 2.us.pool.ntp.org
         - 3.us.pool.ntp.org
   - From the Select Action drop-down, you can also select **Edit**, **Remove**, or **Query** selected servers.
   - Select **Enable as time server** to allow this console to become an NTP server which, in turn, allows another console to obtain the current date and time from this Hardware Management Console.
   - Select **Automatically contact the support system if the time source cannot be reached** when you want the support system automatically notified when the selected CPCs are not available.
   - From the Select Action drop-down, you can select **Manage Symmetric Keys...**, **Configure Autokey...**, and **Issue NTP Commands...** to configure symmetric keys, Autokey, and issue informational NTP commands, respectively.
3. Select **Select CPCs...** time source to set up the Hardware Management Console to follow the time on selected CPC Support Elements which includes the time source and status details.

   You can optionally select **Automatically contact the support system if the time source cannot be reached** when you want the support system automatically notified when the NTP servers are not available.
4. Click **OK** when you have completed this task, or click **Cancel** to exit the task without making any changes.

Date and Time

Use this task to configure the date, time, and time zone of the battery operated clock on the console and to set up the console's time source including the Network Time Protocol (NTP) client.

Battery Operated Hardware Management Console Clock

You can change the settings under the following conditions:

- The battery is replaced in the console.
- Your system is physically moved to a different time zone.

The following fields are applicable:

Date
This field displays the current date set for the console. To change the setting, specify a new date. The default is set to the console's current date.

Set the assigned date for your system. Specify the new date using the same format as shown in the Date field. For example, `August 10, 2005`.

This information is used to establish and control operating sessions.

Time
This field displays the current time set for the console. To change the setting, specify a new time. The default is set to the console's current time.

A time is required for your local system operation.

Set the assigned time for your system. Specify the new time using the same format as shown in the Time field. For example, `8:35:00 AM`.

This information is used to establish and control operating sessions.

Time zone
To select the time zone for the console, select the down arrow on the entry field and select one. The time zone can be changed regardless of which time source you select. The default is set to the console's current time zone.

Select a city from the list that has the same time as the one you need. For example, if the console is located in Austin, Texas, select **America/Chicago** since that is the city in the list located in the same time zone as Austin.

Note: Each time zone has its own unique daylight saving time rules. Also, when you make changes to the time zone a reboot of the console is required.

Following are some examples when setting the battery operated Hardware Management Console clock.

To set the time-of day (TOD) to Local time at 8:35 am, on August 10, 2007 in Austin, the panel entries would be:

Date: `August 10, 2007`
Time: `8:35:00 AM`
Time zone: `America/Chicago`

To set the TOD to UTC time at 8:35 am, on August 10, 2007 in Austin, the recommended panel entries would be:

Date: `August 10, 2007`
Time: `1:35:00 PM`
Time zone: `UTC`

Time Source

Network Time Protocol (NTP)...
To enable the Network Time Protocol (NTP) time source, select **Network Time Protocol (NTP)...**. The “Details for Network Time Protocol (NTP)” on page 669 is displayed in the Date and Time window. To allow this console to obtain the current date and time from any of the NTP servers that are listed, click **OK**.

Note: You can only change the **Time zone** with this selection.

Selected CPCs...
To view a list of defined CPCs which includes CPC name, time source, and status details, select **Selected CPCs...** The Details for Selected CPCs table is displayed in the Date and Time window. The table include the name of the CPC, the Coordinated Timing Network (CTN) ID, and the current status. If the status is set to "Communications not active" then the CTN ID is not displayed. To obtain the latest status of the CPCs, click **Refresh**.

Note: You can only change the **Time zone** with this selection.

None
To change the battery operated Hardware Management Console clock settings, select **None**. This disables all the other time sources. This is the default selection.

Additional options are available from this window, depending on your time source selection:

Enable as time server
To allow this Hardware Management Console to become an NTP server which in turn allows another console to obtain the current date and time from this Hardware Management Console provided that this Hardware Management Console is listed in the console's list of NTP servers, select **Enable as time server**. This option is displayed when you selected NTP as a time source.

Automatically contact the support system if the time source cannot be reached.
To have the support system automatically notified when the NTP servers or selected CPCs are not available, select **Automatically contact the support system if the time source cannot be reached**.

Regardless of your selection, you will be notified with a hardware message, approximately two hours after being unable to communicate with the NTP servers or selected CPCs.

Additional functions are available from this window:

Refresh
To redisplay the current date and time and to redisplay the current list of CPCs, click **Refresh**.

OK
To continue the task with the settings you have chosen, click **OK**.

Cancel
To close this window and exit this task without saving new settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Details for Network Time Protocol (NTP)

Use this table to set up NTP servers. You can add an NTP server to the NTP servers table by clicking the drop-down arrow next to **--- Select Action ---**, then click Add Server. The Add Network Time Server window is displayed.

You can work with the items listed in the NTP servers table by selecting one or more servers, then from the **---Select Action---** list on the table tool bar you can choose one of the following actions:

- Edit Server - modify an existing NTP server in the table
- To delete a selected NTP server from the table, select **Remove Server**.
- To query all the NTP serves for determining NTP server connection, click **Query Servers**. The information is displayed in the table.

The toolbar at the top of the NTP servers table also contains icons used to select, filter, sort, and arrange the columns in the NTP servers table.

You can work with the table by using the table icons or **---Select Action--- Table Actions** list from the table tool bar. Filter the data you would like to appear in the NTP servers table by manipulating the information in the table. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions:

Select All
The **Select All** icon allows you to select all the objects in the Overview table.

Deselect All
The **Deselect All** icon allows you to deselect all the objects in the Overview table.

Show Filter Row
The **Show Filter Row** icon allows you to define a filter for a table column to limit the entries in a table. Tables can be filtered to show only those entries most important to you. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row.

Clear All Filters
The **Clear All Filters** icon allows you to return to the complete table summary. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Configure Columns
The **Configure Columns** icon allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns.

You can find more detailed help on the following elements of this window:

NTP Servers

This table displays a list of the currently defined time servers in the NTP configuration file.

Server
Specifies the NTP time server TCP/IP addresses.

Note: Beginning with System z10, IPv6 addresses are acceptable. Normal IPv6 addresses should resolve correctly to the target NTP server. Link-local address (FE80:*) are not routable addresses and are only for use on the same link (same subnet). These link-local addresses will not resolve correctly unless they are on the same subnet as an interface to the console and are fully qualified with the zone identifier. Without the appended zone identifier, the NTP access on the query will fail with a "Communication failure" displayed in the **Status** column of this table.

Stratum
Identifies the accuracy of the time at the NTP time server. A stratum level of one (1) indicates the NTP time server obtained its time directly from a reference time source. A stratum level of *n* indicates the NTP time server is *n*-1 hops away from the time source.

Source
If the NTP time server has a stratum of 1, the source indicates where that NTP time server is getting the time from. If the NTP time server has a stratum > 1, the source indicates the address of the NTP time server that it got the time from. Some of the possible source values and their descriptions include:

Not available
The source address could not be determined from the information in the NTP packet.

Local
Uncalibrated local clock

Cesium
Calibrated Cesium clock

Rubidium
Calibrated Rubidium clock

PPS
Calibrated quartz clock or other pulse-per-second source

IRIG
Inter-Range Instrumentation Group

ACTS
NIST telephone modem service

USNO
USNO telephone modem service

PTB
PTB (Germany) telephone modem service

TDF
Allouis (France) Radio 164 kHz

DCF
Mainflingen (Germany) Radio 77.5 kHz

MSF
Rugby (UK) Radio 60 kHz

WWV
Ft.Collins (US) Radio 2.5, 5, 10, 15, 20 MHz

WWVB
Boulder (US) Radio 60 kHz

WWVH
Kaui, Hawaii (US) Radio 2.5, 5, 10, 15 MHz

CHU
Ottawa (Canada) Radio 3330, 7335, 14760 kHz

LORAN-C
LORAN-C radio navigation system

OMEGA
OMEGA radio navigation system

GPS
Global Positioning Service

HBG
Prangins, HB 75 kHz

JJY
Fukushima, JP 40 kHz, Saga, JP 60 kHz

GOES
Geostationary Orbit Environment Satellite

INIT
Initializing

Authentication
Displays the type of authentication that was assigned to the server. The authentication could be:

- none
- key <key#>
- autokey

Status
Displays the current status of the NTP time server or the results of a query to that server. Possible status messages include:

Success

Message:
Success

Explanation:
Access to the NTP time server was successful.

Action:
None.

Success - initializing

Message:
Success - initializing

Explanation:
Access to the NTP time server was successful. The NTP time server is still initializing.

Action:
There is the possibility for the post initialization status to be "Success - local source", recheck the status in 20 minutes.

Success - local source

Message:
Success - local source

Explanation:
Access to the NTP time server was successful, however, the local clock of the NTP time server is being used as the time source.

Action:
If the NTP time server was just configured for use, it may be using its local clock while synchronization to its real time source is taking place. If the status persists for too long, consider assigning a different NTP time server to ensure an accurate time source.

Incorrect IP address

Message:
Incorrect IP address

Explanation:
The NTP IP address is not in the proper format or the DNS failed to recognize the web address and could not convert it into an IP address.

Action:
Correct the IP address or the web address and click **Query Servers**.

Socket failure

Message:
Socket failure

Explanation:
The console is resource constrained and is unable to create a connection to the NTP time server.

Action:
Contact next level of support.

Communication failure

Message:
Communication failure

Explanation:

- An error occurred reading from or writing to the NTP time server.
- IPv6 link-local address is specified that is not fully qualified.

Action:

- Verify the ethernet connection between the NTP time server and the console. Click **Query Servers** to test access to the NTP time server. If the problem persists, contact next level of support.
- System z10 and later accepts IPv6 addresses for target NTP servers. Normal IPv6 addresses should resolve correctly to the target NTP server. Link-local address (FE80:*) are not routable addresses and are only for use on the same link (same subnet). These link-local addresses will not resolve correctly unless they are on the same subnet as an interface to the console and are fully qualified with the zone identifier. Find the fully qualified setting for the link-local address.

Timeout failure

Message:
Timeout failure

Explanation:
A time out occurred waiting for the NTP time server to respond to a request.

Action:
Verify the IP address or web address of the NTP time server, the status of the NTP time server, and the connections to the physical NTP time server to ensure that the request is reaching its destination. If a problem is found, click **Query Servers** to test access to the NTP time server.

Server access denied

Message:
Server access denied

Explanation:
The NTP time server denied access to the request.

Action:
Verify the IP address or web address is a valid NTP time server and click **Query Servers**.

Server unsynchronized

Message:
Server unsynchronized

Explanation:
The NTP time server has never synchronized to a valid time source.

Action:
Verify the NTP time server is properly configured to connect to a time source and click **Query Servers**.

Server must resynchronize

Message:
Server must resynchronize

Explanation:
The NTP time server has not recently been able to synchronize to a valid time source.

Action:
Verify the NTP time server is properly configured to connect to a time source and click **Query Servers**.

NTP server error

Message:
NTP server error

Explanation:
An undefined error was returned while accessing the NTP time server.

Action:
Verify the IP address or web address is a valid NTP time server and click **Query Servers**.

Unsupported NTP server version

Message:
Unsupported NTP server version

Explanation:
The NTP time server is using an NTP version that is not supported.

Action:
Configure an NTP time server that is using NTP V3 or higher and click **Query Servers**.

NTP server stratum greater than 15

Message:
NTP server stratum greater than 15

Explanation:
The NTP time server returned a stratum greater than fifteen (15). Fifteen (15) is the maximum allowable NTP time server stratum.

Action:
Change the IP address or web address to a valid NTP time server and click **Query Servers**.

NTP server packets bad

Message:
NTP server packets bad

Explanation:
The NTP packets received were not in the proper format.

Action:
Change the IP address or web address to a valid NTP time sever and click **Query Servers**.

Invalid source ID

Message:
Invalid source ID

Explanation:
The source ID (NTP reference ID) returned from the stratum-1 NTP time server does not contain printable characters.

Action:
Change the IP address or web address to a valid NTP time server and click **Query Servers**.

Server access problem

Message:
Server access problem

Explanation:
The target server is not configured for Autokey.

Action:
Configure Autokey on the target server.

Autokey not configured

Message:
Autokey not configured

Explanation:
Autokey was specified for the server but the local Autokey was never generated.

Action:
Generate the local host key from the Autokey Configuration window.

Autokey reconfigure

Message:
Autokey reconfigure

Explanation:
Autokey is in an improper state, the local host key needs to be regenerated.

Action:
Regenerate the local host key from the Autokey Configuration window.

Add/Edit Network Time Server

Use this window to add a new time server or change an existing one that you selected. You can also select NTP authentication.

Enter the time server host name or IP address
Specify the time server host name or TCP/IP (IPv4 or IPv6) address. The address information is stored in the NTP configuration file (/etc/ntp.conf).

IPv6 addresses are written as eight groups of four hexadecimal digits. For example, fe80:0:0:0:204:acff:feab:b811 is a valid IPv6 address. If one or more four digit groups are 0000, the zeros can be omitted and replaced with two colons (::).

You can also specify an external NTP server. To locate an external NTP server you can:

- Use a known NTP server.
- See *www.ntp.org* for a list of public NTP servers as well as a list of NTP "pools" that allow the console to get the NTP time from a server that is in the pool.

Authentication Selection
To select a specific authentication type for the particular server, use the drop-down arrow for your choices.

None
This is the default.

Symmetric Key
If you select **Symmetric Key** an additional drop-down input area is displayed where you will specify the symmetric key index. For symmetric key specification, `key` followed by the symmetric key index will be added to the end of the server string in the NTP configuration file. During NTP processing the symmetric key will be used to index the /etc/ntp/keys file to obtain the key to add the digital signature to the NTP packet. In order for the symmetric key index to display in the **Symmetric Key** drop-down, it must first be added by clicking **Manage Symmetric Keys...** from the Select Action drop-down.

Autokey
The `Autokey` string will be added to the end of the server string. During NTP processing, Autokey keys are used to add the digital signature to the NTP packet. All of the packet handling is performed by the Linux supplied NTP application. Local Host Autokey generation must first be performed on the Autokey Configuration window (by clicking **Configure Autokey...** from the Select Action drop-down) before autokey can be exploited by NTP.

OK
To save the changes you have made, click **OK**.

Cancel
To close this window and return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Manage Symmetric Keys

To add a new symmetric key to the Symmetric Keys table or manage existing symmetric keys that are listed in the table, click **Manage Symmetric Keys...** from the Selection Action drop-down. The Manage Symmetric Keys page is displayed.

From the **---Select Action---** drop-down on the table tool bar, choose one of the following actions:

- To add a symmetric key to the table, select Add Key ..., the Add Symmetric Key Data window is displayed.
- To change an existing key, select a key from the table, select Edit Key ..., the Edit Symmetric Key Data window is displayed.
- To delete existing keys, select one or more from the table, select **Remove Key...**. Those selected will no longer appear in the table.

The information displayed in this table is contained in the NTP keys file, etc/ntp/keys. Each symmetric key that is stored in this file is available to NTP acting as a client and a server. The format of the ntp key is the symmetric key index, followed by the key type, and then the key string for each key to be defined. The Symmetric Keys table displays the **Index** and **String** for each key. The symmetric keys (Index and String) are obtained from the server and they must match the server's symmetric key entry for the authentication to work.

Index
Specifies the key index of the symmetric key. It has a numeric value that ranges from 1 to 65534.

String
Specifies the key string of the symmetric key. It can be up to 40 characters long. If the string is 40 characters, the characters must be hexadecimal ASCII characters (0-9, a-f). If the string is less than 40 characters, the characters must be any printable ASCII character.

Note: The key type is always MD5 and cannot be changed.

The toolbar at the top of the Manage Symmetric Keys table contains icons used to select, filter, sort, and arrange the columns in the Manage Symmetric Keys table.

You can work with the table by using the table icons or **---Select Action---** *Table Actions* list from the table tool bar. Filter the data you would like to appear in the NTP servers table by manipulating the information in the table. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions:

Select All
The **Select All** icon allows you to select all the objects in the Overview table.

Deselect All
The **Deselect All** icon allows you to deselect all the objects in the Overview table.

Show Filter Row
The **Show Filter Row** icon allows you to define a filter for a table column to limit the entries in a table. Tables can be filtered to show only those entries most important to you. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row.

Clear All Filters
The **Clear All Filters** icon allows you to return to the complete table summary. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Configure Columns
The **Configure Columns** icon allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns.

Additional functions are available from this window:

OK
To save the changes to the /etc/ntp/keys file and return to the previous window, click **OK**.

Cancel
To close this window and return to the previous window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Add/Edit Symmetric Key Data

Use this window to add or edit symmetric key data.

The key data provided here is saved in the /etc/ntp/keys file and all keys are added to the 'trustedkey' section of the NTP configuration file. This enables the keys to be used and verified by the client (Hardware Management Console). The symmetric key index and key string are obtained from the server and they must match the server’s symmetric key entry for the authentication to work.

Key index
Specify a numeric key index between 1 and 65534.

Key string
Specify a unique key string, up to 40 characters.

If the string is 40 characters long, the characters must be hexadecimal ASCII characters (0-9, a-f). If the string is less than 40 characters long, the characters must be any printable ASCII character.

OK
To save the input you provided, click **OK**. The keys are verified and the Symmetric Keys table is updated.

Cancel
To close this window and return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Autokey Configuration

To generate, on the Hardware Management Console, an RSA private/public key file and a self-signed certificate file for the RSA digital signature algorithm with the MD5 message digest algorithm, click **Configure Autokey...** from the Select Action drop-down. These values are automatically passed toward the target server via NTP packets and are used to verify that packets were not tampered with.

Local host key: Generated
To initiate key generation for the Hardware Management Console NTP, click **Generate**. This issues the `ntp-keygen` command to generate the specific key and certificate for this system. You only need to click **Generate** once.

Close
To close this window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Issue NTP Commands

To determine configuration problems, certificate expiration, and other causes of NTP errors, click **Issue NTP Commands...** from the Select Action drop-down. Select a command depending on the type of problem you encounter, your results are displayed in the Command Result text area. To close this window and return to the previous window, click **Close**. To display help for the current window, click **Help**.

Display state of peers by host name - (`ntpq -p`)
Displays a list of peers known to the server as well as a summary of their state. This is equivalent to the peers interactive command. The output summary includes:

remote
Specifies the host name (IP number) of the peer

refid
Specifies the association identifier

st
Specifies the stratum

t
u = unicast or manycast client, b = broadcast or multicast client, l = local (reference clock), s = symmetric (peer), A = manycast server, B = broadcast server, M = multicast server

when
Specifies seconds (sec), minutes (min), hours (hr) since packet last received

poll
Specifies poll interval

reach
Specifies the reach shift register (octal)

delay
Specifies roundtrip delay

offset
Specifies offset of server relative to this host

jitter
Identifies jitter (or dispersion)

Display state of peers by ip address - (`ntpq -np`)
Displays how the Hardware Management Console NTP client perceives its NTP servers via IP address. The output summary includes:

remote
Specifies the address of the time server

refid
Indicates the type of the time server

st
Specifies the Stratum which indicates the accuracy to be expected

t
u = unicast or manycast client, b = broadcast or multicast client, l = local (reference clock), s = symmetric (peer), A = manycast server, B = broadcast server, M = multicast server

when
Specifies the time to the next update

poll
Specifies the count that 'when' has to reach before an update is attempted

reach
An octal number that is left-shifted on each update

delay
Specifies the RTT to the time server

offset
Specifies the difference between the remote and local clock

jitter
Identifies dispersion

Display list of peer associations - (`ntpq -c as`)
Displays a list of associations, including authentication status. The output summary includes:

ind
Index numbering of associations from one.

assID
Association identifier returned by the server

status
Displays the status word for the peer. The peer status code bits are in hexadecimal consisting of four fields: status (0-4), select (5-7), count (8-11), code (12-15).

conf
yes - persistent, no - ephemeral

reach
yes - reachable, no - unreachable

auth
ok, yes, bad, and none

condition
Displays the current selection status

last_event
Displays the current event report

cnt
Displays the number of events since the last time the code changed

Display peer variables - (`ntpq -c rv`)
Displays the server information. Select the association ID from the drop-down area. See system variables or peer variables to determine NTP authentication problems.

The following output for *system* variables allows you to determine NTP authentication problems:

status
Specifies the system status word. It consists of four fields: system leap indicator bits (0-1), current synchronization source code (2-7), number of events since the last time the code changed (8-11), and the most recent event message coded (12-15).

version
Specifies the NTP software version and build time.

processor
Specifies the hardware platform and version.

system
Specifies the operating system and version.

leap
Specifies the leap warning indicator (0-3).

stratum
Specifies the number of hops away from the source (1-15).

precision
Specifies the precision of the time of the target system.

rootdelay
Specifies the total roundtrip delay to the primary reference clock.

rootdisp
Specifies the total dispersion to the primary reference clock.

peer
Specifies the system peer association ID.

tc
Specifies the time constraint and poll exponent (3-17).

mintc
Specifies the minimum time constraint (3-10).

clock
Specifies the date and time of day.

refid
Specifies the reference ID or kiss code. The kiss codes include the following:

ACST
Specifies the manycast server.

AUTH
Specifies the authentication error.

AUTO
Specifies the Autokey sequence error.

BCST
Specifies the broadcast server.

CRYPT
Specifies the Autokey protocol server.

DENY
Specifies the access denied server.

INIT
Specifies the association initialized.

MCST
Specifies the multicast server.

RATE
Specifies the rate exceeded.

TIME
Specifies the association timeout.

STEP
Specifies the step time change.

reftime
Specifies the reference time.

offset
Specifies the combined offset of server relative to this host.

sys jitter
Specifies combined system jitter.

frequency
Specifies frequency offset (PPM) relative to hardware clock.

clk_wander
Specifies clock frequency wander (PPM).

clk_jitter
Specifies clock jitter.

tai
Specifies TAI-UTC offset (s).

leapsec
Specifies NTP seconds when the next leap second is/was inserted.

expire
Specifies NTP seconds when the NIST leap seconds file expires.

host
Specifies the Autokey host name for this host.

ident
Specifies the Autokey group name for this host.

flags
Specifies host flags.

digest
Specifies OpenSSL message digest algorithm.

signature
Specifies OpenSSL digest/signature scheme.

update
Specifies NTP seconds at last signature update.

cert
Specifies certificate subject, issuer, and certificate flags.

until
Specifies NTP seconds when the certificate expires.

The following output for *peer* variables allows you to determine NTP authentication problems:

associd
Specifies the associate ID.

status
Specifies the system status word. It consists of four fields: peer status code bits in hexadecimal (0-4), current selection status (5-7), number of events since the last time the code changed (8-11), and the most recent event message coded (12-15).

srcadr/srcport
Specifies the source (remote) IP address and port.

dstadr/dstport
Specifies the destination (local) IP address and port.

leap
Specifies the leap warning indicator (0-3).

stratum
Specifies the number of hops away from the source (0-15).

precision
Specifies the precision of the time of the target system.

rootdelay
Specifies the total roundtrip delay to the primary reference clock.

rootdisp
Specifies the total dispersion to the primary reference clock.

refid
Specifies the reference ID or kiss code. The kiss codes include the following:

ACST
Specifies the manycast server.

AUTH
Specifies the authentication error.

AUTO
Specifies the Autokey sequence error.

BCST
Specifies the broadcast server.

CRYPT
Specifies the Autokey protocol server.

DENY
Specifies the access denied server.

INIT
Specifies the association initialized.

MCST
Specifies the multicast server.

RATE
Specifies the rate exceeded.

TIME
Specifies the association timeout.

STEP
Specifies the step time change.

reftime
Specifies the reference time.

reach
Specifies the reach register (octal).

unreach
Specifies the unreach counter.

hmode
Specifies the host mode (1-6).

pmode
Specifies the peer mode (1-5).

hpoll
Specifies the host poll mode (3-17).

ppoll
Specifies the peer poll mode (3-17).

headway
Specifies the headway for the peer variables. The headway is defined for each source as the interval between the last packet set or received and the next packet for that source.

flash
Specifies the flash status word.

offset
Specifies the filter offset.

delay
Specifies the filter delay.

dispersion
Specifies the filter dispersion.

jitter
Specifies the filter jitter.

ident
Specifies the Autokey group name for this association.

bias
Specifies the unicast/broadcast bias.

xleave
Specifies the interleave delay.

flags
Specifies peer flags.

host
Specifies the Autokey server name.

signature
Specifies OpenSSL digest/signature scheme.

initsequence
Specifies the initial key ID.

initkey
Specifies the initial key index.

timestamp
Specifies the Autokey signature timestamp.

For more information, see the Standard NTP query program website (www.eecis.udel.edu/~mills/ntp/html/ntpq.html).

Customize Console Services

Accessing the Customize Console Services task

This task enables or disables Hardware Management Console services. A Hardware Management Console service is a facility or function of the Hardware Management Console Application that allows the console to interact with other consoles and systems. Enabling a service lets the console provide tasks and perform operations associated with the service. Disabling a service prevents the console from providing tasks and performing operations associated with the service.

Services include:

Remote operation
Controls whether this Hardware Management Console can be operated using a web browser from a remote workstation. If it is enabled for remote web browser access you can also grant remote web browser access by IP address and by user.

Note: The tasks that require removable media cannot be performed remotely.

Remote power off or restart
Controls whether this Hardware Management Console can be powered off or restarted by a user accessing it from a remote workstation. If this service is Disabled, only local users at this Hardware Management Console can use the **Power Off or Restart** task. Only user IDs with system programmer or service roles can access this option.

LIC change
Controls whether this Hardware Management Console provides change management operations for its defined objects and for other Hardware Management Consoles.

Optical error analysis
Controls whether this Hardware Management Console analyzes and reports optical problems for its defined objects. (Optical problems are problems occurring on ESCON or coupling facility channel links.)

Console messenger
Controls whether the console messenger facility is active on this Hardware Management Console or not. The console messenger facility allows users of this Hardware Management Console to send and receive instant messages and broadcast messages to other users of this console and remote consoles.

Fibre channel analysis
Controls whether this Hardware Management Console analyzes and reports fibre channel problems. (Fibre channel problems are problems occurring on FICON channel links.)

Large retrieves from the support system
Controls whether this Hardware Management Console can retrieve internal code changes from the support system for engineering change streams that are expected to contain a large amount of data.

Check held LIC changes during install
Controls whether this console will check the support system for any LIC changes on hold when an install and activate is performed. *Enabled* is the recommended setting in order to prevent activation of released fixes that have later been discovered to have problems.

SSLv3 and RC4 compatibility
Controls whether or not this console supports the SSLv3 (Secure Sockets Layer Version 3) protocol and RC4 (Rivest Cipher 4) cipher when establishing specific secure connections.

Licensed Internal Code security mode
Controls whether to change the Licensed Internal Code security mode to monitor the integrity and security protected firmware file on the Hardware Management Console.

TLSv1.2 only
Controls whether or not this console only allows the Transport Layer Security (TLS) version 1.2 protocol for establishing secure connections.

SSL anonymous cipher suites
Controls whether or not this console supports anonymous cipher suites when establishing specific secure connections.

To enable or disable Hardware Management Console services:

1. Open the **Customize Console Services** task. The Customize Console Services window is displayed.
2. Select **Enabled** or **Disabled** for each service.
3. Click **OK** to complete the task.

Customize Console Services

Use this window to enable or disable console services.

A *console service* is a facility or function of the Hardware Management Console Application that allows the console to interact with other consoles and systems.

The window displays a list of the services for each console service. The controls next to the services initially indicate whether the console services are currently enabled or disabled. You can use the controls, if necessary, to change the settings of the services:

- *Enabling* a service allows the console to provide tasks and perform operations associated with the service.
- *Disabling* a service prevents the console from providing tasks and performing operations associated with the service.

Remote operation

Use this service to control whether this console can be operated using a web browser from a remote workstation. If it is enabled for remote web browser access you can also grant remote web browser access by IP address and by user.

In effect, remote operation of this Hardware Management Console enables remote operation of its defined objects.

Note: The tasks that require removable media cannot be performed remotely and this option cannot be enabled from a remote Hardware Management Console.

Enabled
Specifies that this console allows remote operations.

Disabled
Specifies that this console does not allow remote operations.

Change...
To enable or disable remote operations of this console, click Change....

Remote power off or restart

Use this service to control whether this Hardware Management Console can be powered off or restarted by a user accessing it from a remote workstation. If this service is **Disabled**, only local users at this console can use the **Power Off or Restart** task. Only user IDs with system programmer or service roles can access this option.

Note: This option cannot be enabled from a remote Hardware Management Console.

Disabled
Prevents the power off or restart of this console by a remote user.

Restart console
Allows the restart of this console by a remote user.

Power off and restart
Allows the power off and restart of this console by a remote user.

Change...
To enable or disable remote restart or power off of this console, click Change....

LIC change

Use this service to control whether this Hardware Management Console provides change management operations for its defined objects and for other Hardware Management Consoles.

LIC change must be enabled to:

- Use this console to change Licensed Internal Code (LIC) on its defined Central Processor Complexes (CPCs) and their support elements.
- Use this console to change Licensed Internal Code (LIC) on other Hardware Management Consoles.
- Use the Hardware Configuration Definition (HCD) feature of a Multiple Virtual Storage (MVS™) or OS/390 operating system to distribute HCD Input/Output Configuration Data Sets (IOCDSs) to CPCs defined to this Hardware Management Console.

Note: All CPCs must be defined to the Hardware Management Console if LIC is enabled.

Enabled
To allow using this Hardware Management Console to manage LIC changes for its defined objects and other consoles, select **Enabled**.

Enabling LIC change also allows using HCD to distribute HCD IOCDSs to defined objects.

Disabled
To prevent using this Hardware Management Console to manage LIC changes for its defined objects and other consoles, select **Disabled**.

Disabling LIC change also prevents using HCD to distribute HCD IOCDSs to defined objects.

Optical error analysis

Use this service to control whether this console analyzes and reports optical problems for its defined objects. Optical problems are problems occurring on ESCON or coupling facility channel links.

Enabled
To authorize this console to analyze and report optical problems for its defined objects, select **Enabled**.

Disabled
To exempt this console from analyzing and reporting optical problems for its defined objects, select **Disabled**.

Console messenger

Use this service to control whether the console messenger facility is active on this console or not. The console messenger facility allows users of this console to send and receive instant messages and broadcast messages to other users of this console and remote consoles.

Enabled
To allow users on this console to send and receive instant messages and broadcast messages select **Enabled**.

Disabled
To prevent users on this console from sending or receiving instant messages and broadcast messages select **Disabled**.

Fibre channel analysis

Use this service to control whether this console analyzes and reports fibre channel problems.

Enabled
To authorize this console to analyze and report fibre channel problems, select **Enabled**.

Disabled
To exempt this console from analyzing and reporting fibre channel problems, select **Disabled**.

Large retrieves from support system

Use this service to control whether this console can retrieve internal code changes from the support system for Engineering Change (EC) streams that are expected to contain a large amount of data.

Enabled
To authorize this console to retrieve all available internal code changes from the support system when there is a broadband connection, select **Enabled**.

Disabled
To exempt this console from retrieving from the support system for EC steams that are expected to contain a large amount of data, select **Disabled**. Internal code changes for the exempted EC streams will need to be retrieved from media.

Check held LIC changes during install

Use this service to control whether this console will check the support system for any LIC changes on hold when an install and activate is performed.

Note: *Enabled* is the recommended setting in order to prevent activation of released fixes that have later been discovered to have problems.

Enabled
To authorize this console to check the support system for any LIC changes on hold when an install and activate is performed, select **Enabled**.

Disabled
To exempt this console from checking the support system for any LIC changes on hold when an install and activate is performed, select **Disabled**.

SSLv3 and RC4 compatibility

Use this service to control whether or not this console supports the SSLv3 (Secure Sockets Layer Version 3) protocol and RC4 (Rivest Cipher 4) cipher when establishing specific secure connections. The secure connections affected are as follows:

- Connections between HMCs and their Support Element (for example, in support of maintaining and displaying the status of the Support Elements on the HMC user interface, and in support of any task used to act on a Support Element, such as **Activate**, **Deactivate**, **System Details**).
- Connections between HMCs (for example, in support of the **Customize Data Replication** task and the **Remote Hardware Management Console** task)
- Connections between HMCs and LDAP servers
- Connections between the following Java Applet based tasks and the HMC:
  - **Operating System Messages**
  - **Integrated 3270 Console**
  - **Integrated ASCII Console**
  - **Open Text Console**
  - **OSA Advanced Facilities** (**Advanced Facilities** task when you target an SE) (**Card specific advanced facilities...** > **Manual configuration options...** > **Edit source file**)
- Connections between HMCs and remote servers when using the **Manage Trusting Signing Certificates** option within the **Certificate Management** task
- Connections between HMCs and the support system servers
- Connections between HMCs and proxy servers located between the HMC and support system servers

Disabling this service may cause connections to and from HMCs and SEs to be unsuccessful if the HMCs and SEs are at a level that does not include this corresponding service.

For all other secure connections, the SSLv3 protocol and RC4 cipher are not supported. These connections include:

- Connections to the HMC from remote browsers
- Connections to the HMC HTTP server from Web Services API client applications
- Connections to the Java Message Service (JMS) message broker from Web Services API clients; including the use of Streaming Text Oriented Messaging Protocol (STOMP) and OpenWire protocols
- Connections to the HMC using the Common Information Model (CIM) interface

Enabled
To allow SSLv3 and RC4 to be used, select **Enabled**.

Disabled
To prevent SSLv3 and RC4 from being used, select **Disabled**.

Licensed Internal Code security mode:

Use this service to change the Licensed Internal Code security mode on the console.

Change
To change the Licensed Internal Code security mode, click "Change Licensed Internal Code Security Mode" on page 689.

TLSv1.2 only

Use this service to control whether or not this console only allows the Transport Layer Security (TLS) version 1.2 protocol when establishing secure connections.

Enabled
To only allow the TLS version 1.2 protocol to be used, select **Enabled**.

Note: The SSL v3 compatibility flag is disabled if TLS v1.2 protocol is enabled. Also, if your HMC is at version 2.12.1 or above and it is enabled with this protocol, then you will lose communication if you are connected to an SE at version 2.11.1 or below.

Disabled
To prevent the TLS version 1.2 protocol from being used, select **Disabled**.

SSL anonymous cipher suites

Use this service to control whether or not this console supports anonymous cipher suites when establishing specific secure connections. The secure connections affected are as follows:

- Connections between HMCs and their Support Element (for example, in support of maintaining and displaying the status of the Support Elements on the HMC user interface, and in support of any task used to act on a Support Element, such as **Activate**, **Deactivate**, **System Details**).
- Connections between HMCs (for example, in support of the **Customize Data Replication** task and the **Remote Hardware Management Console** task)

This service cannot be disabled if the HMC manages any system prior to version 2.14.0 as disablement would prevent management of those older systems.

Enabled
To allow anonymous cipher suites to be used, select **Enabled**.

Disabled
To prevent anonymous cipher suites from being used, select **Disabled**.

Additional functions are available from this window:

OK
After you have changed the settings of the services, click **OK**.

Cancel
To end this task without changing any settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Remote Access Settings

Use this window to control whether this console can be operated by using a web browser from a remote workstation. If it is enabled for remote access, you can also grant remote web browser access by IP address and by user.

To allow this Hardware Management Console remote web browser access, select **Enable remote web browser access**. A check mark appears which indicates the remote browser access is enabled and the previous window displays **Enabled** for the **Remote operation** service. If you want to disable the remote browser access, select **Enable remote web browser access** to remove the check mark. **Disabled** is displayed on the previous window for the **Remote operation** service.

IP Access Control

If you enabled the Hardware Management Console remote web browser access, select one of the following IP access controls:

Allow all IP addresses
To allow all the IP addresses listed in the IP Addresses table remote web browser access, select **Allow all IP addresses**.

Allow specific IP addresses
To allow a specific IP address remote browser access, select **Allow specific IP addresses**. Then, select the IP address that you want to allow remote web browser access.

If you select **Allow specific IP Addresses**, use the IP Addresses table to work with specific IP addresses or add new IP addresses.

IP Addresses table
This table displays the IP addresses that you can allow remote web browser access to.

Add
To add an IP address to the table, click **Add**. The Define IP address and mask window is displayed.

1. Make a selection of how you want to define the IP address and mask.
2. Provide a valid IP address (and mask) that is appropriate for that selection.
3. Click **Add** to include this information in the IP Addresses table.

To return to the previous window without adding this information, click **Cancel**.

Edit
To edit a selected IP address, click **Edit**. The Define IP address and mask window is displayed. Make appropriate changes, then click **Update** to include this information in the IP Addresses table. To return to the previous window without changing the information, click **Cancel**.

Remove
To remove an IP address from the table, select the IP address, then click **Remove**. The IP address is no longer available.

User Access Control

Use this table to select which users you want to grant access to remote browser access. You can select one or more names from this table.

Note: This table is only available if you have authorization to manage other user IDs.

More functions are available from this window:

OK
To save the remote access settings, click **OK**.

Cancel
To return to the previous window without making changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Remote Power Off and Restart Settings

Use this window to control whether this Hardware Management Console can be remotely powered off and restarted. Only user IDs with system programmer or service roles can access this option.

Disabled
To not allow remote power off or restart for this HMC, select **Disabled**.

Restart
To allow this HMC to be restarted remotely, select **Restart**.

Power off and restart
To allow this HMC to be powered off and restarted remotely, select **Power off and restart**.

Additional functions are available from this window:

OK
After you have changed the settings, click **OK**.

Cancel
To end this task without changing any settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Licensed Internal Code Security Mode

Use this window to change the Licensed Internal Code security mode for monitoring the integrity and security of protected firmware files on the Hardware Management Console.

Note: The Change Licensed Internal Code Security Mode field displays only if the Firmware Integrity Monitoring feature is installed.

The ACSADMIN default user or a user that has permission to the **Change Licensed Internal Code Security Mode** task can change **Monitor Mode** to **Monitor and Protect Mode**. The SERVICE default user or user that has the Service Representative tasks role or a role based on the Service Representative tasks role can change **Monitor Mode** to **Monitor and Protect Mode** and **Monitor and Protect Mode** to **Monitor Mode**. When changing from **Monitor and Protect Mode** to **Monitor Mode**, you must be physically present at the Hardware Management Console to confirm the console changes when rebooted. Physical presence is not required when changing from **Monitor Mode** to **Monitor and Protect Mode**.

Monitor Mode
To provide threat detection, reporting, and analysis, select **Monitor Mode**. If a potential threat is detected, a hardware message is generated. Additionally, the next level of support will be required to reload the Hardware Management Console .

Monitor and Protect Mode
To provide threat detection, reporting, analysis, and stop all operations when a threat is detected, select **Monitor and Protect Mode**. If a potential threat is detected, a hardware message is generated and the console is stopped. Additionally, the next level of support will be required to reload and restart the Hardware Management Console.

Additional functions are available from this window:

OK
After you have changed the settings of the services, click **OK**.

Cancel
To end this task without changing any settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Customer Information

Accessing the Customize Customer Information task

Note: If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the **Configure Data Replication** task for more information.

This task enables you to customize the customer information for the Hardware Management Console.

To customize your customer information:

1. Open the **Customize Customer Information** task. The Customize Customer Information window is displayed.

2. Select one of the following tabs from the **Customize Customer Information** window.
   - Administrator
   - System
   - Account.
3. Supply the appropriate information in the fields provided.
4. Click **OK** when you have completed the task.

Customize Customer Information

Use this task to specify administrator, system, and account information about the system being installed. Completing these entry fields for each managed system allows your service structure to record necessary contact information.

Proceed through each tabbed page to specify the information for your administrator, system, and account fields.

Customer Information tabs

Provide the fields with contact information.

- Select **Administrator** to set up your administrator information for this system.
- Select **System** to set up information about this system.
- Select **Account** to set up customer account information for this system.

Additional options are available with these pages:

OK
After providing the appropriate information in the fields, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Administrator

Use this page to specify the appropriate administrator information in the provided fields. This data is used to set up your customer contact information for this system.

Company name
Specify your company name in this required field, up to 36 characters.

Administrator name
Specify the name of an individual within the company to contact about the system in this required field, up to 36 characters.

Email address
Specify an email address of a company contact, up to 256 characters.

Phone number
Specify a telephone number for a company contact in this required field, up to 20 numeric characters.

Alternate phone number
Specify an alternate telephone number for a company contact, up to 20 numeric characters.

Fax number
Specify a fax telephone number for a company contact, up to 20 numeric characters.

Alternate fax number
Specify an alternate fax telephone number for a company contact, up to 20 numeric characters.

Street address
Specify the street address where the administrator resides in this required field. Include the building, floor, or room number, up to 68 characters for both address fields, combined.

Street address 2
Specify the second line of the street address where the administrator resides. Include the building, floor, or room number, up to 68 characters for both address fields, combined.

City or locality
Specify the city or locality where the administrator resides in this required field, up to 36 characters.

Country or region
Select the country or region where the administrator resides in this required field.

State or province
Select the state or province where the administrator resides in this required field.

Postal Code
Required to specify the postal or zip code where the administrator resides, up to 12 characters.

System

Use this page to specify the appropriate system information in the fields provided. This data is used to set up your customer account information for this system.

Use the administrator mailing address
Selecting this causes the administrator's mailing address to also be used as the system location.

Street address
Required to specify the street address where the system resides. Include the building, floor, or room number, up to 68 characters for both address fields, combined.

Street address 2
Specify the second line of the street address where the system resides. Include the building, floor, or room number, up to 68 characters for both address fields, combined.

City or locality
Specify the city or locality where the system resides in this required field, up to 36 characters.

Country or region
Select the country or region where the system resides in this required field.

State or province
Select the state or province where the system resides in this required field.

Postal code
Specify the postal or zip code where the system resides in this required field, up to 12 characters.

Account

Use this page to specify the appropriate information in the customer account fields provided. This data is used to set up your customer account information for this system.

If you do not know or are unsure of this information, contact your support structure for assistance.

Customer number
Specify the number assigned to your account for this purchase, up to 10 characters.

Enterprise number
Specify the number assigned to your account as your single enterprise number, up to 10 characters.

Sales branch office
Specify the three-digit sales branch office number that services this system.

Service branch office
Specify the three-digit service branch office number that services this system.

Area
Specify the three-digit area number that services this system.

Customize Network Settings

Accessing the Customize Network Settings task

Note: If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the **Configure Data Replication** task.

This task allows you to view the current network information for the Hardware Management Console and to change the network settings as shown in the following list.

Identification
Contains the host name and domain name of the Hardware Management Console.

Console name
Your Hardware Management Console user name, the name that identifies your console to other consoles on the network. This console name is the short host name, for example:

```
hmcibm1
```

Domain name
An alphabetic name that Domain Name Services (DNS) can translate to the IP address, For example, DNS might translate the domain name 222.example.com to 198.105.232.4. The long host name consists of console name plus a period plus a domain name, for example:

```
hmcibm1.endicott.ibm.com
```

Console description
This description is for your use only. An example might be:

```
Main Hardware Management Console for customer finance
```

LAN Adapters
A summarized list of all (visible) Local Area Network (LAN) adapters. You can select any of the LAN adapters and click **Details...** to open a window allowing you to work with the basic LAN settings.

Basic Settings
This tab allows you to view and change current LAN adapter settings for your console, specifically for IPv4 addresses. This page also allows you to indicate that an IPv4 address is not available.

IPv6 Settings
This tab allows IPv6 configuration settings for the selected network adapter defined on this console. An IPv6 address is always available locally (within the subnet defined).

Name Services
The Domain Name Services (DNS) and domain suffix values.

Routing
Routing information and default gateway information.

The **Gateway address** is the route to all networks. The default gateway address (if defined) informs the Hardware Management Console where to send data if the target station does not reside on the same subnet as this Hardware Management Console. This information is needed to allow the Hardware Management Console to connect to the support system using the internet.

You can assign a specific LAN to be the **Gateway device** or you can choose "any."

You can select **Enable 'routed'** to start the routed daemon. (**Note:** Use this option only if a Routing Information Protocol (RIP) daemon is required.

To customize the network settings:

1. Open the **Customize Network Settings** task. The Customize Network Settings window is displayed.

2. Proceed through the tabs and provide the appropriate information.
3. Click **OK** to save the changes and exit the task.

Note: Depending on the type of change that you make, the network or console automatically restarts or the console automatically reboots.

Customize Network Settings

Use this task to view the current network information for the Hardware Management Console and to make changes to those settings. From this window, you can view or change information pertaining to each of the following tabs.

- Identification
- LAN Adapters
- Name Services
- Routing

Note: Depending on the type of change that you make, the network or console automatically restarts or the console automatically reboots.

OK
To save all changes made to the network configuration and exit this task, click **OK**.

Cancel
To exit this task without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Network Settings tabs

Click a tab to configure the network settings for your console.

Identification
Specify your console name, domain name, and console description to identify your console to the network.

LAN Adapters
Specify the LAN adapter for LAN adapter-specific information.

Name Services
Specify the DNS for configuring the console network settings.

Routing
Specify Routing information for configuring static routing options for the Hardware Management Console.

Identification

Use this page to identify your console.

Specify the console name and the domain name to create the host name, sometimes known as the host name and the domain name suffix. It is important that you specify the correct domain name. If you do not know or are not sure, contact your system administrator.

Specify a console description you can use for your own reference.

Console name
Specify the name or identifier specified as your console name to identify your console on the network.

The console name cannot exceed 16 characters. The characters can consist of:

- Uppercase letters (A - Z)
- Lowercase letters (a - z)
- Numerals (0 - 9)

Note: There are no restrictions on the first character for the console name.

The console name identifies your console to other consoles on the network. If you use a name other than your Hardware Management Console user name, you will not be properly identified on the network.

If you do not know or are unsure of your console name, contact your system administrator.

Domain name
Specify the name assigned as the domain name for your console.

This unique name identifies an Internet site.

If you do not know or are not sure of your domain name, contact your system administrator.

Console description
Specify a description for your Hardware Management Console that you want to use for reference and identification.

This description identifies your console in more detail. For example, your console name can be **HMC12** and your description can be **Main HMC for customer finance**.

LAN Adapters

Use this page to select a Local Area Network (LAN) adapter for adapter-specific information on that LAN adapter.

Select one adapter at a time in the list and click **Details...**.

LAN Adapters
Displays a list of LAN adapters to choose from to view and change the current settings.

Details...
To view and change current settings for the selected LAN adapter, click **Details...**.

LAN Adapter Details

Use this window to view and change the current settings for the selected LAN adapter.

- Basic Settings tab - Specify the LAN adapter settings for your console.
- IPv6 Settings tab - Specify the IPv6 settings for your console.

OK
To save all changes and close this window, click **OK**.

Cancel
To close this window without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Basic Settings

Use this page to view and change current Local Area Network (LAN) adapter settings for your console.

Use the IPv6 Settings tab to specify the IPv6 settings for your console.

LAN interface address
This consists of the Media Access Control (MAC) address on the card, the type of card (Token Ring or Ethernet), and the adapter name (for example, eth0, tr1). These values uniquely identify the LAN adapter and cannot be changed.

A physical LAN adapter receptacle is identified by the Media Access Control (MAC) address ('MAC address') that is printed on the label attached near the receptacle. The information that is displayed for LAN adapters contains the MAC address associated with that receptacle, along with the interface type and name.

Media Speed
Specifies the speed in duplex mode of an ethernet adapter. Use the down arrow and select **Autodetection** unless you have a requirement to specify a fixed media speed.

No IPv4 address
To indicate that an IPv4 address is not available, select **No IPv4 address**.

Obtain an IP address automatically (DHCP)
To allow the Hardware Management Console to obtain an available IP address automatically, select **Obtain an IP address automatically**.

Specify an IP address
To specify that an IP address is to be used, select **Specify an IP address**. Then, in the fields provided, specify a TCP/IP address and TCP/IP interface Network Mask.

TCP/IP interface address
Specify the TCP/IP interface address of the Hardware Management Console.

The TCP/IP interface address is the setting used to identify the Hardware Management Console while using Transmission Control Protocol/Internet Protocol (TCP/IP) for communications in the network. The TCP/IP interface address displays the TCP/IP address of the LAN interface.

The Hardware Management Console network settings are customized for the network it is connected to when it is installed. After that, there is no need to change the network settings while the configuration of the network remains unchanged. Only consider changing the network settings when:

- The Hardware Management Console remains connected to the same network, but a network address or identifier changes.
- The Hardware Management Console remains connected to the same network, but the console is no longer uniquely identified in the network due to the connection of additional devices to the network.
- The Hardware Management Console is connected to a different network.

TCP/IP interface network mask
Specify the TCP/IP interface network mask of the Hardware Management Console adapter.

The TCP/IP network mask, combined with the TCP/IP address, identifies the subnetwork in which the Hardware Management Console adapter is located.

If you do not know or are not sure of the Hardware Management Console IP address/network mask, contact your system administrator.

IPv6 Settings

Use this page for allowing IPv6 configuration settings for the selected network adapter defined on this Hardware Management Console.

Autoconfigure IP addresses
To automatically configure IP addresses, select **Autoconfigure IP addresses** (a check mark appears).

If this option is selected, the autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both). In the case of addresses, whether they should be obtained through the stateless mechanism, the stateful mechanism, or both.

Use DHCPv6 to configure IP settings
To enable stateful autoconfiguration of IPv6 addresses using the DHCPv6 protocol, select **Use DHCPv6 to configure IP settings** (a check mark appears).

Autoconfigured Addresses table
This table lists the automatically configured IPv6 addresses for this adapter.

Static IP Addresses table
This table lists the statically configured IPv6 addresses for this adapter. Addresses can be added or selectively changed or removed from this table.

Add...
To add a valid IPv6 address for this adapter, click **Add...**.

Edit...
To change a selected IPv6 address, click **Edit...**.

Remove
To remove a selected IPv6 address, click **Remove**.

IPv6 Settings

Use this window to add a static IPv6 address.

IPv6 address
Specify a 128 bit IPv6 address.

IPv6 addresses are written as eight groups of four hexadecimal digits. For example, fe80:0:0:0:204:acff:feab:b811 is a valid IPv6 address. If one or more four digit groups are 0000, the zeros can be omitted and replaced with two colons (::).

Prefix length
Specify a prefix length value.

The prefix length value is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.

OK
To save all changes and close this window, click **OK**.

Cancel
To close this window without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Name Services

Use this page to specify Domain Name Services (DNS) for configuring the console network settings.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.jkltoys.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all Domain names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

DNS enabled
To enable the Domain Name Services (DNS), select **DNS enabled** (a check mark appears). You may want to enable DNS because you have DNS servers for mapping IP addresses to host names.

To disable the DNS, deselect **DNS enabled**.

DNS Server Search Order
Displays the order in which the DNS server search is performed.

Add
To add the IP address to the list of configured DNS servers, click **Add**. The New DNS Server window is displayed. The following functions are available from this window:

DNS Server Address
Specify an IP address of the DNS server to be searched for mapping the host names and IP addresses in the **DNS Server Address** input area.

OK
To add the new DNS server address to the DNS Server Search Order list, click **OK**.

Cancel
To return to the previous window without adding a new DNS server address, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove
To delete a selected IP address from the list, click **Remove**.

Move Up
To move a selected IP address up in the list, click **Move Up**.

Move Down
To move a selected IP address down in the list, click **Move Up**.

Note: The DNS Server Search Order list is available only when the **DNS enabled** check box is selected.

Domain Suffix Search Order
Displays the order in which a domain suffix search is performed.

Add
To add a domain suffix to the list, click **Add**. The New Domain Suffix window is displayed. The following functions are available from this window:

Domain Suffix
Specify a domain suffix in the **Domain Suffix** input area.

OK
To add the new domain suffix to the Domain Suffix Search Order list, click **OK**.

Cancel
To return to the previous window without adding a new domain suffix, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove
To delete a selected domain suffix from the list, click **Remove**.

Move Up
To move a selected domain suffix up in the list, click **Move Up**.

Move Down
To move a selected domain suffix down in the list, click **Move Up**.

Note: The DNS Suffix Search Order list is available only when the **DNS enabled** check box is selected.

Note: If you do not know or are not sure of the IP address or the domain suffix of the DNS servers, consult your network administrator.

Routing

Use this page to specify routing information for configuring the console network settings. You can add, delete, or change routing entries and specify routing options for the Hardware Management Console.

Routing Information

This displays the Hardware Management Console's current static routing information. Click **New...** to add a new routing entry, **Change...** to edit the selected routing entry, or **Delete** to remove selected routing entries and specify routing options for the Hardware Management Console.

The routing information table displays:

Type
Net

Specifies a network-specific route. With a net route, the destination address is the TCP/IP address of a particular network. All TCP/IP communications destined for that network are routed using the TCP/IP address of the router, unless a host route also applies for the communication to the destination host address. When a conflict occurs between a host and net route, the host route is used.

Host

Specifies a host-specific destination. With a host route, the destination address is the TCP/IP address of a particular host. All TCP/IP communications destined for that host are routed through the router using the router address as the TCP/IP address.

Destination
Displays the TCP/IP address of the destination host, network, or subnet.

Gateway
Displays the TCP/IP address of the next hop in the path to the destination.

Subnet Mask
Displays the subnet mask used by network interfaces to add routes.

Interface
Displays the name of the network interface that is associated with the table entry.

Default Gateway Information

Gateway address
Displays the current gateway address. To change this default information, specify a new gateway address.

Note: The default gateway is the route to all networks. The default gateway address informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside the area, it is usually because of an incorrectly configured default gateway.

Gateway device
Displays the current gateway device. To change this default information, use the down arrow to choose a Gateway device.

Enable 'routed'
To enable the network routing daemon, select **Enable 'routed'**.

Note: Use this option only if a Routing Information Protocol (RIP) daemon is required. If you are not sure if this daemon is required, consult your network administrator.

- If a check appears this enables the routing daemon, 'routed'.
- If no check appears (to disable) this stops it from running and prevents any routing information from being exported from this Hardware Management Console.

Route Entry

Use this window to manage static routing information.

Route Type
Select a Route type:

Net
Specifies that a network is the target for this route. With net route, the destination address is the TCP/IP address of a particular network. All TCP/IP communications destined for that network are routed through the router using the TCP/IP address of the route, unless a host route also applies for the communication to the destination host address. When a conflict between a host and net route occurs, the host route is used.

Host
Specifies that a host is the target for this route. With a host route, the destination address is the TCP/IP address of a particular host. All TCP/IP communications destined for that host are routed through the router using the router address as the TCP/IP address.

Destination
Specify the TCP/IP destination network host or subnet address.

Gateway
Specify the TCP/IP gateway address for routing the IP packets. This must be in 32-bit dotted-decimal notation.

Subnet mask
Specify the subnet mask to use as the network mask when adding a route. This is the subnet work address for the host portion of the IP address. Network interfaces can use different subnet masks, providing the capability of adding routes by specifying a subnet mask (variable subnet routes). You must specify a subnet mask when adding a route, in 32-bit dotted-decimal notation.

Adapter
Select the adapter by using the down arrow. This is the name of the network adapter that is associated with the table entry.

OK
To save all changes and close this window, click **OK**.

Cancel
To close this window without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Outbound Connectivity

Accessing the Customize Outbound Connectivity task

This task allows you to customize the internet connectivity options for the Hardware Management Console used to connect to the support system. The connection can only be initiated by the Hardware Management Console. The support system never attempts to initiate a connection to the Hardware Management Console.

Before you can customize the outbound connectivity for the Hardware Management Console, you must first decide which Hardware Management Consoles will handle call-home requests that are initiated by this Hardware Management Console.

1. Open the **Customize Outbound Connectivity** task. The Call-Home Server Consoles window is displayed.
2. You can click **Configure...** to configure this console as a local call-home server. The Outbound Connectivity Settings window is displayed.
3. Click **Cancel** to end this task without making changes, otherwise continue customizing outbound connectivity settings.

Customize Outbound Connectivity

The **Customize Outbound Connectivity** task allows you to customize for outbound connectivity for the Hardware Management Console to use to connect to the support system. Use this task to:

- Configure this Hardware Management Console to perform Remote Support Facility functions on behalf of itself, systems it manages (when configured to "act as a call-home server" in the CPC Object Definition), and other HMCs through an existing internet connection. See the “Add or Change Object Definition” on page 382 task.
- Configure the set of call-home server consoles that may handle call-home requests initiated by this console.

Notes:

- The support system never attempts to initiate a connection to the Hardware Management Console.
- Connections can only be initiated by the Hardware Management Console.
- If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data specified in this task might change depending on automatic

replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the **Configure Data Replication** task.

- See the **Remote support facility** section from the **Introduction** for more information about the Remote Support Facility.

Configure...
To configure this Hardware Management Console as a call-home server, select **Configure...**. The Outbound Connectivity Settings window is displayed. When configured as a call-home server, this Hardware Management Console is listed in the Call-Home Server Consoles table with a type of **Local**.

Call-Home Server Consoles
Use this table to manage the set of call-home server consoles that may handle call-home requests initiate by this Hardware Management Console. This table displays the current set of call-home servers configured and available to handle call-home requests initiated by this Hardware Management Console, and whether they are local, discovered automatically, or added to the configuration.

From this window you can:

Add...
To add a Hardware Management Console to handle call-home requests initiated by this Hardware Management Console, click **Add...**. This may be useful when you have a call-home server Hardware Management Console that is not discovered. Added call-home servers are listed in the Call-Home Server Consoles table with a type of **Added**. **Configure...** must be used to configure this Hardware Management Console as a call-home server since it requires additional connectivity information.

Remove
To remove an added call-home server Hardware Management Console, select one then click **Remove**.

Use discovered call-home server consoles
To allow any discovered call-home server console to handle call-home requests initiated by this Hardware Management Console, select **Use discovered call-home server consoles**. A Hardware Management Console is discovered under the following circumstances:

- It is at the same level or higher as the source Hardware Management Console.
- It has been enabled to call-home and the Outbound Connectivity Settings window has been configured.
- It is configured to communicate on the same TCP/IP subnet as the source Hardware Management Console.

When selected, discovered call-home server consoles are listed in the Call-Home Server Consoles table with a type of **Discovered**.

Additional functions from this window include:

OK
To accept changes you made and exit the task, click **OK**.

Cancel
To close this window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Call-Home Server Console

Use this window to provide an IP address or host name that you want added to the list of call-home server consoles. If the option is available, you can also add a descriptive comment that relates to the IP address or host name.

IP address or host name
Specify the IP address or host name that you want added to the list of call-home server consoles.

Comment
If this option is available, specify a descriptive comment about the IP address or host name you are adding.

Add
To add the specified IP address to the list of call-home server consoles, click **Add**.

Cancel
To close this window without making changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Outbound Connectivity Settings

Use this window to configure and test outbound connections between this machine and the support system through an existing internet connection. This internet connection may be a:

- Direct connection from your console to the Internet, or
- Connection to an SSL proxy server at your installation that connects to the Internet.

The *traditional* support system is no longer supported on HMC Version 2.15.0. Any references to "support system" now refer to the *enhanced* support system.

Select **Enable the local console as a call-home server** to allow the local Hardware Management Console to connect to the support system for call-home requests through an existing internet connection.

A configured outbound connectivity connection flows over the console's default gateway to the internet. In order for the console to successfully use the Internet, the following items must be properly configured in the **Customize Network Settings** task:

- The console must have a Local Area Network (LAN) adapter that is connected to a network with internet access. This may be a direct internet connection, or an internet connection from an SSL proxy.
- The LAN adapter must be configured with a default gateway that provides access to the Internet (or SSL proxy).
- Using the support system requires a Domain Name Server (DNS) to be configured on your console, unless the connection is through an SSL proxy, which has a DNS configured.

All requests to the support system are sent to **esupport.ibm.com** on port **443** (esupport.ibm.com:443). If a firewall is in place between the HMC (or SSL proxy) and the Internet, it must allow outgoing TCP/IP connections to this destination. If the IP addresses of the support system are required for your firewall or proxy configurations, then see the lists below based on your Internet Protocol selection.

- Internet connectivity that uses IPv4 requires outbound connectivity to the following IP addresses:
  - 129.42.54.189
  - 129.42.56.189
  - 129.42.60.189
- Internet connectivity using the IPv6 requires outbound connectivity to the following IP addresses:
  - 2620:0:6c0:200:129:42:54:189
  - 2620:0:6c0:200:129:42:56:189
  - 2620:0:6c2:200:129:42:60:189
- If an SSL Proxy is used to access the internet, you can configure the Hardware Management Console to send an HTTP Connect request to the proxy with either the IP address (as shown above), or using the support system's host name (see **Resolve IP addresses on console**).

Enable the local console as a call-home server
To allow the local Hardware Management Console to connect to your support system for call-home requests using an existing internet connection, select **Enable the local console as a call-home server**. When selected, **Configure Internet Options** become available.

Use SSL Proxy Connection to Internet
To enable by using an SSL proxy to access the Internet, select **Use SSL Proxy Connection to Internet**.

Address
Specify the IPv4 or IPv6 TCP/IP address or host name of the SSL proxy to be used to access the Internet, up to 256 alphanumeric characters.

The format of the IPv4 address is four decimal numbers, representing the four bytes of the IP address, which is separated by periods (for example, `9.60.12.123`).

The format of the IPv6 address can be eight groups of four hexadecimal digits, which are separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`). However, for simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or a double colon is used in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

Port
Specify the IP port number of the SSL proxy to be used to access the Internet, a number from 1 to 65535.

Resolve IP addresses on console
When an SSL proxy connection is used to forward call-home requests to the support system, you can use this option to control the type of address being sent to the HTTP CONNECT request to your SSL proxy. This performs a DNS lookup of the support system's host name on the HMC, and then uses the resulting IP address in the connections to the proxy.

To allow the Hardware Management Console to direct your SSL proxy to connect to one of the previously specified IP addresses, select **Resolve IP addresses on console**. Do not select this option if you prefer to have the Hardware Management Console direct your SSL proxy to connect to the support system by host name.

This configuration requires your SSL proxy to translate this host name into its corresponding IP address.

Use SSL proxy authentication
To enable authentication with the SSL proxy, select **Use SSL proxy authentication**.

User
Specify the user name used to authenticate with the SSL proxy. The name may not contain the colon (:) character.

Note: For Microsoft Windows based proxy servers, by using NT LAN Manager (NTLM), enter your domain and user name in this field that is separated by a "\". For example: `domain\username`. Also, when you authenticate with NT credentials, the Hardware Management Console passes its name as the workstation name, such as "HMC1".

Password
Specify the password used to authenticate with the SSL proxy.

Confirm password
Respecify the password used to authenticate with the SSL proxy to confirm the password.

Internet Protocol
To select an Internet protocol, use the down arrow on the entry field and select one. The selected protocol determines what version of IP addresses the console uses for connections to your service provider.

The value that you select here must reflect the internet protocol that is used by your installation. Most installations use Internet Protocol Version 4 in which addresses appear in the format representing the four bytes of the IPv4 address, which is separated by periods (for example, 9.60.12.123) to access the internet. If you are unsure of the internet protocol that is used by your installation, contact your network administrator.

Note: If an SSL proxy is used to access the internet, use of the Internet Protocol depends on the value of **Resolve IP addresses on console**:

- If **Resolve IP addresses on console** is selected, the protocol that is selected here must reflect the internet protocol that is used by the SSL proxy to connect to the internet. It may differ from the protocol that is used by the console to connect to the SSL proxy.
- If **Resolve IP address on console** is not selected, the Internet Protocol option is ignored. In that case, IP address resolution including the internet protocol determination is determined by the SSL Proxy.

Available values are:

IPv4
Internet Protocol version 4 only. This is the default.

IPv6
Internet Protocol version 6 only.

IPv6 and IPv4
The Hardware Management Console will first attempt to connect to the service provider by using Internet Protocol. This selection provides redundancy in case a version of IP addresses temporarily fail.

Test...
To test the availability of an SSL connection over the Internet, click **Test...**.

This tests connectivity to the support system and verifies service entitlement.

If you selected **IPv6 and IPv4**, you will be able to see the availability of SSL over the internet by using each protocol.

OK
To continue the task with your selections, click **OK**.

Apply
To apply any unsaved changes, click **Apply**.

Note: If there are unsaved changes, this is required to perform a full connectivity test.

Cancel
To exit this task without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Test Internet

Use this window to test an existing Internet connection that allows the console to perform call-home functions over an encrypted SSL connection.

Test Status
Displays the diagnostic information about the test for connection availability.

The overall test statuses are:

Test completed successfully
Indicates that the Hardware Management Console (HMC) was able to establish a connection to the support system and validate entitlement for the HMC and all managed CPCs.

Test failed
Indicates that a test connection to the support system failed.

Test partially successful
The partial success indicates that an entitlement check has failed for the HMC or one or more managed systems.

You can find more detailed help on the following messages:

Connection failed to the enhanced support system
A probable cause for this error is your firewall has not yet enabled the Hardware Management Console to connect to the IP addresses associated with the enhanced infrastructure. For more

information on how to connect to the enhanced support system, refer to "Outbound Connectivity Settings" on page 701 or the **Remote support facility** section under **Introduction** in the help table of contents.

Additionally, using the enhanced support system now requires that the Hardware Management Console has DNS enabled, with one or more valid name servers defined. The one exception is if an SSL Proxy is being used for outbound connections ***and*** the **Resolve IP addresses on the console** option is not enabled.

The Hardware Management Console's DNS settings are available from the **Customize Network Settings** task.

Failed to encrypt the socket: address:port

Probable causes for this failure include:

- A problem with the X509 certificates that are used for the SSL handshake.
- An external firewall blocking the connection from the Hardware Management Console to the service provider. Write down the address and port from the error message and consult with network security to determine what needs to be done to allow access to this address and port through the firewall.

Repeat the test. If the failure continues to occur, contact your next level of support for problem resolution and have them collect the HMC log and problem determination data.

Socket Exception: javax.net.ssl.SSLHandshakeException

If a proxy server is defined, then this error might be seen when the proxy attempts to perform SSL inspection by terminating SSL connections at the proxy instead of the support system.

To resolve, you must import the proxy's SSL certificate into the HMC as a trusted certificate. See the "Manage Trusted Signing Certificates" on page 446 section of the **Certificate Management** task for more details.

If a proxy server is not in use, and you receive this error, notify your service representative or your network administrator.

The current Outbound Connectivity Settings require DNS be enabled on the console in order to connect to the enhanced support system.

Indicates that DNS is not enabled on the HMC, though required based on the current Outbound Connectivity settings.

Review the Hardware Management Console DNS settings available in the **Customize Network Settings** task.

Socket Exception: java.net.NoRouteToHostException: No route to host

Probable causes for this exception include:

- A problem with the network interface on the Hardware Management Console making outbound connections impossible. This might be as simple as the network cable has been disconnected. Check the Hardware Management Console network cables to ensure they are connected.
- The proxy server has been configured with an address that does not exist. If you configured a proxy server, ensure that its address has been entered correctly in the **Use SSL proxy Address** field. This address is obtained from the network administrator, or proxy owner.

Make necessary changes and retry the test. If the failure continues to occur, contact your next level of support for problem resolution and have them collect the HMC log and problem determination data.

Socket Exception: java.net.ConnectException: Connection timed out OR java.net.SocketTimoutException - Connection timed out

Indicates the HMC does not have connectivity to the support system or the proxy server.

If a Proxy is not defined, a probable cause is a local firewall between the HMC and the support system is blocking the request. Refer your network administrators to "Outbound Connectivity Settings" on page 701 for details on the Outbound Connectivity requirements and ensure the HMC

has network connectivity to the support system. If the failure continues to occur, contact your next level of support for problem resolution and have them collect the HMC log and problem determination data.

If a Proxy is defined, a probable cause for this exception is that the proxy server has been configured with an incorrect address or port. Ensure that the proxy server's address and port has been entered correctly in the **Use SSL proxy address** field. This address is obtained from the network administrator, or proxy owner. Make necessary changes and retry the test. If the failure continues to occur, contact your network administrator, or proxy owner.

Socket Exception: java.net.ConnectException: Connection refused

A probable cause for this exception is that the proxy server port has been configured with the wrong port number. Ensure that the proxy server port has been entered correctly in the **Use SSL proxy Port** field. This port number is obtained from the network administrator, or proxy owner. Make necessary changes and retry the test. If the failure continues to occur, contact your next level of support for problem resolution and have them collect the HMC log and problem determination data.

Socket Exception: java.net.UnknownHostException: esupport.ibm.com

Indicates a DNS issue. Connecting to the enhanced support system without a proxy requires that:

1. HMC has DNS properly configured
2. HMC has connectivity to the DNS server or servers, and
3. DNS server or servers are able to resolve the host names.

Review the Hardware Management Console's DNS settings available in the **Customize Network Settings** task.

Socket Exception: java.io.IOException: Failed to authenticate to proxy server; Response: (Proxy Authentication Required)

Probable causes for this exception include:

- The user or the password that is used to authenticate to the proxy server has been configured incorrectly. Ensure that the user and password that is used to authenticate to the proxy server has been entered correctly in the **User** and **Password** fields of the **Outbound Connectivity Settings** window. The user and password are obtained from the network administrator or proxy owner.
- The proxy server requires a user and password for authentication and these have not been configured. Obtain a user and password from the network administrator or proxy owner. Configure them by selecting **Authenticate with SSL proxy** on the **Outbound Connectivity Settings** window and specify user and password in the **User** and **Password** fields.

Make necessary changes and retry the test. If the failure continues to occur, contact your next level of support for problem resolution and have them collect the HMC log and problem determination data.

Invalid configuration for proxy

A probable cause for this error is that the port that has been configured to connect to the proxy server has been set to zero. Zero is an invalid value for this port. Verify the value that is entered in the **Port** field on the **Outbound Connectivity Settings** window. If the value is zero, replace it with the port value for connecting to the proxy. This value is obtained from the network administrator, or proxy owner. Repeat the test. If the failure continues to occur, contact your next level of support for problem resolution and have them collect the HMC log and problem determination data.

Skipping the test transaction: There are pending changes you must first apply.

This message is displayed if a test is run, and there are unsaved changes that are made to the Outbound Connectivity Settings. It is recommended that you perform a test both before and after you apply the changes.

Warning: No entitlement record was found for managed system

The given system (identified by machine type and serial number) is not entitled for service.

Warning: Estimated (upload or download) speed: x Mbit/s - Less than the recommended: 10 Mbit/s
Downloads of console recovery images and fixes may take an excessive amount of time to download.

Test transaction failed: Reason: Machine is not registered.
This message appears if the HMC itself is not associated to an entitled system. However, this HMC would still be a fully functioning callhome server for managed systems that are entitled.

Start
To begin the test, click **Start**.

Stop
To end the test, click **Stop**.

Cancel
To return to the previous window without testing, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Product Engineering Access

Accessing the Customize Product Engineering Access task

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables or disables the authorization of Product Engineering access to the Hardware Management Console. Once product engineering is enabled to access the Hardware Management Console you can decide whether or not product engineering can access the system remotely.

With access authority and a specified time frame, Product Engineering can log on the Hardware Management Console with an exclusive user identification that provides tasks and operations for problem determination.

Product Engineering access is provided by a reserved password and permanent user identification. You cannot view, discard, or change the password and user identification, but you can control their use for accessing the Hardware Management Console.

To customize product engineering access:

1. Open the **Customize Product Engineering Access** task. The Customize Product Engineering Access window is displayed.
2. Select the appropriate accesses for product engineering or remote product engineering.
3. Click **OK** to save the changes and exit the task.

Customize Product Engineering Access

Use this window to set the authorization and a length of time for Product Engineering (PE) access to the console. When you enable Product Engineering access, you can also decide whether or not to allow Product Engineering to remotely access the console.

When access is authorized, a product engineer can use an exclusive user ID and reserved password to log on to the console that provides tasks for problem determination.

You cannot view, discard, or change the password and user identification, but you can control its use for logging on to the application by customizing the console's PE access setting.

Note: Although PE access does not compromise the security of your system or the console, customizing the console's PE access setting completes your control of user access to them.

Product Engineering Access

Disable product engineering access
To prevent logging on the application with an exclusive user ID reserved for Product Engineering, select **Disable product engineering access**.

Enable product engineering access
To allow logging on the console with an exclusive user ID reserved for Product Engineering, select **Enable product engineering access**.

You can optionally provide a length of time, between 1 minute and 24 hours, that the product engineering access is available.

Remote Product Engineering Access (Restart required)

Disable remote product engineering access
To prevent Product Engineering remote access to the console with an exclusive user ID, select **Disable remote product engineering access**.

Note: Restart your login session for this option to take effect.

Enable remote product engineering access
To allow Product Engineering remote access to the console with an exclusive user ID, select **Enable remote product engineering access**.

Note: Restart your login session for this option to take effect.

OK
To close this window with the current selection, click **OK**.

Apply
To save the current selection without closing the window, click **Apply**.

Cancel
To close this window without saving the changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Remote Service

Accessing the Customize Remote Service task

Note: If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the **Configure Data Replication** task.

This task allows you to customize the Hardware Management Console for using remote service. ***Remote service*** is two-way communication between the console and the support system for conducting automated service operations. Using remote service reduces the operator interaction needed to complete some service operations and provides some console tasks with another source or destination for sending or receiving service information. The connection can only be initiated by the Hardware Management Console. The support system never attempts to initiate a connection to the Hardware Management Console. Some examples for enabling remote service:

- Allows the Hardware Management Console to automatically report a problem and request service through the support system.
- Uses the support system as a source for retrieving internal code changes and as a destination for transmitting service data.

When remote service is disabled, error information and requests for service must be done through voice communications.

To configure remote service:

1. Open the **Customize Remote Service** task. The Customize Remote Service window is displayed.
2. Select **Enable remote service requests**. This option allows the Hardware Management Console to establish remote connections to the support system.
3. To enable automatic service calling for problems, select **Authorize automatic service call reporting**. This option allows the Hardware Management Console to automatically report problems and get service through its remote connection to the support system.
4. You must customize the telephone number the console's hardware messages will include as an option for reporting problems.
5. When you complete the necessary fields, click **OK** to save your changes.

Customize Remote Service

Use this window to customize the console for using remote service.

Remote service is two-way communication between the console and the support system for the purpose of conducting automated service operations. Using remote service reduces the operator interaction needed to complete some service operations and provides some console tasks with another source or destination for sending or receiving service information.

The controls you will use to customize the console's remote service settings are determined by whether you want to enable or disable remote service.

Controls for enabling remote service

Enable remote service if you want to allow console connections to the support system.

Select Enable remote service requests to enable remote service. If it is not selected remote service is disabled.

After enabling remote service, customize how service calls are reported:

Authorize automatic service call reporting
: To set the console to automatically report problems and request service, select **Authorize automatic service call reporting**.

Customer Service Center Telephone Number
: This field displays the telephone number the console's hardware messages will include as an option for reporting problems and requesting service if automatic service call reporting is disabled. You can change the telephone number whenever necessary.

Additional functions are available from this window:

OK
: To continue with the remote service configuration you have selected, click **OK**.

Cancel
: To exit this window without configuring for remote service, click **Cancel**.

Help
: To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Enable remote service requests

To enable remote service, select **Enable remote service requests**.

About remote service

Remote service is two-way communication between the console and the support system for the purpose of conducting automated service operations.

- *Enable* remote service if you want to allow console connections to the support system (a check mark appears).

- *Disable* remote service if you do *not* want to allow console connections to the support system (a check mark does not appear).

Using remote service reduces the operator interaction needed to complete some service operations and provides some console tasks with another source or destination for sending or receiving service information. For example, by using remote service:

- You can allow the console to automatically report problems and request service through the support system.
- You can use the support system as a source for retrieving internal code changes.
- You can use the support system as a destination for transmitting service data.

Authorize automatic service call reporting

If remote service is enabled, select **Authorize automatic service call reporting** to set the console for authorization to automatically report problems that require service (referred to as *automatic service call reporting*).

About automatic service call reporting

The console issues hardware messages to notify console operators of problems that require service. When automatic service call reporting is authorized, the console can automatically report problems and request service through console connections to the support system.

Otherwise, when automatic service call reporting is *not* authorized, a console operator must decide how to report problems and request service. A problem's hardware message provides two options:

- Calling the customer service center to speak to a service representative.
- Or manually authorizing the console to make the service call through a console connection to the support system.

Customer Service Center Telephone Number

Displays the telephone number of the customer service center console operators can call to speak to a service representative about product problems and service.

If remote service is disabled, the console includes the customer service center telephone number in the hardware messages it issues to notify console operators of problems that require service. Such hardware messages typically instruct the console operator to call the customer service center to report the problem and request service.

But the customer service center telephone number is required *even when remote service is enabled*. The console may not always be able to automatically report a problem that requires service, and will issue a hardware message to instruct the console operator to call the customer service center instead. For example:

- The console may fail to connect to the support system while making a service call.
- The console may not be authorized to automatically make service calls.

  Note: In this case, hardware messages for problems that require service provide two options: calling the customer service center or manually authorizing the console to make the service call.

Customize Scheduled Operations

Accessing the Customize Scheduled Operations task for the Hardware Management Console

This task enables you to do some of the following:

- Schedule an operation to run at a later time

- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or console.

You can schedule the times and dates for automatic licensed internal code updates and backup of critical hard disk data for the Hardware Management Console. Using this task displays the following information for each operation:

- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions.

An operation can be scheduled to occur one time or it can be scheduled to be repeated. You will be required to provide the time and date that you want the operation to occur. If the operation is scheduled to be repeated, you will be asked to select:

- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

The operations that can be scheduled for the Hardware Management Console are:

Single step code changes retrieve and apply
Schedules an operation to copy (retrieve) the Hardware Management Console internal code changes to the Hardware Management Console hard disk and then install (apply) the code changes.

Backup critical hard disk information
Schedules an operation to make a backup of critical hard disk information for the Hardware Management Console.

Accept internal code changes
Schedules an operation to make activated internal code changes a permanent working part of the licensed internal code of the Hardware Management Console.

Install and activate concurrent code changes
Schedules an operation for installing and activating internal code changes retrieved for the Hardware Management Console.

Remove and activate concurrent code changes
Schedules an operation for removing and activating internal code changes installed for the Hardware Management Console.

Note: After changes are accepted, they cannot be removed.

Retrieve internal code changes
Schedules an operation to copy internal code changes from a remote service support system to the Hardware Management Console hard disk.

Retrieve internal code changes for defined CPCs
Schedules an operation to copy internal code changes for Central Processor Complexes (CPCs) from a remote support system to the hard disk of the Support Element for each of the CPCs.

Transmit system availability data
Schedules a transmittal of system availability data from the Hardware Management Console to the Product Support System (PSS).

Audit and Log Management
Schedules an operation to generate an audit report on selected types of audit data.

To schedule operations on the Hardware Management Console:

1. Open the **Customize Scheduled Operations** task. The Customize Scheduled Operations window is displayed.
2. Click **Options** from the menu bar to display the following menu options:
   a. To add a scheduled operation, click **New...**. The Add a Scheduled Operation window is displayed.
   b. To delete a scheduled operation, select the operation you want to delete, then click **Delete**. The Confirm the action window is displayed.
   c. To edit a scheduled operation, select the operation you want to edit, then click **Edit**. The Edit a Scheduled Operation window is displayed.
   d. To return to the Hardware Management Console workplace, click **Exit**.
3. Click **View** from the menu bar to display the following menu options:
   a. To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details...**.
   b. To change the list of scheduled operations viewed within a certain time range, point to **View** and then click **New Time Range...**.
4. Click **Sort** from the menu bar to sort the scheduled operations, select a sort group that you prefer.

Accessing the Customize Scheduled Operations task targeting one or more systems or an appropriate object

This task allows you to schedule the times and dates for automatic licensed machine code updates and backup of critical hard disk data for one or more systems or an appropriate object. Calling customize scheduled operations displays all scheduled operations, their scheduled dates and times, the functions, and the numbers of repetitions.

You can schedule an operation to occur one time or to be repeated. You are required to specify the time and date that you want the operation to occur. If the operation is scheduled to repeat, you are asked to select:

- The day or days of the week that you want the operation to occur (optional)
- The interval or time between occurrence (required)
- The total number of repetitions (required).

The operations that can be scheduled on a Hardware Management Console , targeting one or more systems or an appropriate object, include the following:

Single step code changes retrieve and apply
Schedules an operation to copy (retrieve) the Support Element internal code changes to the Support Element hard disk and then install (apply) the code changes.

Backup critical hard disk information
Schedules an operation to make a backup of critical hard disk information for the selected systems or object.

Accept internal code changes
Schedules an operation to make activated internal code changes a permanent working part of the licensed internal code of selected systems or object.

Install and activate concurrent code changes
Schedules an operation for installing and activating internal code changes retrieved for the selected systems or object.

Remove and activate concurrent code changes
Schedules an operation for removing and activating internal code changes installed for the selected systems or object.

Retrieve internal code changes
Schedules an operation to copy internal code changes from a remote service support system to the Support Element hard disk.

Activate selected CPC
Schedules an operation for activating a selected CPC (system).

Note: This operation is not available when one or more managed systems have DPM enabled.

Start
Schedules an operation for starting a stopped IBM Dynamic Partition Manager (DPM) system.

Note: This operation is available only when one or more managed systems have DPM enabled.

Stop
Schedules an operation for stopping a running IBM Dynamic Partition Manager (DPM) system.

Note: This operation is available only when one or more managed systems have DPM enabled.

Deactivate (Power off) selected CPC
Stops the operating system, deallocates resources, clears associated hardware and powers off the system.

Note: This operation is not available when one or more managed systems have DPM enabled.

Access external time source
Schedules an operation to obtain data from an external time source by dialing out to the Hardware Management Console for the purpose of synchronizing the time of the selected systems that are participating in a Server Time Protocol (STP) Coordinated Timing Network (CTN).

Note: This operation is available only on systems prior to zEC12.

Transmit attestation report
Transmits console firmware integrity reports to the service support system.

Transmit system availability data
Sends service data generated by the selected object to the support system. This data is used to ensure a high level of availability.

Manage Processor Sharing
Schedules the controls through which you can set weights, weight capping, and absolute capping for partitions and partition groups with shared processors on a specific IBM Dynamic Partition Manager (DPM) system.

Note: This operation is available only when one or more managed systems have DPM enabled.

Transmit vital product data
Transmits the type of Vital Product Data (VPD) that you want transmitted to the support system.

Change LPAR Controls
Schedules an operation to change the defined capacity, WLM, absolute capping, processing weights, and initial capping value for processor types assigned to one or more active logical partitions. If a partition specified does not exist or is not active at the time the operation runs, then the entire scheduled operation will not be executed (it will fail). For more detailed information, see “Change Logical Partition Controls” on page 487.

Note: This operation is not available when one or more managed systems have DPM enabled.

Change LPAR Group Controls
Schedules an operation to change a group assignment for logical partitions and to change the group capacity and absolute capping value for processor types that are assigned to one or more active logical partitions. For more detailed information, see “Change Logical Partition Group Controls” on page 497.

At the time this operation runs, it will fail if the following conditions are not true.

- All groups in the request must exist and contain at least one active partition.
- In order for a partition to be added to a group or removed from a group, the partition must exist and be active.

Note: This operation is not available when one or more managed systems have DPM enabled.

Audit and Log Management
Schedules an operation to generate an audit report on selected types of audit data.

Set Power Saving
Schedules an operation to reduce the average energy consumption of a target system including a IBM Dynamic Partition Manager (DPM) system that is enabled.

To schedule any of the previous operations:

1. Select one or more systems or an appropriate object.
2. Open the **Customize Scheduled Operations** task. The Customize Scheduled Operations window is displayed.
   - To add a scheduled operation, point to **Options** from the menu bar, then click **New...**. The Add a Scheduled Operation window is displayed. From this window select an operation that you want performed and select an object to perform if you targeted more than one system for this task, then click **OK**. The Set up a Scheduled Operation window is displayed. In this window select the date and time for the operation to occur and whether or not it repeats, then click **Save**.
   - To delete a scheduled operation, select the operation you want to delete, point to **Options** from the menu bar, then click **Delete**. The Confirm the action window is displayed, click **OK** to remove the scheduled operation.
   - To edit a scheduled operation, select the operation you want to edit, then click **Edit**. The Edit a Scheduled Operation window is displayed.
   - To view a scheduled operation, select the operation you want to view, point to **View** from the menu bar, then click **Schedule Details...**. The Details window is displayed.
   - To change the list of scheduled operations viewed within a certain time range, point to **View** from the menu bar, then click **New Time Range...**. The Change the Time Range window is displayed.
   - To sort the scheduled operations, point to **Sort** from the menu bar, then click one of the sort groups that appear.
3. To return to the Hardware Management Console workplace, point to **Options** from the menu bar, then click **Exit**.

Customize Scheduled Operations

Use this window to customize a schedule for certain operations for the Hardware Management Console and selected systems including systems on which IBM Dynamic Partition Manager (DPM) is enabled.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times.

Select a scheduled operation for the Hardware Management Console, for a selected system including a system on which IBM Dynamic Partition Manager (DPM) is enabled from the list, if necessary, then select a choice from the menu bar.

Notes:

- All times displayed on the main Scheduled Operations user interface are local to the target of the operation. For example, an operation is scheduled to execute at 10:00 A.M. on a remote, managed system in a timezone that is different than where the Hardware Management Console is located. The operation will execute at 10:00 A.M. local to the remote, managed system, not at 10:00 A.M. local to the Hardware Management Console.
- If you are creating a Start, Stop, or Manage Processor Sharing scheduled operation for a system on which IBM Dynamic Partition Manager (DPM) is enabled, it must be done on the Hardware Management Console. However, you can view those scheduled operations from this system.

Click **Options** on the menu bar to select the following:

- **New...** to create a new scheduled operation
- **Delete** to remove a scheduled operation

- **Edit** to change or update the properties of a selected scheduled operation
- **Refresh** to update the current list of scheduled operations
- **Select All** to choose all scheduled operations currently displayed
- **Deselect All** to deselect all scheduled operations that were currently selected
- **Exit** to exit this task.

Click **View** on the menu bar to select the following:

- **Schedule Details...** to display schedule information for the selected scheduled operation.
- **New Time Range...** to change the list of scheduled operations viewed within a certain time range.

Click **Sort** on the menu bar to sort how you want to view the list of scheduled operations; **By Date and Time**, **By Object**, or **By Operation**.

Click **Help** to display help for the current window.

You can find more detailed help on the following elements of this window:

Options

From **Options** on the menu bar, click:

New...
To create a new scheduled operation. Adding a scheduled operation requires that you specify a type of operation, and set the schedule.

Delete
To remove the selected scheduled operations from the list. One or more scheduled operations must be selected to remove them from the list of scheduled operations, otherwise the option is unavailable. Delete a single or repeated scheduled operation when you no longer want or need the operation performed at its scheduled date and time. Deleting a repeated operation cancels all scheduled repetitions of the operation.

A confirmation window allows you to confirm or cancel your request to delete the selected operation.

Edit
To change or update the properties of a selected scheduled operation. The Edit a Scheduled Operation window is displayed. You can make any applicable updates, then click **Save** to proceed with those changes.

Note: This option is only available when you select an existing scheduled operation.

Refresh
To update the list of scheduled operations with the current schedules for the console and selected system including a system on which IBM Dynamic Partition Manager (DPM) is enabled. Initially, the list of scheduled operations displays the current schedules of the console, selected CPC, or DPM CPC. Afterwards, while using the task, the list is updated automatically only when you add or delete scheduled operations. But this console does not automatically update the list when the current schedule of the console or selected system including a system on which IBM Dynamic Partition Manager (DPM) is enabled changes. The current schedule of console, selected system changes when:

- A scheduled operation is performed
- Any console is used to add a new operation to the schedule
- Any console is used to delete an operation from the schedule.

Refresh the list of scheduled operations, at any time, to ensure it displays the current schedule.

Select All
To select, at once, all the operations in the list.

Deselect All
To deselect, at once, all the operations in the list.

Exit
To close the window and return to the console workplace.

Sort

From **Sort** on the menu bar, click:

By Date and Time
To sort the scheduled operation list according to date in descending order with the most recent operation at the top.

By Object
To sort the scheduled operation list according to object name in alphabetical order.

By Operation
To sort the scheduled operation list according to operation in alphabetical order.

Scheduled operations table

Target
Displays the name of the object the scheduled operation applies to.

You can schedule operations on the following objects:

- The Hardware Management Console itself
- Any selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Date
Identifies the day the scheduled operation will occur.

Time
Identifies the time of day the scheduled operation will occur.

Operation
Identifies the scheduled operation.

Remaining Repetitions
Identifies how many times the scheduled operation will occur.

Description
Provides a brief description of the scheduled operation.

Add a Scheduled Operation

Use this window to create a new scheduled operation for the Hardware Management Console and any selected system including a system on which IBM Dynamic Partition Manager (DPM) is enabled. The list of operations available is based on the target with which the task is launched.

On the Hardware Management Console, select an operation, then click **OK** to schedule the operation.

For a selected system including a system on which IBM Dynamic Partition Manager (DPM) is enabled, select one that is listed, select an operation, then click **OK** to schedule an operation.

You can find more detailed help on the following elements of this window:

Select an Object

Select one system including a system on which IBM Dynamic Partition Manager (DPM) is enabled to assign a scheduled operation.

The first object is selected by default, but you can select any one object you want to schedule the selected operation.

Note: This selection does not appear in the window when you are performing this task on the Hardware Management Console.

Select an Operation

Accept internal code changes
Schedules an operation to make activated internal code changes a permanent working part of the licensed internal code of the Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Activate
Schedules an operation for activating a selected system.

Note: This operation is not available when one or more managed systems have DPM enabled.

Backup critical hard disk information
Schedules an operation to make a backup of critical hard disk information for this Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Deactivate (Power off)
Schedules an operation for deactivating a selected system.

Note: This operation is not available when one or more managed systems have DPM enabled.

Install and activate concurrent code changes
Schedules an operation for installing and activating internal code changes retrieved for this Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Remove and activate concurrent code changes
Schedules an operation for removing and activating internal code changes installed for this Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Retrieve internal code changes
Schedules an operation to copy internal code changes from a remote service support system to the Hardware Management Console hard disk.

Note: This operation is available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Retrieve internal code changes for defined CPCs
Schedules an operation to copy internal code changes for systems from a remote service support system to the Hardware Management Console hard disk.

Note: This operation is available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

“Start” on page 720
Schedules an operation for starting a stopped system or partition on which IBM Dynamic Partition Manager (DPM) is enabled.

Note: This operation only appears when you are targeting a system on which IBM Dynamic Partition Manager (DPM) is enabled.

“Stop” on page 720
Schedules an operation for stopping a running system or partition on which IBM Dynamic Partition Manager (DPM) is enabled.

Note: This operation only appears when you are targeting a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Single step code changes retrieve and apply
Schedules an operation to copy (retrieve) the Hardware Management Console internal code changes to the Hardware Management Console hard disk and then install (apply) the code changes.

Note: This operation is available on a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Transmit system availability data
Schedules a transmittal of system availability data from the selected system including a system on which IBM Dynamic Partition Manager (DPM) is enabled to the Product Support System (PSS).

“Transmit attestation report” on page 720
Schedules a transmittal of console firmware integrity reports to the service support system.

“Manage Processor Sharing” on page 720
Schedules an operation to manage processor sharing on a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Note: This operation only appears when you are targeting a system on which IBM Dynamic Partition Manager (DPM) is enabled.

“Transmit vital product data” on page 720
Transmits the type of Vital Product Data (VPD) that you want transmitted to the support system.

“Change LPAR Controls” on page 720
Schedules an operation to change the defined capacity, WLM, absolute capping, processing weights, and initial capping value for processor types assigned to one or more active logical partitions.

Note: This operation is not available when one or more managed systems have DPM enabled.

“Change LPAR Group Controls” on page 721
Schedules an operation to change a group assignment for logical partitions and to change the group capacity and absolute capping value for processor types assigned to one or more active logical partitions.

Note: This operation is not available when one or more managed systems have DPM enabled.

Audit and Log Management
Schedules an operation to generate an audit report on selected types of audit data.

Note: This operation is available on a system on which IBM Dynamic Partition Manager (DPM) is enabled.

“Set Power Saving” on page 721
Schedules an operation to reduce the average energy consumption of a system component or group of components.

Note: This operation is only available when the appropriate feature is installed. This operation is available on a system on which IBM Dynamic Partition Manager (DPM) is enabled.

OK
To schedule the operation for the objects you have selected, click **OK**.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Accept internal code changes

To schedule an operation to make activated internal code changes a permanent working part of the licensed internal code of the Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled, select **Accept internal code changes**.

Activated internal code changes are accepted only if they are more recent than internal code changes currently accepted.

Accepting internal code changes permanently modifies the licensed internal code of the Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled. You cannot remove accepted changes to restore the licensed internal code to a previous state.

Activate

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an activation of the selected object, select **Activate**.

Activating an object makes it operational.

Scheduling an activation on a system requires you to provide additional information on the **Options** tab in the Set up a Scheduled Operation window. You must select a reset profile to use with the operation, and you must specify whether activation is to start if the system is already activated.

Backup critical hard disk information

To schedule an operation to make a backup of critical hard disk information for this Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled, select **Backup critical hard disk information**.

Making a backup, copies information from the hard disk to a removable media or to an FTP server.

Critical hard disk information is information stored on the hard disk of a Hardware Management Console that is unique to it or stored on a system that is unique to its system.

Critical data includes most data written to the hard disk by console operations and procedures. For example:

- User profiles saved by access administrators to control who can log on the console.
- Information saved by operators performing tasks to customize console settings.
- Information saved by service representatives performing tasks to install or repair the console.

Note: Files stored on the hard disk for user applications, if any, will be saved only if their archive attributes are set on.

Selecting this option requires that you only set a schedule for the operation.

Deactivate

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule a deactivation of the selected object, select **Deactivate**.

Deactivating a selected system stops its processor activity and turns off its power.

Install and activate concurrent code changes

To schedule an operation for installing and activating internal code changes retrieved for this Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled, select **Install and activate concurrent code changes**.

Installing and activating internal code changes for the console temporarily changes the console's licensed internal code. Installing retrieved internal code changes makes them eligible for being activated. Activating installed changes makes them operational.

Note: Installing and activating the console's internal code changes requires rebooting it. Rebooting the console will temporarily prevent using it, so you should schedule this operation for a time when the console is not in use. However, if a user is logged on when this scheduled operation starts, a message will notify the user that the operation will reboot the console. The message will allow the user to choose either to continue the operation and reboot the console or to cancel the operation instead.

Remove and activate concurrent code changes

To schedule an operation for removing and activating internal code changes installed for this Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled, select **Remove and activate concurrent code changes**.

Removing and activating internal code changes for the console restores the licensed internal code they changed. Removing installed internal code changes restores the internal code. Then activating the restored internal code makes it operational.

Removed changes are not erased. They remain stored on the console and can be installed again at any time.

Note: Removing and activating the console's internal code changes requires rebooting it. Rebooting the console will temporarily prevent using it, so you should schedule this operation for a time when the console is not in use. However, if a user is logged on when this scheduled operation starts, a message will notify the user that the operation will reboot the console. The message will allow the user to choose either to continue the operation and reboot the console or to cancel the operation instead.

Retrieve internal code changes

To schedule an operation to copy internal code changes from a remote service support system to the Hardware Management Console hard disk, select **Retrieve internal code changes**.

Note: This operation is available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Retrieving internal code changes makes them available for installation and activation as the working part of the licensed internal code of the Hardware Management Console. Retrieved internal code changes do not affect the operation of the console until they are installed and activated.

To use this option, automatic dialing must be enabled for this Hardware Management Console. Also, its remote service settings must be customized with remote service enabled and include a valid telephone number for the service support system.

Retrieve internal code changes for defined systems

To schedule an operation to copy internal code changes for systems from a remote service support system to the Hardware Management Console hard disk, select **Retrieve internal code changes for defined systems**.

Note: This operation is available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Retrieving internal code changes copies them from the source to the Hardware Management Console hard disk, to make them available for installation and activation as the working part of the licensed internal code of one or more systems. Retrieved internal code changes do not affect the operation of a system until they are installed and activated.

To use this option, automatic dialing must be enabled for this Hardware Management Console. Also, its remote service settings must be customized with remote service enabled and include a valid telephone number for the service support system.

Single step code changes retrieve and apply

To schedule an operation to copy (retrieve) the Hardware Management Console internal code changes to the Hardware Management Console hard disk and then install (apply) the code changes, select **Single step code changes retrieve and apply**.

The task:

- Verifies the system environment
- Processes a Backup Critical Data function
- Accepts all previously activated internal code changes
- Retrieves internal code changes for the support system
- Connects to the support system and downloads any internal code change **hold** status for pending internal code changes
- Installs and activates the internal code changes.

Selecting this option requires only that you set a schedule for the operation.

Start

Note: This operation is available only on a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an operation for starting a stopped system or partition on which IBM Dynamic Partition Manager (DPM) is enabled, select **Start**.

Stop

Note: This operation is available only on a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an operation for stopping a running system or partition on which IBM Dynamic Partition Manager (DPM) is enabled, select **Stop**.

Transmit system availability data

To schedule a transmittal of system availability data from the selected system to the Product Support System (PSS), select **Transmit system availability data**.

System availability data is information used by the PSS to ensure a high level of system availability.

When this operation is selected, all service data generated by the selected objects during the specified interval will be sent to the PSS at the specified time.

Transmit attestation report

To schedule an operation for transmitting console firmware integrity reports to the support system, select **Transmit attestation report**.

The attestation report is information used by the support system to monitoring the integrity and security of protected firmware files on the Hardware Management Console.

When this operation is selected, this operation schedules transmission of an attestation report to the support system.

Manage Processor Sharing

Note: This operation is only available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an operation for setting weights, weight capping, and absolute capping for partitions and partition groups with shared processors on a system on which IBM Dynamic Partition Manager (DPM) is enabled, select **Manage Processor Sharing**.

Transmit vital product data

To schedule an operation for transmitting vital product data from the Support Element of all CPCs that are defined to your Hardware Management Console to the support system, select **Transmit vital product data**.

When this operation is selected, this operation schedules transmission of vital product data to the support system.

Change LPAR Controls

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an operation to change the defined capacity, WLM, absolute capping, processing weights, and initial capping value for processor types that are assigned to one or more active logical partitions, select **Change LPAR Controls**.

If a specified partition does not exist or is not active at the time the operation is scheduled to run, the scheduled operation will not be executed.

You are not allowed to change the image profiles with this operation.

Note: A scheduled operation is run based on the active partitions at the time the scheduled operation is executed. It is possible to create a scheduled operation while one IOCDS is being used and to have a different IOCDS active when the scheduled operation is executed. As long as the partition names that are contained in the scheduled operation are active when the operation is scheduled to execute, it runs regardless of the IOCDS.

For more detailed information, see "Change Logical Partition Controls" on page 487.

Change LPAR Group Controls

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an operation to change a group assignment for logical partitions and to change the group capacity and absolute capping values for processor types that are assigned to one or more active logical partitions, select **Change LPAR Group Controls**.

At the time this operation runs, it will fail if the following conditions are not true.

- All groups in the request must exist and contain at least one active partition.
- In order for a partition to be added to a group or removed from a group, the partition must exist and be active.

It is possible to create a scheduled operation while one IOCDS is being used and to have a different IOCDS active when the scheduled operation is executed.

You are not allowed to change the image profiles with this operation.

For more detailed information, see "Change Logical Partition Group Controls" on page 497.

Audit and Log Management

To schedule an operation that generates and offloads an audit report select **Audit and Log Management**.

To generate the audit report for a scheduled operation:

- Select the report type to be generated
- Select the audit data types to be included in the report from the **Audit data types** list
- Optionally, select **Limit event based audit data to a specific number of days** and specify the number of preceding days included in the report
- Specify the FTP destination offload information for the generated audit report
- Click **Save** to include the audit data report information for the scheduled operation.

Scheduling an Audit and Log Management requires additional information on the **Options** tab in the Set up a Scheduled Operation window.

Set Power Saving

Note: This operation is only available when the appropriate feature is installed. This operation is available on a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an operation to set power saving settings for the system, click **Set Power Saving**.

Use this operation to schedule the reduction of the average energy consumption of a system component or group of components. You can closely manage power allocations within the physical limits of your data center.

See the **Set Power Saving** task for more information.

Note: This operation fails if the configuration of the system does not match the configuration of the system when the operation was scheduled.

Details

Note: This menu choice remains unavailable until you select a scheduled operation.

Displays the schedule information for the selected operation and system.

Options tab
Displays a summary of additional information when a scheduled operation was created from the **Options** menu selection. To exit this window and return to the previous window, click **OK**.

Object
Displays the name of the Hardware Management Console or system including a system on which IBM Dynamic Partition Manager (DPM) is enabled the operation is scheduled for.

Operation
Identifies the operation that is scheduled for the Hardware Management Console or selected system including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Window begins at
Displays the date and the time of day that begins the time window in which the operation will occur.

Window length
Displays the length of the time window, in minutes, in which the operation will occur.

Remaining repetitions
Displays the remaining number of times the operation will be repeated.

Time interval between each repetition
Displays the amount of time between each repetition.

OK
To exit this window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Change the Time Range

Use this window to change the subset of scheduled operations listed, to list more or fewer operations.

Initially, the list includes all scheduled operations. The time range is indefinite while all operations are listed.

To list a subset of the scheduled operations, you can specify a definite time range as a number of days, weeks, or months from the current date. Then only those operations scheduled within the time range are listed.

New Time Range
To enter a new time range, specify or click the scroll arrows to select a number (1 through 99) in the entry field, then select a unit of time for the number.

Days
To specify the time range as a number of days, select **Days**.

Weeks
To specify the time range as a number of weeks, select **Weeks**.

Months
To specify the time range as a number of months, select **Months**.

Display all scheduled operations
To list all scheduled operations, select **Display all scheduled operations**.

Note: Selecting this choice makes the **New time range** entry field unavailable.

OK
To close this window and save the changes you have made to the time range list, click **OK**.

Reset
To reset the time range list to the previously saved values, click **Reset**.

Cancel
To close this window without saving any changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Set up or Edit a Scheduled Operation

Use this window to set up or edit an existing scheduled operation for performing a selected operation on the Hardware Management Console or selected systems including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Note: All times displayed on the main Scheduled Operations user interface are local to the target of the operation. For example, an operation is scheduled to execute at 10:00 A.M. on a remote, managed system in a timezone that is different than where the Hardware Management Console is located. The operation will execute at 10:00 A.M. local to the remote, managed system, not at 10:00 A.M. local to the Hardware Management Console.

Click on the **Date and Time** and **Repeat** tabs to set up scheduled operations, then click **Save**. Click on the tabs to toggle between the pages. If available, click on the **Options** tab for additional parameters.

Description
Allows you to add a description of the scheduled operation in the **Description** input area. This information is displayed in the **Description** column of the "Scheduled operations table" on page 715.

"Date and Time" on page 723
Specifies the date, time, and a time window to perform a scheduled operation.

"Repeat" on page 724
Specifies the scheduled operation to be performed once or repeatedly.

"Options" on page 725
Provides additional options that you can include when scheduling certain operations.

"Backup Settings" on page 731

Note: This tab is available when you are scheduling a **Backup critical hard disk information** operation.

Allows you to choose the console backup destination.

Scope

Note: This tab is available when the **Transmit system availability data** operation is selected.

Allows you to select the scope of the data collected. Choose either WEEKLY or DAILY from the **Select the scope of this operation** drop-down arrow. This value should be in agreement with the frequency specified under the **Repeat** tab.

"Backup SE Schedule Operation" on page 731
Allows you to choose the back up Support Element destination.

"Single Step Settings" on page 732

Note: This tab is available when you are scheduling a **Single step code changes retrieve and apply** operation.

Allows you to choose the internal code bundle to apply and the backup destination.

Save
To save the settings you inputted for the set up of a scheduled operation, click **Save**.

Cancel
To discard the changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Date and Time

Use this page to set the date, time, and a time window to perform a scheduled operation.

Note: If you make no changes to this page, the default settings will be the current date and time, and the time window will be 10 minutes.

The time window provides a "window of opportunity" in which the scheduled operation must start. For example, if a scheduled operation requires the use of removable media, but the removable media is currently being used by another task, you can delay starting that task up to the point that it remains within the time window. If it does not start within the time window, it is marked as a failure for that iteration. If necessary, it will be scheduled for the next scheduled start, regardless of success or failure. For instance, if a Backup Critical Data operation is scheduled to start at 10:00 A.M. with a time window of 60 minutes, but the removable media is in use when the operation begins, the operation will be tried again some number of times until it begins successfully or 60 minutes elapses. If the operation does not begin successfully at 11:00 A.M., that iteration is marked as a failure. A log entry is made and the next iteration, if any, is scheduled.

Date
Set the date when you want the operation performed. Specify the month, day, and year (mm/dd/yy) or click the clock icon, using the arrows, to select the month, day, and year.

Note: When parsing dates with an abbreviated year pattern, such as "YY", the year must be interpreted relative to some century. The parsing code provided by the Java runtime does this by adjusting dates to be within 80 years before and 20 years after the current date. For example, if the current date is June 4, 2008, the string "01/11/12"would be interpreted as January 11, 2012 while the string "05/04/64" would be interpreted as May 4, 1964.

Time
Set the time when you want to begin the time window for performing the operation. Specify the hours, minutes, seconds (hh:mm:ss), and time of day (AM or PM) or click the clock icon to specify the hours, minutes, seconds, and select AM or PM.

Time Window
Select the length of time within which a scheduled operation must start. Specify how long you want to wait to try the operation again in case a scheduled operation fails; for example, if a device is not available.

Repeat

Use this page to set up a scheduled operation to be performed once or repeatedly.

Single or Repeated
Specifies whether to perform the scheduled operation once or repeatedly.

Set up a single scheduled operation
To perform the scheduled operation once, click **Set up a single scheduled operation**.

The scheduled operation is performed only once, starting at the date and time specified, and within the time window selected on the **Date and Time** page.

When this choice is selected, the other controls on this page become unavailable and cannot be used. The information is not needed for a single scheduled operation.

Set up a repeated scheduled operation
To perform the scheduled operation repeatedly, click **Set up a repeated scheduled operation**.

Select the **Days of the Week** you want to repeat the operation and specify under **Options** how often to repeat it.

A repeated scheduled operation is performed first on the selected day of the week that is on, or most closely after, the date and time specified on the **Date and Time** page. Then the operation is repeated according to the information you provide on this page.

Note: When you save these settings only one scheduled operation is created and only the next scheduled operation is displayed. You can select a scheduled operation on the main panel and select **Options** > **Edit** to see when the subsequent executions will occur or to make changes. You can also display this information by selecting **View** > **Scheduled Detatils...**.

Days of the Week
Select the day or days of the week you want to perform the scheduled operation.

Options
Specify the Interval and Repetitions and if the scheduled operation should repeat forever.

Interval
Specify or select the number of weeks to elapse before performing the scheduled operation again on each selected day.

For example, if you want the operation performed every week, on each selected day, specify 1. If you want it performed every fourth week, on each selected day, specify 4.

The interval can be from 1 to 26 weeks.

This is a required field. You must specify an interval to set up a repeated scheduled operation.

Repetitions
Specify or select the total number of times you want the scheduled operation performed.

For example, if you want the operation performed once every week for one year, select a day of the week to perform the operation, specify 1 in the **Interval** field, then specify 52 in this field for the number of repetitions.

The number of repetitions can be from 1 to 100.

This is a required field. You must specify a number of repetitions to set up a repeated scheduled operation.

Note: If **Repeat indefinitely** is selected, the **Repetitions** field is unavailable and input inhibited.

Repeat indefinitely
Select **Repeat indefinitely** if you want the scheduled operation repeated forever.

The scheduled operation is repeated at the selected interval without an end time or date.

For example, if you want the operation performed once every week forever, select a day of the week to perform the operation, specify 1 in the **Interval** field, then select **Repeat indefinitely**.

Note: If **Repeat indefinitely** is selected, the **Repetitions** field is unavailable and input inhibited.

Options

The **Options** tab is displayed for the following operations.

Activate

This page appears for the **Activate** operation.

When you want to schedule the **Activate** operation use this page to select a profile to use to perform the operation (Profile tab) and to select whether, you want an activation to start as scheduled when the system has a status of operating or exceptions (Force tab).

Note: This option is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

You can find more detailed help on the following elements of this window:

Profile

A profile provides additional information necessary to perform an operation. For example, scheduling an operation for activating the system requires selecting the activation profile you want used when the activation is performed.

The list displays the profiles available for the selected operation.

- **Profile** - Displays the name of the profile.
- **Description** - Displays a brief description of the profile, if available.

Force

A scheduled activation is performed unconditionally when system status is anything other than operating or exceptions. But since activation disrupts system activity, you must authorize activating a system when its status is operating or exceptions.

Select **Force a scheduled activation** to authorize activating a system even if its status is operating or exceptions.

If you do not select **Force a scheduled activation** the activation will not be started while the target has a status of operating or exceptions.

If the target status is anything other than operating or exceptions, it is activated. If the system status becomes anything other than operating or exceptions within the time window for starting the operation, it is activated.

Change LPAR Controls

This page appears for the **Change LPAR Controls** operation.

When you want to schedule the **Change LPAR Controls** operation, use this page to set scheduled defined capacity, scheduled WLM, scheduled absolute capping, weights, and initial capping value for the selected processor type (CP, ICF, IFL, zAAP, and/or zIIP). Select one or more partition names then continue to specify the wanted defined capacity, WLM, absolute capping, weight, and initial capping values in the **Defined Capacity**, **WLM**, **Scheduled Initial Weight**, **Scheduled Minimum Weight**, **Scheduled Maximum Weight**, **Scheduled Initial Capping**, and **Absolute Capping** columns. When all the values are specified to be included in the scheduled operation, click **Save**.

Note: This option is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

You can find more detailed help on the following elements of this window:

Edit Absolute Capping

Use this window to specify the absolute capping of the selected logical partitions that share processors.

No change
To choose not to change the absolute capping value, select **No change**.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR Group Controls

This page appears for the **Change LPAR Group Controls** operation.

When you want to schedule the **Change LPAR Group Controls** operation, you can use the "Capacity and Capping" on page 727 tab to verify or change the values for group capacity or absolute capping. You can also use the "Members" on page 728 tab to verify or change the group member name. When all the values are set, click **Save**.

Note: You can use the **Capacity and Capping** or **Members** tabs to update the values for capacity, capping, or group member name before this operation runs.

At the time this operation runs, it will fail if the following conditions are not true.

- All groups in the request must exist and contain at least one active partition.
- The partition must exist and be active, in order for a partition to be added to a group or removed from a group.

Note: This option is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

You can find more detailed help on the following elements of this window:

Capacity and Capping

The **Capacity and Capping** tab includes a table that lists the LPAR groups that might be included in this scheduled operation. Each row in the table represents a group that you might want to include for this scheduled operation. If you want to set a scheduled operation for the group capacity and absolute capping, select one or more groups. For each selection, you can "Set Group Capacity" on page 727 and "Set Group Absolute Capping" on page 727 for the processor types that are displayed in the table.

Set Group Capacity

Use this window to update the scheduled group capacity value for a selected group. The initial selection that appears in this window is the value that is displayed by the clicked hyperlink.

No change
To choose not to change the scheduled group capacity value, select **No change**.

Group capacity (0 to 2147483647)
To specify the group capacity value, select **Group capacity (0 to 2147483647)**. In the input area, specify a number in the range of 0 to 2147483647, but no more than 10 characters.

OK
To proceed with the selection and return to the previous window, click **OK**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Set Group Absolute Capping

Use this window to update the group absolute capping for a selected partition. The initial selection that appears in this window is the value that is displayed by the clicked hyperlink.

No change
To keep the value of the number of processors, click **No change**.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)**. In the input area, specify a number in the range of 0.01 to 255.00 in increments of 0.01, but no more than 6 characters.

Note: This value must be a decimal number between 0.01 and 255.00 in increments of 0.01.

OK
To proceed with the selection you made and return to the previous window, click **OK**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Members

The **Members** tab includes a table that lists the partition names that might be included in this scheduled operation. Each row in the table represents a partition name that you might want to include for this scheduled operation. If you want to set a scheduled operation for members, select one or more partitions. For each selection, you can set the desired group from the "Set Member Group Name" on page 728 window.

Set Member Group Name

Use this window to update the scheduled group name for a selected partition. The initial selection that appears in this window is the value that is displayed by the clicked hyperlink.

No change
To keep the value of the scheduled group name, click **No change**.

None
To choose not to specify a scheduled group name, select **None**.

Group name
To specify a scheduled group name, select **Group name**, then enter the name in the input area.

Note: The name cannot be more than 8 characters.

OK
To proceed with the selection and return to the previous window, click **OK**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Audit and Log Management

This page appears for the **Audit and Log Management** operation.

When you want to set the schedule for the **Audit and Log Management** operation use this page to select the "Report type" on page 728, "Range for Event-based Audit Data Types" on page 728, "Offload information" on page 729, and "Audit Data Types" on page 729. When you set the audit and log management values, to be included in the scheduled operation, click **Save**.

You can find more detailed help on the following elements of this window:

Report type

Select the audit data type report to be generated. The supported audit data types of reports are:

HTML
HyperText Markup Language is used to generate an easily viewable report.

XML
eXtensible Markup Language is used to generate a report that is easily parsed by programs for backend processing.

Range for Event-based Audit Data Types

Use this section to limit the selected event based audit data log to a specific number of days and specifying the preceding days to be included in the audit report.

Limit event based audit data to a specific number of days
To limit the report content for the selected event based audit data types to specific number of preceding days, select **Limit event based audit data to a specific number of days**.

Number of preceding days included in report
Specify the number of preceding days used to limit the content of event based audit data types contained in the report.

Offload information

Use this section to specify the FTP destination offload information for the generated audit report.

Host or address
Specify the host name or address used for offloading the generated audit report.

User name
Specify the user name used for FTP authentication when offloading the generated audit report.

File name
Specify the file name used when the generated audit report is transferred to the specified host. The file name should include any leading directory names that may be required to correctly place the report file on the remote host. In order to be able to have periodic reports with unique names the file name can include %D, which will be replaced with the year, month, day, hour, minute, and second of when the report was generated.

Password
Specify the password used for FTP authentication when offloading the generated audit report.

Offload using secure file transfer
To enable offloading of the audit data to a secure FTP connection, select **Offload using secure file transfer**. If you are using secure FTP file transfer you must define a host key for the target system by using the **Manage SSH Keys** task.

Audit Data Types

Select the audit data types that you want included in the scheduled operations audit report from the list.

Note: The audit data types list only displays the data types that the user has authority to view. For example, the "User profiles" data type is only shown to users who are authorized to the **User Management** task.

Manage Processor Sharing

This page appears for the **Manage Processor Sharing** operation.

When you want to schedule the **Manage Processor Sharing** operation use this page to view the “Manage Processor Sharing Options table” on page 729. When you set the manager processor sharing values, to be included in the scheduled operation, click **Save**.

Note: This option is only available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

You can find more detailed help on the following elements of this window:

Manage Processor Sharing Options table

This page displays two tabs, **CP** and **IFL**. A tab is only shown if there are partitions defined with shared processors of that type (i.e. if no partitions use IFLs or if partitions only use dedicated IFLs, the tab is not displayed).

Each processor tab contains a table that lists partitions of the targeted system which IBM Dynamic Partition Manager (DPM) is enabled that have that type of shared processors and the partition cap groups to which they belong. Partitions and groups are displayed in the table even if you do not have access to the managed object.

Select
Initially no table rows are selected and the Scheduled Weight, Scheduled Weight Capping, and Scheduled Absolute Capping cell values are empty. Only the partitions that you select in the table are included in the scheduled operation. The Processors, Current Weight, Scheduled Weight, Current Weight Capping, and Scheduled Weight Capping cells are always blank and non-editable for group rows.

Name
Lists the name of a partition or a partition group. Partitions that do not belong to a group are listed before any table entries for a partition group. If a partition is a member of a group, its table entry is listed only under the group to which it belongs.

Processors
Specifies the number of processors that are defined to the partition. The number of defined processors ranges from the minimum value of 1 to a maximum value of the total number of entitled processors on the system.

Current Weight and Scheduled Weight
Indicates the relative amount of processor time that a specific active partition receives when it is in contention with other active partitions that share the same pool of processor resources. The suggested practice is to specify a processing weight that satisfies the peak workload requirements of the partition.

If you edit this value, enter an integer from 1 - 999. Integer values at the low end of the value range result in less relative processor time; integers at the higher end of the value range result in more relative processor time.

Note: These values only apply to partitions and not groups.

Current Weight Capping and Scheduled Weight Capping
Indicates whether weight capping is in effect for a specific partition. When weight capping is enabled, the partition cannot use more processor time than its weight, relative to other partitions that share the same pool of processor resources, even when additional processor resources are available.

A check mark in the Current Weight Capping column indicates that it is enabled, a dash indicates that it is disabled. This only applies to partitions and does not apply to groups.

To make a change for the partition, select **Enabled** or **Disabled** from the corresponding drop-down list.

Current Absolute Capping and Scheduled Absolute Capping
Indicates whether absolute capping is in effect for a specific partition or for a partition group. When absolute capping is enabled, an active partition, or active partitions in a group, cannot use any more than a specified number of physical processors. To change the absolute capping for a partition or partition group, click on the hyperlink, the "Set Absolute Capping" on page 730 window is displayed.

If you edit this value, enter a value from 0.01 - 255.0, in increments of 0.01. An absolute capping value is required for a partition group.

Save
To proceed with the values you have provided for the scheduled operation, click **Save**.

Cancel
To return to the summary window without creating a scheduled operation, click **Cancel**.

Help
To display help for the current window, click **Help**.

Set Absolute Capping

Use this window to update the absolute capping for a selected partition. The selection that appears in this window is the value displayed by the clicked hyperlink.

Do not change
To keep the value of the number of processors, click **Do not change**.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Note: This value must be a decimal number between 0.01 and 255.00 in increments of 0.01.

OK
To proceed with the selection you have made and return to the previous window, click **OK**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Backup Settings

Use this page to select the destination in which to back up critical data. The backup critical data operation copies critical files from this Hardware Management Console or selected CPCs to a USB flash memory drive, to an FTP server, or to both.

Select your backup destination
Select one of the choices provided in the drop-down.

USB
To choose to have your files backed up to a USB flash memory drive, select **USB** and inset a formatted USB flash memory drive into the drive.

The USB flash memory drive for the **Backup Critical Console Data** task must be formatted with a value label of **ACTBKP**, using the **Format Media** task.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP server
To choose to have your files backed up to an FTP server, choose **FTP server**. Set up a connection to the FTP server from the **Configure Backup Settings** task.

Note: If you have not set up a connection to the FTP server, then a message appears to configure your FTP server. You might also receive a message indicating the transfer rate of the data is not acceptable, you can choose whether or not to continue or cancel this task.

USB and FTP server
To choose to have your files backed up to both a USB flash memory drive and an FTP server, select **USB and FTP server**.

Note: If you have not set up a connection to the FTP server, then a message appears to configure your FTP server. You might also receive a message indicating the transfer rate of the data is not acceptable, you can choose whether or not to continue or cancel this task.

Save
To back up the hard disk information for this console or CPC depending on your selection of the backup destination, click **Save**.

Cancel
To cancel your request to schedule a back up of critical data, click **Cancel**.

Help
To display help for the current window, click **Help**.

Backup SE Schedule Operation

Use this page to select the destination in which to back up Support Element critical data. The backup critical data operation copies critical files from selected systems to a Primary SE, Alternate SE, or FTP server.

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Primary and Alternate SE
To choose to back up files to the hard disk on the Support Elements, select **Primary and Alternate SE**.

Primary SE, Alternate SE, and FTP Server
To choose to back up files to the hard disk on the Support Elements and to an FTP server, select **Primary SE, Alternate SE, and FTP Server**. Set up a connection to the FTP server from the **Configure Backup Settings** task.

Note: If you have not set up a connection to the FTP server, then a message appears to configure your FTP server. You might also receive a message indicating the transfer rate of the data is not acceptable, you can choose whether or not to continue or cancel this task.

Single Step Settings

Use this page to choose which internal code change to apply and the backup destination for a scheduled operation.

Apply all bundles
To choose to apply all the bundles, select **Apply all bundles**.

Apply a specific bundle
To only apply a specific bundle, select **Apply a specific bundle**.

Bundle level
Specify the bundle level in the input area.

USB
To use a USB as the backup destination, select **USB**.

FTP
To use file transfer protocol (FTP) as the backup destination, select **FTP**.

Customize Support Element Date/Time

Accessing the Customize Support Element Date/Time task

This task enables you to update the date and time of the Support Element of a single CPC, multiple CPCs, or a group of CPCs that are defined to this Hardware Management Console. The updated date and time can be the date and time that is currently set for the Hardware Management Console or it can be a date and time that you enter.

Notes:

- A CPC that is synchronized to a time source using either the External Time Reference (ETR) feature or the Server Time Protocol (STP) feature cannot have its date and time customized with this task. However, this task will cause the Support Element to synchronize its time to the time source.
- Depending on your machine type and model the Support Element **Clock** and **Time zone** fields cannot be modified by the Hardware Management Console. In that case, you must use the **Single Object Operations** task to set the Support Element clock and time zone.

For a procedure on changing the Support Element date and time, see the "Changing your time of day clock" topic in the **Introduction** section.

Customize Support Element Date and Time

Use this window to set the battery operated clocks of the Support Element of the selected Central Processor Complexes (CPCs).

Although you use this window to set Support Element clocks, the fields are initialized to the current time, date, and time zone of the battery operated clock of the Hardware Management Console.

Notes:

- Depending on your machine type and model, the time zone of the Support Element can or cannot be changed by the Hardware Management Console.

- Depending on your machine type and model, if you need to set the time zone or time-zone offset of the Support Element, you must use the Hardware Management Console **Single Object Operations** task to make that change. Any time zone change on the Support Element will not modify the time zone on the Hardware Management Console. However, if the Support Element is in a different time zone from the Hardware Management Console, the Hardware Management Console time will be adjusted accordingly even though it is in a different time zone.

Clock
Select **Local** or **UTC** (Universal Time Coordinate) by using the down arrow on the entry field.

Local
Sets the **Time** to the current time of the time zone that you selected.

UTC
Sets the **Time** to the Greenwich Mean Time (GMT) no matter what time zone you have chosen.

Note: You should not specify **Local** when the Time zone specifies **not initialized**. That combination does not guarantee that the actual time zone that is being used is what you really want.

Time
This required field is initialized to the current time of the battery operated clock of the Hardware Management Console.

Specify a new time, if necessary, while setting the battery operated clocks of Support Elements of the selected CPCs. Specify the new time using the same format as shown in the **Time** field. For example, `8:35:00 AM`.

Date
This required field is initialized to the current date of the battery operated clock of the Hardware Management Console.

Specify a new date, if necessary, while setting the battery operated clocks of Support Elements of the selected CPCs. Specify the new date using the same format as shown in the **Date** field. For example, `August 10, 2005`.

Time zone
To select the time zone for the battery operated clocks of Support Elements of the selected CPCs, use the down arrow on the entry field and select one.

Select a city from the list that has the same time as the one you need. For example, if the console is located in Austin, Texas, select **America/Chicago** since that is the city in the list located in the same time zone as Austin.

Note: Depending on your machine type and model determines whether or not the time zone can be set or not. For the Support Elements that cannot be set, the time zone can be used to view what time it is in the different time zone

Use Console Time...
To set the Support Element clocks to the same time and date currently set for the console clock, click **Use Console Time...**.

Use New Time...
To set the Support Element clocks to the time and date currently displayed on the window, click **Use New Time...**.

Refresh
To reinitialize the window's fields to the time and date currently set for the console clock, click **Refresh**.

Cancel
To close this window without saving new settings and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Support Element Date and Time Confirmation

Use this window to confirm or cancel your request to set the battery operated clocks of the Support Elements of the selected CPCs.

The **Object List** lists the names of the selected CPCs; the battery operated clocks of their Support Elements will be set by this operation.

Note: The date and time cannot be changed for some Support Elements.

Yes
To confirm your request to set the Support Element clocks with the settings displayed on this window, click **Yes**.

No
To cancel your request to set the Support Element clocks and return to the previous window, click **No**.

Help
To display help for the current window, click **Help**.

Customize/Delete Activation Profiles

Accessing the Customize/Delete Activation Profiles task

This task enables you to create new activation profiles, customize existing profiles, or delete unwanted profiles that are stored in the Support Element. An activation profile is required for CPC or image activation and defines the IOCDS, storage sizes, and other parameters that will be available when the object is activated.

Note: Depending on your user task role, you may only be able to view this task.

The *DEFAULT RESET*, *DEFAULT IMAGE*, and *DEFAULT GROUP* profiles are the only profiles that can use the same name.

To create new, customize existing, or delete activation profiles:

1. Select one or more objects.
2. Open the **Customize/Delete Activation Profiles** task. The Customize/Delete Activation Profiles List window is displayed.
3. If you selected more than one object for this task, then tabs on the right side of the window allow you to work with the objects you selected.
4. Select a profile from the list, then click an action you want to perform, such as **Customize selected profile**. The Customize Activation Profiles window is displayed. This window uses a tree view to present the activation profile information.

   The tree view located on the left side of the window includes the CPC that you want to work with and its images, if applicable. You can expand on each of these items by clicking on the square and you can then click on each name for more details or to make appropriate changes to the profile.

You can also use the **Multiple Images Profile Wizard** to modify parameters of image profiles. From the Customize/Delete Activation Profiles List window:

1. Select the profile name that requires modification, then click **Customize**. The Select one or more images window is displayed.
2. Select two or more profiles to modify, then click **OK**. The Image Wizard window is displayed.
3. Proceed through the wizard windows propagating the desired information.
4. Click **Finish** when you have completed the task and are ready to save the changes.

Activation profiles

Customize activation profiles to define the information that sets the operational capabilities and characteristics of the objects you want to activate. There are four types of activation profiles:

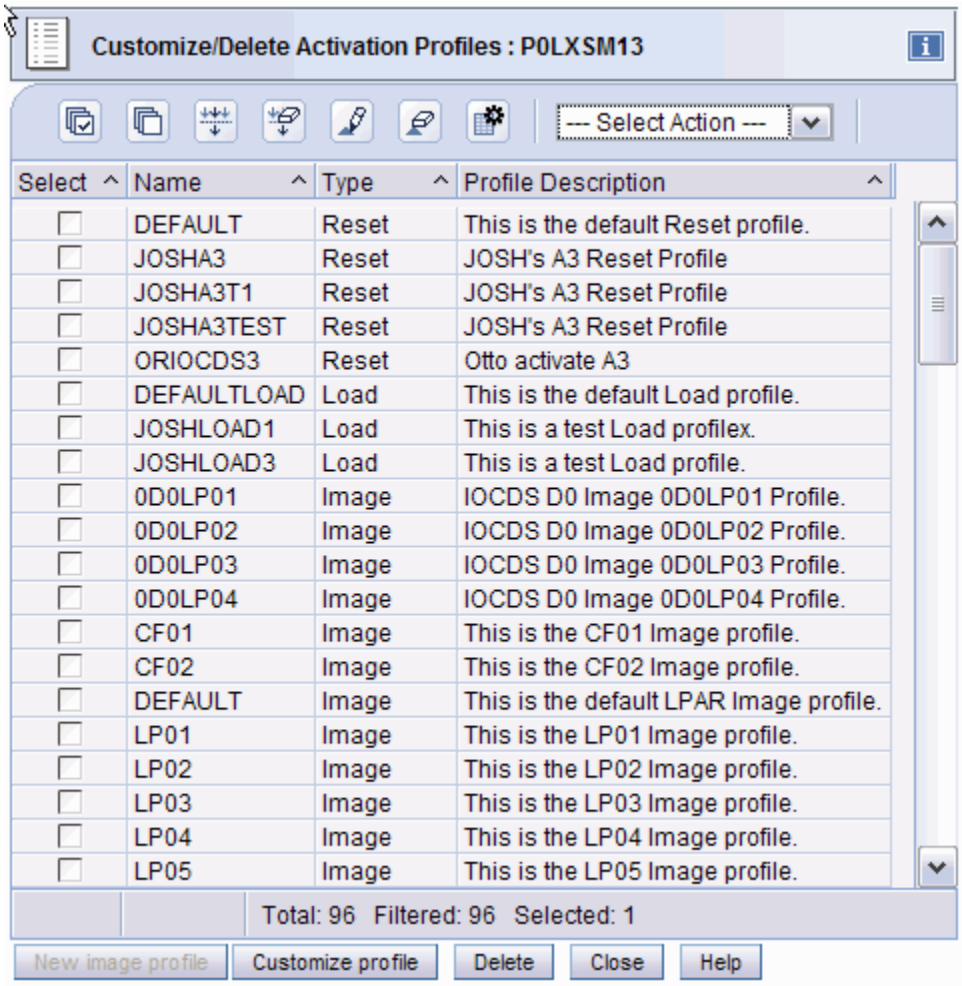


Figure 43. Activation profiles

- A *reset profile* is used to activate a central processor complex (CPC) and its images.
- An *image profile* is used to activate an image and load a control program or operating system.
- A *load profile* is used to activate an image of a CPC.
- A *group profile* is used to specify the capacity of a group of logical partitions.

A set of default activation profiles is provided by IBM with the Support Element Console Application. There is one default profile of each type:

Type	Default profile name
Reset	DEFAULT
Image	DEFAULT
Load	DEFAULTLOAD
Group	DEFAULT

The default profiles are not meant to be used to activate your central processor complex (CPC) or its images; the information in them may not be correct for your configuration or needs. Instead, customize the default profiles to meet your needs. Or customize the default profiles to meet your general needs, then use them as templates for creating new profiles that meet your specific needs.

You can perform a complete activation of a central processor complex (CPC) and its images by using a properly customized reset profile:

- When a reset profile is customized for activating the CPC, the reset profile includes the image profiles necessary to activate and load the images. That is, you can customize reset and image profiles at once for performing a complete activation of the CPC and its images:
  - Customize the reset profile for activation.
  - Customize the image profiles included in it for activating and loading one or more images during CPC activation.

You can customize load profiles and image profiles. After you use a reset profile to activate the central processor complex (CPC), you can use individual load profiles or image profiles as follows:

- You can use an image profile to activate a logical partition.

  Activating the logical partition with its image profile, rather than activating the CPC again with a reset profile, allows activating only the logical partition, while maintaining current operational capabilities and characteristics of the CPC and other logical partitions. You can activate an image this way whether you are activating it for the first time, or activating it again.
- You can use a load profile to load its image with an operating system.

  Activating the image with a load profile, rather than activating the logical partition again with an image profile, allows loading the image, while maintaining the rest of the logical partition's current operational capabilities and characteristics. You can load an image this way regardless of whether you are loading it for the first time, or loading it again but with a different operating system.

Customize unique activation profiles for each different way you want to activate the central processor complex (CPC) and its images. You can customize unique activation profiles by giving them unique names. That is, all reset profiles, load profiles, and image profiles you create must have unique names.

Recall that a reset profile includes one or more image profiles. A reset profile includes an image profile by referencing its unique profile name. While you are customizing a reset profile, you have the option of customizing the image profiles included in it. You can also customize load profiles and image profiles individually. Regardless of whether you customize them within reset profiles or individually, load profiles and image profiles remain unique.

- **Example 1:** a reset profile named LPARMODE includes image profiles named LP01 and LP02.

  While customizing the LP01 image profile individually, any changes you make also affects the LPARMODE reset profile. While customizing the LP01 image profile included in the LPARMODE reset profile, any changes you make also changes the individual LP01 image profile.

  While customizing the LP02 image profile individually any changes you make also affects the LPARMODE reset profile. While customizing the LP02 image profile included in the LPARMODE reset profile, any changes you make also changes the individual LP02 image profile.

Profiles for complete activation

A *complete activation* activates the central processor complex (CPC) and its images completely and in a single step. The result of a complete activation is an operational CPC with images loaded and running operating systems.

A properly customized reset profile includes the image profiles necessary to perform a complete activation of the CPC and its images. Using a properly customized reset profile for performing a complete activation is the recommended activation strategy for establishing the CPC's normal, day-to-day operational capabilities and characteristics.

You can perform a complete activation of a central processor complex (CPC) and its images by using a reset profile.

A complete activation means customizing a reset profile to activate the CPC, then load them with operating systems.

Staged activation

A *staged activation* activates the central processor complex (CPC) and its images in steps:

- An initial activation of the CPC and one or more images.
- And any number of subsequent, selective activations of images.

Staged activations are useful for changing the operational capabilities and characteristics of the images, but without performing a complete activation of the CPC. They allow meeting different processing needs at different times of day or on different days of the week. For example, you may want to use one logical partition as a production system during first shift, and use other logical partitions as batch and test systems on second shift.

You could perform a complete activation of the CPC each time you want to change the operational capabilities and characteristics of its images. You can get the same results by planning and performing staged activations instead. Staged activations will not require performing a complete activation of the CPC each time you want to change its operational capabilities and characteristics of its images. Instead, you can activate the CPC once, and then activate only its images when you want to change their operational capabilities and characteristics.

A reset profile is required for performing the initial activation of a staged activation. Afterwards, you can use image profiles to selectively activate logical partitions, and load profiles to selectively load images.

Information and instructions for customizing reset profiles, image profiles, and load profiles are provided in the topics that follow “Profiles for staged activations” on page 758.

Reset profiles

You can perform a complete activation of a central processor complex (CPC) and its images by using a reset profile.

A complete activation means customizing a reset profile to activate the CPC then load them with operating systems.

- See “Supporting LPAR mode operation” on page 738 , “Activating logical partitions during CPC activation” on page 744, and “Loading an operating system during activation” on page 754 along with the other topics that follow them.

Use the Support Element workplace to start the task for customizing reset profiles for a central processor complex (CPC). Starting a task is referred to also as opening a reset profile.

To open a reset profile:

1. Locate the **CPC** you want to work with.
2. Locate and open the **Customize/Delete Activation Profiles** task to start it.

   When the profile list of profiles is initially displayed, the highlighted profile is the currently assigned profile.
3. Select from the list the name of the reset profile you want to customize.
4. Click **Customize** to open the selected reset profile.

   After you start the task, use the online Help for more information about the control.

Navigating a reset profile

A reset profile includes information for activating a central processor complex (CPC) and its images.

Opening a reset profile displays its information on the windows that are organized as pages in a notebook.

The pages are identified in a profile tree view on the left side of the window with a description label. If the reset profile activates the CPC with multiple images, the profile tree view list the names of each image section with the identifying name. The information in each section is used to activate a single object either the CPC or a logical partition.

To use the profile tree view to open each page on the window:

- Click on the description label for each page within a section of the profile you want to open.
- Click on the '**+**' for each image to get a list of pages in the section of the profile.

- To save the changes made, click **Save**.
- To close the window, click **Cancel**.

Creating a new reset profile

You are responsible for creating reset profiles that meet your unique needs.

You can use the default reset profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and customize your own reset profiles, you can use them as templates for creating more new profiles.

To create a new reset profile:

1. After opening and customizing a reset profile, select the General page.

   The **Profile name** field identifies the reset profile you opened. It will be used as a template for the new reset profile.
2. To use a different reset profile as a template:
3. Select the list button beside the **Profile name** field.

   This opens a list of the names of all the CPC's reset profiles. The reset profile named DEFAULT is the default reset profile provided.
4. Select from the list the name of the reset profile you want to use as a template.

   This opens the selected reset profile. Its information replaces the previous profile's information on the pages of the window.
5. Enter a unique name for the new profile in the **Profile name** field.
6. To save the profile with the new name, click **Save**.

   Note: Saving the new profile does not change the reset profile you used as a template.

Assigning a reset profile

After you open a reset profile, you can assign it to the central processor complex (CPC) as its activation profile. Whenever the CPC is activated, it is activated according to the information in its assigned activation profile.

To assign an open reset profile as a CPC's activation profile:

1. After opening and customizing a reset profile, select the General page.

   The **Profile name** field identifies the reset profile that will be assigned to the CPC.
2. To assign the reset profile as the CPC's activation profile, click **Assign profile**.

Supporting LPAR mode operation

The reset profile you use to activate a central processor complex (CPC) can establish the support required to operate the CPC. The reset profile must identify:

- An input/output configuration data set (IOCDS) that supports LPAR mode and the logical partitions you want to activate.
- LPAR mode as the operating mode you want to establish.

An IOCDS is used during a power-on reset to define your input/output (I/O) configuration to the channel subsystem of the CPC. The I/O configuration is the set of all I/O devices, control units, and channel paths available to the CPC. Performing a power-on reset also establishes the operating mode of the CPC.

To customize a reset profile to support operating the CPC:

1. Select the General page.
2. Select from the **Input/Output Configuration Data Set** list an IOCDS that defines the logical partitions you want to activate.

   Notes:

a. The **Type** column indicates the operating mode supported by each IOCDS. The column displays **Partition** to indicate an IOCDS supports LPAR mode.

b. The **Partitions** column displays the names of logical partitions supported by the IOCDS.

3. Select **Logically partitioned** from the **Mode** list as the operating mode you want to establish.

Selecting an IOCDS

The reset profile you use to activate a central processor complex (CPC) can identify the input/output configuration data set (IOCDS) you want to use. The IOCDS must be compatible with the operating mode you want to establish. That is, the IOCDS you select must support the type of operating mode you select.

An IOCDS is used during a power-on reset to define your input/output (I/O) configuration to the channel subsystem of the CPC. The I/O configuration is the set of all I/O devices, control units, and channel paths available to the CPC. Performing a power-on reset also establishes the operating mode of the CPC.

You can use the Image Profile Configuration window to:

- Set up initial parameters when you selected an IOCDS that contains two or more images that were defined in the IOCDS, but currently do not exist in the list of image profiles.
- Create one or more image using the New Image Profile Wizard when you selected an IOCDS that does not contain corresponding image profiles.

The Image Profile Configuration window allows you to automatically assign unique logical partition identifiers to each new image profile and enter a profile description to the new image profiles. You can select an existing image profile and have the existing profile's data copied to all new image profiles that are to be created.

You can customize the reset profile to use either a specific IOCDS or the active IOCDS (if you intend to use dynamic I/O configuration, for example). Follow the instructions below for using a specific IOCDS; see “Using the active IOCDS” on page 739 for more information about using the active IOCDS.

To customize a reset profile to select an IOCDS and operating mode:

1. Select the General page.
2. Select an IOCDS from the **Input/Output Configuration Data Set** list.
3. Select an operating mode from the **Mode** list that is compatible with the IOCDS you selected.

   Note the type of operating mode supported by the IOCDS you selected. The **Type** list column indicates the operating mode supported by each IOCDS:

IOCDS type	Operating mode
Partition	Logically partitioned
Currently *ID*I	The operating mode of the IOCDS is not known because the reset profile will use the active IOCDS when activation is performed; the *ID* identifies the current active IOCDS. Select an operating mode from the **Mode** list that is compatible with the IOCDS you *intend* to make active. For more information, see "Using the active IOCDS".

Using the active IOCDS

The reset profile you use to activate a central processor complex (CPC) can be customized for using the active IOCDS rather than a specific IOCDS. The *active IOCDS* is the IOCDS used for the most recent power-on reset. If you use dynamic I/O configuration, you can change the active IOCDS at any time without performing a power-on reset.

You should customize a reset profile to use the active IOCDS if you intend to use dynamic input/output (I/O) configuration. At least one of the images activated on the CPC must be loaded with an operating system that supports an application or facility for using dynamic I/O configuration. Dynamic I/O configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some z/OS and OS/390 operating systems.

- The dynamic I/O configuration facility of some z/VM and VM operating systems.

To customize an activation profile to use the active IOCDS:

1. Select the General page.
2. Select **Use active IOCDS** from the **Input/Output Configuration Data Set** list.

   When activation is performed using this reset profile:

   - The last active IOCDS is used if the CPC is not operational.
   - The active IOCDS is used if the CPC is already operational *and* if a power-on reset must be performed to make at least one other profile setting take effect. For more information, see "How using the active IOCDS affects CPC activation" on page 740.
3. Note the identifier of the IOCDS that is currently active. See **Currently ID** displayed in the **Type** list column for the **Use active IOCDS** selection. The **ID** is the IOCDS identifier.

   With dynamic I/O configuration, you can change the active IOCDS anytime prior to using this reset profile to activate the CPC.
4. Select an operating mode from the **Mode** list that is compatible with the IOCDS you've made active or *intend* to make active.

   To determine the type of operating mode supported by the IOCDS, locate it in the **Input/Output Configuration Data Set** list. The **Type** list column indicates the operating mode supported by the IOCDS.

How using the active IOCDS affects CPC activation

When a reset profile is used to activate the central processor complex (CPC), several profile settings take effect when a power-on reset is performed during activation. Such settings are referred to here as *power-on reset settings* and include, for example, the CPC's storage allocations. If the CPC is already operational and the reset profile's power-on reset settings are already in effect when activation is performed using the profile, then a power-on reset is not performed during activation. That is, a power-on reset is performed during CPC activation only if it is necessary to make one or more of the reset profile's power-on reset settings take effect.

The input/output configuration data set (IOCDS) setting is one of the reset profile's power-on reset settings, *unless* it is set to **Use active IOCDS**. Activating the CPC with a reset profile customized for using the active IOCDS affects CPC activation as follows:

- If the CPC is not operational, then a power-on reset is performed and the last active IOCDS is used.
- If the CPC is already operational, then:
  - A power-on reset is performed and the active IOCDS is used only if one or more of the reset profile's other power-on reset settings are not already in effect. For example, a power-on reset is performed if the CPC's global input/output (I/O) priority queuing flag is not the same as the global I/O priority queuing flag set in the reset profile.
  - A power-on reset is *not* performed and the active IOCDS is ignored if all of the reset profile's other power-on reset settings are already in effect.

    This may be the case when you use dynamic input/output (I/O) configuration. Using dynamic I/O to change the active IOCDS will not affect whether a power-on reset is performed during CPC activation. Only changing the reset profile's other power-on reset settings will cause a power-on reset to be performed.

Delaying the load while devices power-on

The reset profile you use to activate a central processor complex (CPC) can set a load delay for power sequencing.

Activating a CPC includes initializing its images and can include loading the images. The operating systems are loaded from devices in the input/output (I/O) configuration of the CPC.

If the devices are attached to control units that are powered-on by the CPC during activation, operating systems cannot be loaded from the devices until powering-on their control units is complete.

If you know or can estimate the amount of time it takes for control units to be powered-on, you can delay starting the load for that amount of time, up to 100 minutes. The delay may allow the powering-on to complete before the load begins.

To customize a reset profile to delay the load while control units power-on:

1. Select the General page.
2. Enter the amount of time to delay the load, from 0 to 59 seconds or 1 to 100 minutes, in the **Load delay for power sequencing** fields.

Supporting dynamic I/O configuration

The reset profile you use to activate a central processor complex (CPC) can establish the hardware support required to use dynamic input/output (I/O) configuration.

Your I/O configuration is the set of all I/O devices, control units, and channel paths you define to your hardware and software.

Performing a power-on reset establishes the *hardware I/O definition*. That is, it defines the I/O configuration to the hardware. Loading the software establishes the *software I/O definition*. That is, it defines the I/O configuration to the software.

Changing the hardware I/O definition requires performing another power-on reset, and changing the software I/O definition requires loading the software again. If the hardware and software support *dynamic I/O configuration*, you can *dynamically change* their I/O definitions. Changes made dynamically, referred to as *dynamic I/O changes*, take effect immediately. Yet they do *not* require a power-on reset or load to make them take effect.

Hardware support for dynamic I/O

Your hardware is the CPC. Dynamic I/O configuration, or simply *dynamic I/O*, is a facility of the CPC's licensed internal code. The hardware support required for using dynamic I/O can be established during power-on reset of the CPC:

- The IOCDS used during power-on reset must support dynamic I/O. The IOCDS must be either:
  - Built using the Hardware Configuration Definition (HCD) application of an z/OS and OS/390 or other operating system that supports dynamic I/O.
  - Written using the DYN option of the input/output configuration program (IOCP) utility of a z/VM and VM operating system that supports dynamic I/O.
- Dynamic I/O must be enabled for the CPC. That is, the CPC must allow dynamically changing its I/O definition.

  Note: Only a power-on reset of the CPC, performed directly or during CPC activation, can initially enable dynamic I/O. After, you can use the support element workplace at any time, if necessary, to change the dynamic I/O setting. For more information, see “Enabling or disabling dynamic I/O without performing a power-on reset” on page 742.
- Dynamic I/O must be enabled for a logical partition.

To customize a reset profile for hardware support of dynamic I/O:

1. Select the General page.
2. Select an IOCDS that supports dynamic I/O from the **Input/Output Configuration Data Set** list.

   Note: The **Allow Dynamic I/O** column displays **Yes** to indicate an IOCDS supports dynamic I/O.
3. Select the Dynamic page.
4. Mark the **Allow dynamic changes to the channel subsystem input/output (I/O) definition** check box.

The check box displays a check mark when you mark it. The check mark indicates you want to enable dynamic I/O for the CPC.

Enabling or disabling dynamic I/O without performing a power-on reset

Performing a power-on reset of the central processor complex (CPC), either directly or by activating the CPC, establishes many of its initial operational capabilities and characteristics, including whether dynamic input/output (I/O) configuration is enabled or disabled. After a power-on reset of the CPC is performed, changing its operational capabilities and characteristics requires performing another power-on reset.

If a power-on reset of the CPC initially enables dynamic I/O configuration, a task becomes available on the support element workplace for changing the CPC's dynamic I/O setting without performing another power-on reset.

To change the CPC's dynamic I/O setting without performing a power-on reset:

1. Locate the **CPC** to work with.
2. Locate and open the **Enable/Disable Dynamic Channel Subsystem** task to start it.

   The Customize Dynamic Channel Subsystem window displays.
3. Use the window's controls, as follows, to enable or disable dynamic I/O for the CPC:
   a. Review the CPC's current setting for dynamic I/O. The selected **Enabled** or **Disabled**, indicates the current setting.
   b. While dynamic I/O is enabled, select **Disabled** to change the setting to disabled.
   c. Or while dynamic I/O is disabled, select **Enabled** to change the setting to enabled.
   d. Click **OK** to save the setting and close the window.

Selecting CP/SAP to Optimize the performance of an application

Note: Available on the Hardware Management Console Version 2.13.1 and earlier)

You can optimize the performance of an application by selecting a CP/SAP configuration for the central processor complex (CPC) that best suits the instruction processing requirements.

The physical processor units installed in the CPC are used either as central processors (CPs) or system assist processors (SAPs). The model of your machine determines its default configuration of CPs and SAPs. The SAPs, if any, are used exclusively for input/output (I/O) instruction processing.

If other CP/SAP configurations are available, selecting a configuration that configures one or more CPs as additional SAPs may improve the performance of some types of applications (applications that have greater needs for I/O instruction processing, for example). Selecting a non-default CP/SAP configuration may affect how the CPC can be activated.

Effects of changing the CP/SAP configuration

If you intend to activate a CPC, a reduction in the number of available CPs will reduce the number of logical processors you can assign to logical partitions. Activation of a logical partition will fail if the number of logical processors you attempt to assign exceeds the number of CPs available.

To avoid a logical partition activation failure, verify the number of logical processors assigned to a logical partition by its activation profile does not exceed the number of CPs available. For more information about customizing an activation profile to assign logical processors to a logical partition, see “Assigning initial logical or reserved processors” on page 746.

Planning for a fenced book

The reset profile you use to activate a central processor complex (CPC) can determine how the available system processors would be assigned when a hardware problem occurs with one of the system books that cause the book to be fenced or become unavailable for use.

Note: To display this Fenced page, select **Display fenced book page** on the CP/SAP page (2.13.1 and earlier) or Options page (Version 2.14.0) .

To customize a reset profile to let the system determine the processor assignment:

1. Select the Fenced page.
2. Locate the Processor Assignment group box.
3. Select the **Determined by the system** radio button.

To customize a reset profile to set a processor assignment by the user:

1. Select the Fenced page.
2. Select the **Determined by user** radio button.
3. Locate the Processor Assignment group box.
4. Select the processor assignment radio button when a processor book is fenced.
5. Type the values in the **Value Used when Book is Fenced** field.

Enabling or disabling the global input/output I/O) priority queuing

The reset profile you use to activate a CPC can enable or disable the global input/output (I/O) priority queuing.

To customize a reset profile for enabling or disabling global input/output (I/O) priority queuing:

1. Select the Options page.
2. Locate the **Enable global input/output (I/O) priority queuing** check box. Then either:
   - Mark the check box to enable global input/output priority queuing. The check box displays a check mark when you mark it.
   - Or unmark the check box to disable global input/output priority queuing. The check box becomes empty when you unmark it.

Releasing I/O reserves under error conditions

The reset profile you use to activate a central processor complex (CPC) can enable automatically resetting the input/output (I/O) interface under particular error conditions.

In a multiple CPC environment, several objects, which can be CPCs or logical partitions, may share the control units, channel paths, and I/O devices included in their I/O definitions.

The following error conditions may cause shared control units to hold reserves on their devices:

- A machine check places the CPC in a check-stopped state.
- Or the control program places an image of the CPC or a logical partition in a non-restartable wait state.

The reserves are held for the CPC or logical partition affected by the error condition. Holding reserves provides the affected object with exclusive use of devices, preventing them from being used by other objects that share the control units.

To release reserves held by shared control units assigned to an object, you must reset the I/O interface. Although resetting the I/O interface will not recover the object from its error condition, it will make the devices attached to shared control units available to other objects.

To customize a reset profile to enable automatically resetting the I/O interface:

1. Select the Options page.
2. Mark the **Automatic input/output (I/O) interface reset** check box.

   The check box displays a check mark when you mark it. The check mark indicates you want to enable resetting the I/O interface automatically.

Setting processor running time

The reset profile you use to activate a central processor complex (CPC) can set whether you or the CPC determines the processor running time.

When the CPC is activated, the logical processors of logical partitions activated without dedicated processor resources share the remaining processor resources.

Each logical processor is given the same processor running time. *Processor running time* is the amount of continuous time allowed for a logical processor to perform jobs using shared processor resources. Processor running time is referred to also as a *timeslice*.

The processor running time can be dynamically determined by the CPC. That is, the CPC can automatically recalculate the running time whenever the number of active logical processors changes.

You can set the running time to a constant amount. To get optimal use of shared processor resources, IBM recommends letting the CPC dynamically determine the running time.

To customize a reset profile to let the CPC dynamically determine processor running time:

1. Select the Options page.
2. Locate the Processor running time group box.
3. Select **Dynamically determined by the system**.

To customize a reset profile to set a constant processor running time:

1. Select the Options page.
2. Locate the Processor running time group box.
3. Select **Determined by the user**.
4. Type the constant running time, from 1 to 100 milliseconds, in the **Running time** input field.

Note: After activating the CPC, you can use the Support Element workplace to dynamically change its settings for processor running time. See the **Change LPAR Controls** task for more information.

Setting power saving

The reset profile you use to activate a central processor complex (CPC) can set the energy management power saving option to reduce the average energy consumption of the system.

To customize a reset profile to set the power saving option:

1. Select the Options page.
2. Locate the Set Power Saving group box.
3. Select the **Custom Energy Management** radio button to use the power saving settings.
4. Select the **Emergency High Performance** radio button to override the power saving settings and use the high performance setting with no power saving.

Activating logical partitions during CPC activation

The reset profile you use to activate a central processor complex (CPC) can also activate one or more logical partitions.

To customize a reset profile to activate logical partitions during CPC activation:

1. If you have not already done so, customize the reset profile to activate the CPC. For more information, see “Supporting LPAR mode operation” on page 738.
2. Select the Partitions page.
3. Review the logical partition name in each **Partition** field.

   The fields are initialized with the names of logical partitions defined in the input/output configuration data set (IOCDS) selected on the General page of the reset profile.
4. Review the numbers in the **Order** fields beside the logical partition names.

The fields are initialized with the default activation order of the logical partitions. The logical partition with an order of 1 will be activated first, the logical partition with an order of 2 will be activated second, and so on.

5. Optionally, enter a new order number in the **Order** field of a logical partition to change its activation order.

   Note: If you intend to operate one of the logical partitions in coupling facility mode, it should be activated first. That is, you should change the activation order of a coupling facility logical partition to 1.

6. Optionally, delete the order number of a logical partition to *not* activate it during activation of the CPC.

   Note: The names of logical partitions that are not activated will not be saved in the profile. That is, if you delete the order number of a logical partition, its name will be discarded.

The information used to activate a logical partition, though it is included in a reset profile, is actually the logical partition's image profile.

The name of an image profile is the same as the name of the logical partition it activates. So each logical partition has only one image profile.

Since each reset profile that activates a logical partition includes the logical partition's only image profile, changing the logical partition's information in any activation profile changes the same information in all the other profiles as well. That is, if you customize a reset profile for activating a logical partition, for example, changing the reset profile *also* changes the logical partition's information in its image profile *and* in every other reset profile that activates the same logical partition.

Assigning a logical partition identifier

The activation profile you use to activate a logical partition must assign it a unique logical partition identifier.

The logical partition identifier becomes part of the central processor identifier of each logical processor assigned to the logical partition. The central processor identifier is used by subsystems and control programs to distinguish between logical processors.

To customize an activation profile to assign a logical partition identifier:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the General page.
3. In the **Partition identifier** field, type the hexadecimal digit to assign as the logical partition identifier.

   Notes:

   a. The partition identifier must be unique among the identifiers of other logical partitions activated at the same time. If necessary, verify the partition identifier assigned to this image is unique by checking the **Partition identifier** fields on the General pages of the other logical partitions you intend to activate.

Selecting an operating mode

The activation profile you use to activate a logical partition must identify the operating mode you want to establish.

The operating mode describes the architecture that supports the operating system or control program you intend to load. *Coupling facility* and *Linux Only* are examples of operating modes.

To customize an activation profile to select an operating mode:

1. If you opened a reset profile, select the name of the logical partition from the profile tree from the left side of the window.
2. Select the General page.
3. Select the operating mode you want to establish from the **Mode** list.

Assigning a processor type to the logical partition

Depending on the processor installed in the CPC, you can assign a processor type to a logical partition:

- Internal Coupling Facility (ICF) processors
- Integrated Facilities for Linux (IFL) processors
- zEnterprise Application Assist Processors (zAAPs)

  Note: Available on the Hardware Management console Version 2.12.1.
- Integrated Information Processors (zIIPs)

To customize an activation profile to assign logical processors to a processor type:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the General page.
3. Select the operating mode you want to establish from the **Mode** list, select the Processor page.
4. Use the Logical Processor Assignments group box to select the type of processors you want assigned to the logical partition
5. Use the controls available to complete the logical partition assignment for the logical partition processor type.

Setting Workload Manager (WLM) controls

The activation profile you use to activate a logical partition can manage your defined capacity for a logical partition. See "Setting defined capacity" on page 752 to set defined capacity for logical partitions. Workload Manager allows you to run all of your work concurrently while allocating system resources to the most work first. Workload Manager constantly monitors your system, automatically adjusting the resource allocation as necessary.

To customize an activation profile to allow Workload Manager to manage logical partitions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the General page.
3. Select **General**, **LINUX Only**, or **z/VM** from the **Mode** list.
4. Select the Processor page.
5. Unmark the **Initial Capping** box. If there are more than one processor types selected in the processor table, you may need to return to the Not Dedicated Processor Details for each processor type and unmark the Initial Capping box.

   Note: You cannot mark the **Initial Capping** box if the **Enable Workload Manager** is enabled. You must unmark it to allow Initial Capping to be marked.
6. Mark the **Enable Workload Manager** check box to enable Workload Manager.

   A check box displays a check mark when you mark it.
7. Enter the processing weight values for the logical partition that you want to be managed by Workload Manager.

Assigning initial logical or reserved processors

The activation profile you use to activate a logical partition can assign it initial logical or reserved processors.

An initial logical processor is the processor resource defined to operate in a logical partition as a physical central processor. Initial logical processors are the processors a control program uses to perform jobs for the logical partition.

Reserved processors can be defined at partition activation time, but not used during partition activation. The reserved processor is not available when the system is activated, but can become available during concurrent central processor (CP) upgrade.

To customize an activation profile to assign initial logical processors to a logical partition:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the Processor page.
3. Enter the number of initial logical processors to assign to the logical partition or the number of reserved processors.

   Note: You cannot specify initial zEnterprise Application Assist Processors (zAAPs) prior to installation of zAAPs. (Hardware Management Console Version 2.12.1)
4. Use the controls in the Logical processor assignment group box to allocate processor resources to logical partitions.

   Note: After activating logical partitions, you can use the Support Element workplace to dynamically change its settings for sharing processor resources. See the **Change LPAR Controls** task for more information.

Time offset

The Logical partition system time offset provides for the optional specification of a fixed time offset (specified in days, hours, and quarter hours) for each logical partition activation profile. The offset, if specified, will be applied to the time that a logical partition will receive from a Server Time Protocol (STP). This support can be used to address the following customer environment:

- Different local time zone support in multiple sysplexes using the STP Coordinated Timing Network (CTN).Many sysplexes have the requirement to run with a LOCAL=GMT setting in a sysplex (ETRMODE=YES or STPMODE=YES) where the time returned from a store clock (STCK) instruction yields local time. To fulfill this requirement, the time initialized for the STP CTN must be local time. With Logical partition time offset support, multiple sysplexes can each have their own local time reported to them from a STCK instruction if wanted. For instance, the STP CTN can be set to GMT, one set of sysplex partitions could specify a Logical partition offset minus 5 hours, and a second set of sysplex partitions could specify a Logical partition time offset of minus 6 hours.

To customize the image profile for the system time offset:

1. Open an activation profile customized for activating a CPC.
2. Select **Logical partition system time offset** in the Clock type assignment box
3. Select the Time Offset from the window tree view to set the offset and to choose how you want it applied when the logical partition's clock is set.
4. Click **Save**.
5. Activate the CPC.

Ensuring image profile data conforms to current maximum LICCC configuration

The data entered in the image profiles has to be compatible and supported by the Licensed Internal Code Configuration Control (LICCC). If image profile data changes, is imported, or the LICCC definition changes the profiles will be modified automatically to meet the new LICCC configuration. If this option is unchecked, the data entered for an image profile can be outside the valid LICCC configuration.

Note: It is recommended that image profile data conform to the current maximum LICCC configuration.

To customize the image profile to ensure the image profile data conforms to the current maximum LICCC configuration:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the General page.

3. Check **Ensure that the image profile data conforms to the current maximum LICCC configuration** to ensure that the image profile data conforms to the current maximum LICCC configuration.

Controlling access to performance data

The activation profile you use to activate a logical partition can control whether it has global access to performance data.

A logical partition has access to only its own performance data. A logical partition with global access also has access to the performance data of all other logical partitions activated on the same central processor complex (CPC). Performance data includes central processor usage and input/output processor usage by each logical partition.

To customize an activation profile to control global access to performance data:

1. If you opened a reset profile, select the page tab that displays the name of the logical partition.
2. Select the Security page.
3. Locate the **Global performance data control** check box. Then either:
   - Mark the check box to give the logical partition global access to performance data. The check box displays a check mark when you mark it.
   - Or unmark the check box to give the logical partition access to only its own performance data. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the Support Element workplace to dynamically change their security settings, including global performance data control. See the **Change LPAR Security** task for more information.

Controlling I/O configuration changes

The activation profile you use to activate a logical partition can control whether it can change the input/output (I/O) configuration of the central processor complex (CPC) on which it is activated.

Allowing a logical partition to change the I/O configuration enables:

- Reading and writing any input/output configuration data set (IOCDS) of the local CPC.
- Writing an IOCDS to a remote CPC.
- Using dynamic I/O configuration.
- Using the OSA Support Facility to view OSA configuration for other logical partitions.

To customize an activation profile to control changing the I/O configuration:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Input/output (I/O) configuration control** check box. Then either:
   - Mark the check box to allow using the logical partition to change the I/O configuration. The check box displays a check mark when you mark it.
   - Or unmark the check box to prevent using the logical partition to change the I/O configuration. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the Support Element workplace to dynamically change their security settings, including I/O configuration control. See the **Change LPAR Security** task for more information.

Using dynamic I/O configuration

Dynamic input/output (I/O) configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some z/OS and OS/390 operating systems.
- The dynamic I/O configuration facility of some z/VM and VM operating systems.

Input/output configuration control must be enabled for the logical partition that you want to use dynamic I/O configuration. That is, you must mark the **Input/output (I/O) configuration control** check box on the Security page of the activation profile used to activate the logical partition.

Authorizing control of other logical partitions

The activation profile you use to activate a logical partition can control whether it can be used to issue a subset of control program instructions to other logical partitions activated on the same central processor complex (CPC).

Allowing a logical partition to issue instructions to other logical partitions enables:

- Using it to reset or deactivate another logical partition.
- Using the automatic reconfiguration facility (ARF) to backup another logical partition.

To customize an activation profile to authorize control of other logical partitions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Cross partition authority** check box. Then either:
   - Mark the check box to allow using the logical partition to control other logical partitions. The check box displays a check mark when you mark it.
   - Or unmark the check box to prevent using the logical partition to control other logical partitions. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the Support Element workplace to dynamically change their security settings, including cross partition authority. See the **Change LPAR Security** task for more information.

Controlling use of reconfigurable channel paths

The activation profile you use to activate a logical partition can control whether it has exclusive use of its reconfigurable channel paths.

A logical partition has exclusive use of its reconfigurable channel paths only while they are configured on. If the channel paths are configured off, they can be configured on to another logical partition.

Isolating a logical partition's reconfigurable channel paths reserves them for the logical partition while they are configured off, and prevents them from being configured on to other logical partitions.

To customize an activation profile to control the use of reconfigurable channel paths:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Logical partition isolation** check box. Then either:
   - Mark the check box to isolate the logical partition's offline reconfigurable channels paths. The check box displays a check mark when you mark it.
   - Or unmark the check box to make the logical partition's reconfigurable channels paths available to other logical partitions when the channel paths are configured off. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the support element workplace to dynamically change their security settings, including logical partition isolation. See the **Change LPAR Security** task for more information.

Authorizing basic counter set control

The basic counter set authorization control allows authorization to use the basic counter set in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

To customize an activation profile to indicate whether authorization is allowed to use the basic counter set:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Basic counter set authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the basic counter set authorization control in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.
   - Or unmark the check box not to allow authorization to use the basic counter set authorization control.

Authorizing problem state counter set control

The problem state counter set authorization control allows authorization to use the problem state counter set in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

To customize an activation profile to indicate whether authorization for problem state counter set is allowed:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Problem state counter set authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the problem state counter set authorization control in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.
   - Or unmark the check box not to allow authorization to use the problem state counter set authorization control

Authorizing crypto activity counter set control

The crypto activity counter set authorization control allows authorization to use the crypto activity counter set to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

To customize an activation profile to indicate whether authorization for crypto activity counter set authorization control:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Crypto activity counter set authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the crypto activity counter set authorization control to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.
   - Or unmark the check box not to allow authorization to use the crypto activity counter set authorization control.

Authorizing extended counter set control

The extended counter sets authorization control allows authorization of the model-dependent extended counter set.

To customize an activation profile to indicate whether authorization for extended counter set authorization control:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Extended counter set authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the extended counter set authorization control. The counters of this set are model dependent.
   - Or unmark the check box not to allow authorization to use the extended counter set authorization control.

Authorizing basic sampling control

The basic sampling authorization control allows authorization to use the basic sampling function. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

To customize an activation profile to indicate whether authorization for basic sampling authorization control:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Basic sampling authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the basic sampling authorization control function.
   - Or unmark the check box not to allow authorization to use the basic sampling authorization control.

Diagnostic sampling authorization control

The diagnostic sampling authorization control allows authorization to use the diagnostic sampling function. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

To customize an activation profile to indicate whether authorization for diagnostic sampling authorization control:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Diagnostic sampling authorization control** check box. Then either:
   - Select the check box to indicate whether authorization is allowed to use the diagnostic sampling authorization control function.
   - Or, unselect the check box not to allow authorization to use the diagnostic sampling authorization control.

Permit AES key import functions

The permit Advanced Encryption Standard (AES) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

To customize an activation profile to permit AES key import functions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.

3. Locate the **Permit AES key import functions** check box. Then either:
   - Mark the check box to permit AES key import functions.
   - Or unmark the check box not to permit AES key import functions.

Permit DEA key import functions

The permit Data Encryption Algorithm (DEA) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

To customize an activation profile to permit DEA key import functions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Permit DEA key import functions** check box. Then either:
   - Mark the check box to permit DEA key import functions.
   - Or unmark the check box not to permit DEA key import functions.

Allocating central storage (main storage)

The activation profile you use to activate a logical partition can allocate its storage.

The central storage allocated to a logical partition upon activation is its *initial storage*. You must allocate initial central storage to each logical partition you intend to activate.

To customize an activation profile for allocating central storage to a logical partition:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Storage page.
3. Use the Central storage group box to allocate the logical partition's central storage and to set its central storage origin.

Setting I/O priority queuing values

The activation profile you use to activate a logical partition can control the I/O priority queuing assignment of logical partitions.

To customize an activation profile for I/O priority queuing:

1. If you opened a reset profile, select the page tab that displays the name of the logical partition.
2. Select the Options page.
3. Use the controls to set minimum and maximum I/O priority queuing values.

Setting defined capacity

The activation profile you use to activate a logical partition can control the defined capacity for a logical partition. A defined capacity is the portion of your processor resources you order.

Your defined capacity can be associated with:

- A license software product. You specify a defined capacity for a product on the product certificate.
- An LPAR. You specify a defined capacity for an LPAR using the appropriate LPAR controls. A defined capacity applies to the entire LPAR, no matter how many applications it contains.

To customize an activation profile to set defined capacity:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Options page.

3. Enter the defined capacity value for your logical partition.

Assigning zAware configuration settings

Note: Available on the Hardware Management Console Version 2.13.0.

The activation profile you use to activate a logical partition can assign zAware configuration settings of the logical partition. The zAware configuration settings are:

Host name
A host name can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a host name are numbers **0** through **9**, alphabetic, periods, colons, and minus symbols.

Master userid
Use this field to specify the master user ID for the selected firmware logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a master user ID name is numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Use this field to specify the master password for the master user ID you specified. A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Use this field to specify again the same master password you specified in the **Master password** field.

Default gateway
Use this field to specify the default gateway IPv4 or IPv6 address.

To customize an activation profile to set the zAware configurations:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. If you select zAware from the **Mode** list, select the zAware page.
3. Enter the host name, master user ID, master password, and default gateway zAware configuration settings:

Assigning Secure Service Container configuration settings

The activation profile you use to activate a logical partition can assign configuration settings of the logical partition in Secure Service Container mode. The Secure Service Container configuration settings are:

Boot selection
Before a Secure Service Container partition is restarted for the first time, all fields of activation profiles can be updated or saved.

Secure Service Container installer
This option is selected until the Secure Service Container partition is restarted and the input fields contain information that were previously defined.

Secure Service Container
This option is selected after the Secure Service Container partition is restarted. The **Reset Logon Settings** and **Reset Network Settings** can be updated after the restart.

Host name
A host name can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a host name are numbers **0** through **9**, alphabetic, periods, colons, and minus symbols.

Master userid
Use this field to specify the master user ID for the selected firmware logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a master user ID name is numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Use this field to specify the master password for the master user ID you specified. A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Use this field to specify again the same master password you specified in the **Master password** field.

IPv4 gateway
Use this field to specify the default gateway IPv4 address.

IPv6 gateway
Use this field to specify the default gateway IPv6 address.

To customize an activation profile to set the Secure Service Container configurations:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. If you select SSC from the **Mode** list, select the SSC page.
3. Enter the host name, master user ID, master password, and default gateway Secure Service Container configuration settings:

Loading an operating system during activation

The activation profile you use to activate an object can also load its image with an operating system. The object is a central processor complex (CPC) activated in a logical partition.

To customize an activation profile to load an operating system during an object's activation:

1. Open an applicable activation profile:
   - If the object is a logical partition, either open a reset profile or open its image profile.

     For more information, see “Reset profiles” on page 737 or “Images profiles” on page 759.

     Note: The activation profile must *not* be customized to activate the logical partition as a coupling facility. For more information, see “Selecting an operating mode” on page 745.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Load page.
4. Mark the **Load during activation** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will include loading the object's image with an operating system.
5. Use the other controls on the page to provide information about which operating system to load and how to load it.

Selecting a load type

The activation profile you use to load an image can set the load type to perform the load.

To customize an activation profile to set the load address and load parameter:

1. Open an activation profile:
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
4. Locate the **Load type** controls to select the following load types:
   - Select **Standard load** to perform a normal load from a z-architected device (such as internal z DASD).
   - Select **SCSI load** to perform a SCSI load (from certain types of channels).

- Select **SCSI dump** to perform a SCSI dump (to do a standalone dump from a SCSI IPL type of device).
- Select **NVMe load** to perform a NVMe load (from certain types of adapters).
- Select **NVMe dump** to perform a NVMe dump (to do a standalone dump from a NVMe IPL type of adapter).

Using dynamic I/O to set load attributes

The activation profile you use to load an image can enable using dynamic input/output (I/O) configuration, rather than the activation profile, to set the load address and load parameter used to perform the load.

The image must be activated on a CPC that supports dynamic I/O configuration. The image, or at least one of the images activated on the CPC, must be loaded with an operating system that supports an application or facility for using dynamic I/O configuration. Dynamic I/O configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some z/OS and OS/390 operating systems.
- The dynamic I/O configuration facility of some z/VM and VM operating systems.

To customize an activation profile to enable using dynamic I/O to set the load address and load parameter:

1. If you opened a reset profile and the object is a logical partition, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
3. Mark the **Use dynamically changed address** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform each load using the load address set for the image using dynamic I/O configuration.
4. Mark the **Use dynamically changed parameter** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform each load using the load parameter set for the image using dynamic I/O configuration.

Setting a time limit for performing the load

The activation profile you use to load an image sets a time limit for performing the load.

A time limit, or *time-out value*, is the amount of time allowed for performing the load. The load is canceled if it cannot be completed within the time limit.

To customize an activation profile to set the time limit for performing the load:

1. Open an activation profile:
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
4. Enter the time limit, from 60 to 600 seconds, in the **Time-out value** field.

Setting load attributes

The activation profile you use to load an image can set the NVMe or SCSI parameters used to perform the load.

The *load address* is the address of the input/output (I/O) device that provides access to the operating system you want to load. The I/O device must be in the I/O configuration that is active when the load is performed. The I/O device may store the operating system or may be used to read the operating system from a storage device.

The *load parameter* is additional information operating systems support to provide you with additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the operating system to determine the load parameters that are available, and their effect on a load.

The *Worldwide port name* is the number identifying the Fibre Channel port of the SCSI target device. This field contains the 64-bit binary number designating the port name, represented by 16 hexadecimal digits.

Note: If the selected load type is **Standard load**, **NVMe load** or **NVMe dump**, this field is unavailable.

The *Logical unit number* is the number of the logical unit as defined by FCP. This field contains the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for a SCSI load or SCSI dump.

Note: If the selected load type is **Standard load**, **NVMe load**, or **NVMe dump** this field is unavailable.

The *Boot program selector* is a decimal value number specifying the program to be loaded from the FCP-load device during a SCSI load, SCSI dump, NVMe load, or NVMe dump. Valid values range from 0 to 30.

The *Boot record logical block address* is the load block address field represented by 16 hexadecimal characters, designating the logical-block address of a boot record on the FCP-load device. If no block address is specified, the logical-block address of the boot record is assumed to be zero.

The *OS specific load parameters* is a variable number of characters to be used by the program that is loaded during a SCSI load, SCSI dump, NVMe load, or NVMe dump. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system has to support this.

To customize an activation profile to set the NVMe or SCSI parameters:

1. Open an activation profile:
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
4. Enter the worldwide port name in the **Worldwide port name** field.

   Note: For SCSI load or SCSI dump only.
5. Enter the logical unit name in the **Logical unit number** field.

   Note: For SCSI load or SCSI dump only.
6. Enter the boot program number in the **Boot program selector** field.
7. Enter the boot record logical block address in the **Boot record logical block address** field.
8. Enter the OS specific load number in the **OS specific load parameters** field.

Using the Crypto Express feature

The activation profile you use to activate a logical partition can prepare it for running software products that utilize the Crypto Express feature. Using the feature's cryptographic facilities and functions requires customizing the logical partition's activation profile to:

- Give it access to at least one Crypto Express feature. This is accomplished by selecting from the Usage Domain Index and the Cryptographic Candidate list.
- Load it with an operating system, such as z/OS, that supports using cryptographic functions.
- Install the CP Assist for Cryptographic Facility (CPACF) DES/TDES Enablement feature if planning to use ICSF.

For more information about the cryptographic feature, see the **Cryptographic Configuration** task.

To customize an activation profile to allow a logical partition to use cryptographic facilities and functions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the General page.
3. Select **General**, **LINUX Only**, **z/VM**, or **SSC** from the Mode list.

   Note: Available starting on the Hardware Management Console Version 2.14.0 version.
4. Select **Crypto** from the profile tree view on the left side of the window. Use the controls on the Crypto page to indicate whether and how you want the logical partition to use the cryptographic functions and facilities.

   Notes:

   - If you intend to use the Integrated Cryptographic Service Facility (ICSF), see "Using the z/OS Integrated Cryptographic Service Facility (ICSF)" on page 757 for additional instructions for customizing the Crypto page.
   - If you intend to use a Trusted Key Entry (TKE) workstation to manage cryptographic keys, see "Using the Trusted Key Entry (TKE) Workstation feature" on page 758 for additional instructions for customizing the Crypto page.
   - After activating logical partitions customized to use Crypto Express feature, you can use the Support Element workplace to view the settings of the cryptographic controls set on the Crypto page of their activation profiles. See "View LPAR cryptographic controls" on page 758 for more information.
5. Customize the Load page to load an operating system that supports using cryptographic functions and facilities.

   For more information about loading an operating system, see the topics that follow "Loading an operating system during activation" on page 754.

Using the z/OS Integrated Cryptographic Service Facility (ICSF)

The z/OS Integrated Cryptographic Service Facility (ICSF) is a program product that provides secure, high-speed cryptographic services in the operating environment. You can use ICSF services for all logical partitions that are customized for using Crypto Express feature.

Note: Some functions of ICSF may fail if you do not have the CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement feature installed. See the *ICSF Application Programmer's Guide* or the *ICSF System Programmer's Guide* for complete information.

The activation profile you use to activate a logical partition can prepare it for using ICSF services. Customize the activation profiles when installing the CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement feature.

To customize an activation profile for a logical partition to use the ICSF services:

1. Customize a reset profile or image profile to configure the logical partition access to the cryptographic facilities and functions.

   For more information, see "Reset profiles" on page 737 or "Images profiles" on page 759.
2. Select the Crypto page again.
3. If you have not already set the logical partition's controls, set them now:

   a. Select a usage domain index for the logical partition to use for cryptographic functions from the **Usage domain index** list. More than one number should be selected from the **Usage domain index** when z/VM operating environment is running in the logical partition with other guests (for example, Linux) requiring access to the cryptographic hardware.

   Note: The cryptographic number, selected from the Cryptographic Candidate List, coupled with the usage domain index must be unique for each active partition.
4. Select from the Online List the number which specifies the coprocessors to be brought online at partition activation. For each number selected in the Online List, the corresponding number in the Candidate List must be selected.

Using the Trusted Key Entry (TKE) Workstation feature

A Trusted Key Entry (TKE) is a workstation application supported by ICSF to allow an alternative method of securely loading cryptographic keys (DES and PKA master keys and operational keys). A unique set of cryptographic keys is maintained for each domain index within the cryptographic facility. Only one partition can perform TKE functions at a time. The logical partition with this control is referred to as the TKE host. The other partitions that receive key updates from the TKE host are referred to as the TKE targets.

The activation profile you use to activate a logical partition can prepare it for being a TKE host or TKE target.

To customize an activation profile for a TKE host logical partition:

1. Customize a reset profile or image profile to enable the logical partition to use cryptographic facilities and functions.

   For more information, see “Reset profiles” on page 737 or “Images profiles” on page 759.
2. Select the Crypto again.
3. If you have not already set the logical partition's controls, set them now:

   a. Select a usage domain index for the logical partition to use for cryptographic functions from the **Usage domain index** list. It must be the same as the usage domain index set for the logical partition in the ICSF installation options data set.

      Note: The cryptographic number, selected from the Cryptographic Candidate List, coupled with the usage domain index must be unique for each active partition.
4. Select from the Online List the number which specifies the coprocessors to be brought online at partition activation. For each number selected in the Online List, the corresponding number in the Candidate List must be selected.
5. From the **Control domain index** list, also select each index that is the same as the usage domain index of each TKE target logical partition you want to manage through a TKE workstation connection to this TKE host logical partition.

View LPAR cryptographic controls

You can use the Support Element workplace to start the task to review information about the active logical partitions that use the Crypto Express feature assigned to them. You can review:

- A summary tab page of information on all active logical partitions.
- Individual tab pages for each logical partition's cryptographic controls.

To review the logical partition's cryptographic controls:

1. Open the **View LPAR Cryptographic Controls** task.

   The View LPAR Cryptographic Controls window displays. The window includes a summarized view tab for cryptos on all partitions and individual tabs for each logical partition's cryptographic controls.
2. Click **OK** when you have finished.

Profiles for staged activations

You can perform a staged activation of a central processor complex (CPC) and its images by using a reset profile for an initial activation of the CPC, and then using other types of profiles for selective activations of its images.

Typical staged activations include:

- Using a reset profile to initially activate the CPC and to activate and load one or more logical partitions. Then, at a later time, using load profiles to load one or more previously activated logical partitions with a different operating system, or using image profiles to activate and load one or more logical partitions not previously activated.

This type of staged activation allows the operator to change the active logical partitions while maintaining the rest of the CPC's current operational capabilities and characteristics.

Images profiles

Customize an image profile for activating a logical partition when you want to activate only the logical partition, after the central processor complex (CPC) that supports it is initially activated.

Optionally, you can customize the image profile to also load the logical partition during activation.

Notes:

- Initially activating a CPC requires customizing and using a reset profile. For more information, see “Supporting LPAR mode operation” on page 738 and the other topics that follow.
- The name of an image profile is the same as the name of the logical partition it activates. Each logical partition has only one image profile.

  Each reset profile that activates a logical partition includes the logical partition's only image profile, so changing the logical partition's information in any activation profile changes the same information in all the other profiles as well. That is, if you customize an image profile for activating a logical partition, for example, changing the image profile *also* changes the logical partition's information in every reset profile that activates the logical partition.

The information used to activate a logical partition, though it is included in a reset profile, is actually the logical partition's image profile.

To open a logical partition's image profile:

1. Locate the **Images** you want to work with.
2. Locate the image with the same name as the logical partition.
3. Locate and open the **Customize/Delete Activation Profiles** task to start it.

   This opens the image profile and the list of load profiles you want to customize. When the list is initially displayed, the highlighted profile is the currently assigned profile for the partition.
4. Select from the list the name of the image profile you want to customize.
5. Click **Customize**.

Checking a logical partition's assigned activation profile

You can assign a logical partition either its image profile or a load profile as its activation profile. Whenever the logical partition is activated, individually rather than with the central processor complex (CPC), it is activated according to the information in its assigned activation profile.

In addition, whenever you start the task for customizing the logical partition's activation profiles, it opens the logical partition's assigned activation profile. After you start the task, you can customize its assigned activation profile. If its assigned activation profile is a load profile, you can also create new load profiles or open and customize any other existing load profiles.

For example, to customize the image profile for a logical partition, its assigned activation profile must be its image profile. You can check, and change if necessary, the logical partition's assigned activation profile before you begin customizing its profiles.

To check or change a logical partition's activation profile:

1. Locate the **Images** you want to work with.
2. Locate the image with the same name as the logical partition.
3. Click **Change options**.

   This opens the Change Object Options window.
4. Locate the **Profile name** field.

   It displays the name of the profile currently assigned as the logical partition's activation profile.

5. Locate the same name in the **Profile name** column in the list of profiles below the field. Then check the profile's type in the **Type** column.

   Note: The list includes the logical partition's image profile and all the load profiles that can be assigned to the logical partition.

6. If the assigned profile's type is **Image**, then no further action is required.

   Whenever you start the task for customizing the logical partition's activation profiles, you will be able to customize the logical partition's image profile.

7. If the assigned profile's type is **Load**, you will be able to customize only load profiles.

   To assign the logical partition its image profile instead, use the window to select and save the image profile.

Creating a new image profile

You are responsible for creating image profiles that meet your unique needs.

You can use the default image profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and customize your own image profiles, you can use them as templates for creating more new profiles.

To create a new image profile:

1. Select the General page.

   The **Profile name** field identifies the image profile you opened. It will be used as a template for the new image profile.

2. To use a different image profile as a template:
3. Click the list button beside the **Profile name** field.

   This opens a list of the names of all the image profiles. The image profile named DEFAULT is the default image profile provided by IBM.

4. Select from the list the name of the image profile you want to use as a template.

   This opens the selected image profile. Its information replaces the previous profile's information on the pages of the notebook.

5. Enter a unique name for the new profile in the **Profile name** field.
6. Click **Save** to save the profile with the new name.

   Note: Saving the new profile does not change the image profile you used as a template.

Creating one or more image profiles

The New Image Profile Wizard tool can be used to configure new image profile parameters for one or more images currently selected in the IOCDS that do not have corresponding image profiles.

1. Select an image profile that is currently not created.
2. Click **New image profile**.
3. Use the New Image Profiles Wizard to create data for the image profile that you selected.
4. Complete the requested information for the image profile you are creating.
5. Click **Finish** to confirm your changes.

Customize multiple image profiles

The Customize Image Profile Wizard tool can be used to modify parameters for two or more of the image profiles that you select on the customize/delete activation profiles list.

1. Select two or more image profiles that you want to change parameters.
2. Click **Customize profile**.
3. Select the profiles you want to customize from the menu list. Then click **OK**.

4. Use the Customize Multiple Image Profile Wizard to modify data for two or more of the image profiles that you selected.
5. Click **Next** to start.
6. Check the appropriate check box that you want to make changes.
7. Click **Finish** to confirm your changes.

Saving an image profile

You must save an image profile to save the information you customized on its pages.

To save an open image profile:

1. After opening and customizing an image profile, select the General page.

   The **Profile name** field identifies the image profile that will be saved.
2. Click **Save** to save the image profile and close it.

Load profiles

Customize a load profile for loading an object when you want to only load the object after it is initially activated.

Customize a load profile for loading a logical partition when you want to only load the logical partition again, after it is initially activated on a CPC activated.

Note: Initially activating a logical partition requires customizing the reset profile that activates the CPC. For more information, see "Supporting LPAR mode operation" on page 738, and "Activating logical partitions during CPC activation" on page 744 along with the topics that follow.

To open a load profile:

1. Locate the **CPC** to work with.
2. Locate and open the **Customize/Delete Activation Profiles** task to start it.

   This opens the profile list that you want to customize. When the list of profiles is initially displayed, the highlighted profile is the currently assigned profile for the object.
3. Select from the list the name of the load profile you want to customize.
4. Click **Customize**.

   This opens the selected load profile.

Choosing a load type: Standard load, SCSI load, NVMe load, SCSI dump, or NVMe dump

The activation profile you use to load a central processor complex (CPC) can perform either a Standard Load, SCSI load, NVMe load, SCSI dump load, or NVMe dump load.

To customize an activation profile to choose a CPC load type:

1. Locate the **Load type** controls to select the following load types:
   - Select **Standard load** to perform a normal load from a device (such as internal z DASD).

     Notes:

     – If you intend to perform the store status function during the load, select **Store status**.

     – If you intend to clear main memory before loading, select **Clear the main memory on this partition before loading it**.
   - Select **SCSI load** or **NVMe load** to perform a SCSI load (from certain types of channels) or NVMe load (from certain types of adapters).

     Note: If you intend to clear main memory before loading, select **Clear the main memory on this partition before loading it**.
   - Select **SCSI dump** or **NVMe dump** to perform a SCSI dump (to do a standalone dump from a SCSI IPL type of device) or NVMe dump (to do a NVMe dump from a NVMe type of adapter).

Performing store status before a standard load

The activation profile you use to load a central processor complex (CPC) can perform the store status function before performing a standard load.

The store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations.

Note: For this reason, store status can be performed only before a Standard load.

Attention: Do *not* customize an activation profile to perform store status if the profile is customized to load an operating system that already automatically performs store status upon being loaded.

To customize an activation profile to perform store status before a Standard load:

1. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
2. Locate the **Load type** controls. Select **Standard load** to perform a a load from a device.
3. Mark the **Store status** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform the store status function before performing the load.

Creating a new load profile

You are responsible for creating load profiles that meet your unique needs.

You can use the default load profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and customize your own load profiles, you can use them as templates for creating more new profiles.

To create a new load profile:

1. Locate the **Profile name** field.

   The field identifies the load profile you opened. It will be used as a template for the new load profile.
2. To use a different load profile as a template:
   a. Select the list button beside the **Profile name** field.

      This opens a list of the names of all the load profiles. The load profile named DEFAULTLOAD is the default load profile provided.
   b. Select from the list the name of the load profile you want to use as a template.

      This opens the selected load profile. Its information replaces the previous profile's information on the notebook page.
3. Enter a unique name for the new profile in the **Profile name** field.
4. Click **Save** to save the profile with the new name.

   Note: Saving the new profile does not change the load profile you used as a template.

Assigning a load profile

After you open a load profile for an object, either a central processor complex (CPC) or logical partition, you can assign it to the object as its activation profile. Whenever the object is activated, it is activated according to the information in its assigned activation profile.

To assign an open load profile as an object's activation profile:

1. After opening and customizing a load profile, the **Profile name** field identifies the load profile that will be assigned to the object.
2. Select the **Assign profile** push button to assign the load profile as the object's activation profile.

Saving a load profile

You must save a load profile to save the information you customized on its page.

To save an open load profile:

1. After opening and customizing a load profile, the **Profile name** field identifies the load profile that will be saved.
2. Click **Save** to save the load profile and close it.

Group profile

Customize a group profile for activating a logical partition group after the central processor (CPC) that supports it is initially activated.

To open a group profile:

1. Locate the **CPC** to work with.
2. Locate and open the **Customize/Delete Activation Profiles** task to start it.

   This opens the profile list that you want to customize. When the list of profiles is initially displayed, the highlighted profile is the currently assigned profile for the object.
3. Select from the list the group profile to customize.
4. Click **Customize**.

   This opens the selected group profile.

Creating a new group profile

To customize a logical partition group name, enter a new name in the field. To view or customize an exiting logical partition group name, select the arrow beside the field to list the names of existing group names.

You can use the default group name as a template for creating a new group name.

To create a new group name:

1. The **Group name** field identifies the group profile name. It can be used as a template for the new group name.
2. Click the list button beside the **Group name** field to use a different group name as a template.

   This opens a list of the names of all the group names. The group named DEFAULT is the default group name provided.
3. Select from the list the name of the group you want to use as a template.
4. To create a new group name, enter a unique name for the new logical partition in the **Group name** field.
5. Enter a description of the new group name in the **Group description** field.
6. Click **Save** to save the group profile with the new.

Setting a group capacity value

The group capacity value can be specified in determining allocation and management of processor resources assigned for a logical partition group. The activation profile you use to activate a logical partition group can control the defined capacity for the logical partition group.

To customize an activation profile to set group capacity:

1. Enter the group capacity value for your logical partition group.
2. Click **Save** to store the values.

Setting an absolute capping value

The absolute capping value can be specified in determining allocation and management of processor resources assigned for a logical partition group. The activation profile you use to activate a logical

partition group can control the defined absolute capping value for the logical partition group. The absolute capping can be None or a number of processors value from 0.01 to 255.0.

To customize an activation profile to set absolute capping:

1. In the processor type table, select the current absolute capping setting in its field.
2. Use the Customize Group Profiles window to specify the absolute capping for the selected processor type.
3. Click **Save** to store the values.

Grouping the CPC for complete activation

You can customize more than one reset profile for performing complete activations of the CPC and its images. You can customize a reset profile for a complete activation of the CPC.

To use a reset profile for activating the CPC, you must assign it to the CPC before performing the activation. Afterwards, to use a different reset profile for activating the CPC, you could assign it to the CPC, replacing the previously assigned profile.

Rather than changing the reset profile assigned to a CPC each time you want to use a different one, you can instead create a unique group with the CPC for each reset profile you want to assign to it.

To assign the CPC a reset profile for activating it:

1. Create a group with the CPC for activating it:
    a. Give the group a meaningful name, like LPARMODE.
    b. Assign the group's CPC the reset profile for activating it in LPAR mode.

Then to activate the CPC with either profile, simply activate the appropriate group.

Grouping the CPC for staged activations

You can customize a reset profile for performing an initial activation of the CPC and customize a load profile for performing a subsequent activation that only loads it. For example, you may:

- Customize the reset profile to activate the CPC and load the operating system used for production.
- And customize the load profile to only load the CPC with the operating system used for performing dumps.

To use the reset profile for activating the CPC, you must assign it to the CPC before performing the activation. Afterwards, to use the load profile for activating the CPC, you could assign it to the CPC, replacing the previously assigned profile.

Rather than changing the activation profile assigned to a CPC each time you want to use a different one, you can instead create a unique group with the CPC for each activation profile you want to assign to it.

For example, to assign the CPC both a reset profile for activating it initially, and a load profile for only loading it:

1. Create a group with the CPC for activating it initially:
    a. Give the group a meaningful name, like PRODUCTION.
    b. Assign the group's CPC the reset profile.
2. Create another group with the CPC for only loading it:
    a. Give the group a meaningful name, like LOADFORDUMP.
    b. Assign the group's CPC the load profile.

Then to activate the CPC with either profile, simply activate the appropriate group.

Grouping images for staged activations

You can customize more than one activation profile for performing staged activations of the CPC and its images. For example, you may:

- Customize a reset profile for an initial activation of the CPC, with support for activating three logical partitions, but initially activating only of one of the logical partitions to support your production environment.
- And customize image profiles for activating the other two logical partitions to support batch processing and testing environments.

Using the reset profile for activating the CPC and one logical partition still automatically assigns *each* logical partition an image profile of the same name as its activation profile. Afterwards, you may want to deactivate the first logical partition, and then activate the other two logical partitions.

To help distinguish between the different purposes of the logical partitions, you can create a unique group with the logical partitions that support each purpose.

So, for example, to use one logical partition for production, and the other two logical partitions for batch processing and testing:

1. Create a group with the logical partition used for production.

   Give the group a meaningful name, like PRODUCTION.
2. Create another group with the logical partitions used for batch processing and testing.

   Give the group a meaningful name, like BATCHANDTEST.

Then to establish either environment, simply activate the appropriate group after deactivating the other group.

Note: The logical partitions in either group will be activated according to the information in the image profiles automatically assigned to them by the initial activation of the CPC.

Customize/Delete Activation Profiles

Use this task to view, change, create, or delete activation profiles for the central processor complex (CPC) and their images.

There are four types of activation profiles:

- Reset profile used to activate a CPC and its images
- Load profile used to activate image and load a control program or operating system.
- Image profile used to activate an image of a CPC
- Group profile used to specify the capacity of a group of logical partitions.

Save
To save the current information and settings as an activation profile for the CPC, click **Save**.

Copy Profile
To put the current profile information and settings in a temporary storage area to make it available to other profiles and objects on the console, click **Copy Profile**.

Paste Profile
To retrieve the information and settings currently in the temporary storage area for the current profile type, click **Paste Profile**.

Assign Profile
To assign the current profile to the object, to use it to activate the object whenever activation is started from the console, click **Assign Profile**.

Cancel
To close the profile without making changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following:

Profile Tree

This lists all pages for the current profile and a list of referenced profiles and their pages.

Reset pages

This type of activation profile, referred to also as a reset profile, includes all the information necessary to activate a CPC and each image supported by the CPC.

Make a selection from the Profile Tree to view the CPC pages:

General
To describe the selected reset profile and its purpose, and to identify the Input/Output (I/O) configuration and operating mode to establish for the CPC activated by the profile, select **General**.

Storage
To customize the storage configuration to establish for the CPC activated by the profile, select **Storage**.

Dynamic
To customize information that controls whether the Input/Output (I/O) configuration established for the CPC activated by the profile can be dynamically changed, select **Dynamic**.

Options
To enable or disable global input/output (I/O) priority queuing and customize options for error handling and recovery for the CPC activate by the profile, select **Options**.

CP/SAP
To set the number of Central Processors (CPs) and System Assist Processors (SAPs) to configure for the CPC, select **CP/SAP**.

Fenced
To display the number of available processors when a book is fenced and to determine the processor assignment, select **Fenced**.

Partitions
To customize a list of logical partitions to activate, and the order in which they are activated, on the CPC activated by the profile, select **Partitions**.

Note: The CPC pages include this additional page if the operating mode selected on the **General** CPC page is logically partitioned (LPAR) mode.

The window includes a section of image pages for each logical partition listed on the **Partitions** page. The information in each section is used to activate the multiple images supported by the CPC.

General

Use this window to describe the selected profile and its purpose and to identify the Input/Output (I/O) configuration and operating mode to establish for the Central Processor Complex (CPC) activated by the profile.

Note: An activation profile used to activate a CPC is also referred to as a reset profile.

Profile name

Specify or select the name of the profile you want to work with:

- To customize a new profile, you can immediately edit the value that currently appears in the input field or you can select an item that appears in the drop-down list.
- To view or customize an existing profile, select the arrow beside the field to list the names of existing profiles. Then select a profile name from the list to display its information.

A profile name is required to save the information.

A profile name can be from 1 to 16 characters long. It cannot have special characters or imbedded blanks. Valid characters for a profile name are:

Characters 0 through 9
Decimal digits

Characters A through Z
Letters of the English alphabet

Note: Profile names are not case-sensitive. All alphabetic characters are saved in uppercase.

Description
Include a brief note, up to 50 characters long, that describes the contents or purpose of the profile.

Note: A description is recommended, but optional.

IOCDS table

Select an Input/Output Configuration Data Set (IOCDS) to use during activation to define the Input/Output (I/O) configuration for the Central Processor Complex (CPC).

The I/O configuration is the set of all I/O devices and channel paths available to the CPC.

Input/Output Configuration Data Set
Displays the data set identifier and name of the IOCDS.

Type
Identifies the operating mode supported by the IOCDS. This must match the operating mode selected in **Mode**.

Note: Activation will fail if a mismatch exists between an IOCDS and mode.

Allow Dynamic I/O
Indicates whether the IOCDS defines an I/O configuration that supports dynamic changes.

Partitions
This column displays the names of logical partitions supported by the IOCDS.

Mode

Select the operating mode to establish during activation to support the number and type of control programs that can operate on the Central Processor Complex (CPC).

The mode determines some of the other types of information included in the reset profile. Different profile information is associated with each different mode. Only profile information associated with the selected mode will be saved.

Note: Activation will fail if a mismatch exists between an IOCDS and mode.

Load Delay for Power Sequencing

Specify the amount of time to delay between completing power-on reset and performing a load.

The delay can be specified at a maximum of 100 minutes, 0 seconds.

This delay allows Input/Output (I/O) devices to power-on before the load starts.

You can find more detailed help on the following elements of this window:

Image Profile Configuration

Use this window to set up initial parameters when you select an IOCDS that contains two or more images that were defined in the IOCDS, but currently do not exist in the list of image profiles. The default image profile can be used as a template for creating the set of new image profiles.

You can select one of the following options to:

- Automatically creating all new images using the choices specified on this panel, or
- Create each individual image profile using the *New Image Profile Wizard*.

You can select one or more of the following options to apply to all new image profiles:

- Automatically assign unique logical partition identifiers to each new image profile which saves you the need to determine which logical partition identifiers are available for this IOCDS.

- Allows you to assign a profile description to each of the new image profiles. You can insert the logical partition name into the description by using the %NAME parameter. If you want to specify the %, you must type %%.
- Allows you to select an existing image profile and have the existing profile's data be copied to all new image profiles that are to be created.

OK
To apply the selected changes, click **OK**.

Cancel
To close the window without making a selection, click **Cancel**.

Help
To display help for the current window, click **Help**.

Storage

This window displays the storage available for allocating to the CPC's logical partitions. The **Mode** list in **General** of this reset profile identifies the operating mode you selected for activating the CPC.

Installed storage details

Displays the CPC's total amount of storage available for allocating to the CPC's logical partitions.

Customer storage
Displays the storage amount available for allocating to the Central Processor Complex's (CPC) logical partitions.

To customize each logical partition's storage configuration, select its image profile, then select **Storage**.

Dynamic

Use this window to customize information that controls whether the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) activated by the profile can be dynamically changed.

Dynamic I/O

This window allows you to customize the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) activated by the profile.

To set whether the I/O definition established for the CPC activated by the profile can be dynamically changed, select **Allow dynamic changes to the channel subsystem input/output (I/O) definition**.

If this is selected it indicates activating this profile establishes an I/O definition that can be dynamically changed. That is, dynamic I/O will be enabled. Otherwise, this indicates the I/O definition cannot be changed dynamically. That is, dynamic I/O will not be enabled.

The input/output (I/O) definition is the set of all I/O devices and channel paths available to a central processor complex (CPC). An input/output configuration data set (IOCDS) is used during power-on reset as the source of the I/O definition.

Ordinarily, changing the I/O definition requires performing a power-on reset with a modified or different IOCDS. Dynamically changing the I/O definition does not require a power-on reset.

Dynamically changing the I/O definition requires support from the selected IOCDS and from the Hardware Configuration Definition (HCD) feature of a Multiple Virtual Storage (MVS) operating system.

Then the I/O definition can be changed dynamically by using the HCD feature of MVS.

Note: The active IOCDS must also support dynamically changing the channel subsystem I/O definition.

Options

Use this window to enable or disable the global input/output (I/O) priority queuing, customize options for error handling and recovery, and set power saving for the Central Processor Complex (CPC) activated by the profile.

Enable global input/output I/O priority queuing

To enable or disable global I/O priority queuing dynamically after initial microcode load (IML), select **Enable global input/output I/O priority queuing**.

Global I/O priority queuing allows the operating system to specify a priority to be associated with an I/O request at Start Subchannel time. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

Automatic input/output (I/O) interface reset

To indicate whether the I/O interface is reset automatically when any condition occurs that causes shared control units to hold reserves on their devices, select **Automatic input/output (I/O) interface reset**.

- A machine check places the Central Processor Complex (CPC) in a check stopped state.
- A control program places a logical partition in a non-restartable wait state.

If selected, the I/O interface is reset automatically if any of the listed conditions occurs. Otherwise, this indicates the I/O interface is not reset automatically.

In a multiple CPC environment, several objects, which can be CPCs or logical partition, may share the control units, channel paths, and I/O devices included in their I/O interfaces.

Each condition listed above causes shared control units to hold reserves on their devices for the object affected by the condition, Holding reserves provides the affected object with exclusive use of devices, preventing them from being used by other objects that share the control units.

Resetting the I/O interface releases reserves held by shared control units assigned to an object. Their devices become available to other objects.

Note: Automatically resetting the I/O interface will not recover the object from any of the conditions.

Processor running time

If the profile activates the Central Processor Complex (CPC), use this section to indicate how processor running time is determined.

Processor running time is the amount of continuous time allowed for logical processors to perform jobs on shared processors. The amount of continuous time is also referred to as a timeslice.

Dynamically determined by the system

To have the CPC calculate the running time whenever the number of active logical processors changes, select **Dynamically determined by the system**.

Note: When processor running time is dynamically determined, it reduces the possibilities for suboptimal use of processor resources.

Determined by the user

To have this profile set a constant running time, select **Determined by the user**. Then specify the time in the **Running time** field.

Running time

When the processor running time is determined by the user through this profile, type the constant amount of running time set for logical processors to perform jobs on shared processors in the **Running time** field.

The running time can be from 1 to 100 milliseconds.

The running time specified is assigned to all logical processors shared by logical partitions activated without dedicated processing resources. Each logical partition has control of shared processor resources for the specified running time. Control passes to the next logical partition when the running time interval expires.

Note: This field is applicable only when **Determined by the user** is selected. Otherwise, this field is unavailable.

Do not end the timeslice if a partition enters a wait state (HMC Version 2.13.1 and earlier)

When the processor running time is determined by the user through this profile, type the constant amount of running time set for logical processors to perform jobs on shared processors in the **Running time** field.

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

The running time can be from 1 to 100 milliseconds.

The running time specified is assigned to all logical processors shared by logical partitions activated without dedicated processing resources. Each logical partition has control of shared processor resources for the specified running time. Control passes to the next logical partition when the running time interval expires.

Note: This field is applicable only when **Determined by the user** is selected. Otherwise, this field is unavailable.

System Recovery Time

Use this section to indicate whether there is a limit on the amount of time the Central Processor Complex (CPC) is allowed to spend on error handling and recovery.

Limit system recovery time

If recovery time is limited, specify the amount of time the Central Processor Complex (CPC) is allowed to spend on error handling and recovery before it is put into a checkstop state.

The time limit can be from 1 to 999 seconds.

The amount of time determines the type of recovery that is attempted. If recovery time is not limited, then all types of recovery are attempted.

Note: This field is applicable only **Limit system recovery time** is selected. Otherwise, this field is unavailable.

Time limit

If recovery time is limited, specify the amount of time the Central Processor Complex (CPC) is allowed to spend on error handling and recovery before it is put into a checkstop state.

The time limit can be from 1 to 999 seconds.

The amount of time determines the type of recovery that is attempted. If recovery time is not limited, then all types of recovery are attempted.

Note: This field is applicable only **Limit system recovery time** is selected. Otherwise, this field is unavailable.

Set Power Saving

Use this window to select the energy management power saving option for the CPC upon performing the power-on reset. Power saving is used to reduce the average energy consumption of the system.

Custom energy management

Emergency high performance
To use the high performance setting with no power saving, select **Emergency high performance**.

Display fenced book page
Check this option to display the Fenced window.

CP/SAP

Note: This page is available on the Hardware Management Console Version 2.13.1 and earlier.

Use this window to set the number of Central Processors (CPs) and System Assist Processors (SAPs) to configure for the Central Processor Complex (CPC).

The window lists the configurations of CPs and SAPs that can be established. The machine type and model of the CPC determine its possible configurations:

- All CPCs have a default configuration.
- Some CPCs have additional configurations available. That is, some CPC's allow configuring one or more CPs as additional SAPs.

The CPC's default configuration is listed first, followed by its additional configurations, if any. Select the configuration you want established when this profile is used to activate the CPC.

CP/SAP table

CPs
Displays the number of central processors (CPs) in each configuration.

SAPs
Displays the number of system assist processors (SAPs) in each configuration.

The physical processor units installed in a central processor complex (CPC) are used either as central processors (CPs) or system assist processors (SAPs). The model of your machine determines its default configuration of CPs and SAPs. The SAPs are used exclusively for input/output (I/O) instruction processing.

Some CPC machine types and models allow configuring one or more CPs as additional SAPs. If other CP/SAP configurations are available, selecting a configuration that configures one or more CPs as additional SAPs may improve the performance of some types of applications (applications that have greater needs for I/O instruction processing, for example). But this reduces the default number of CPs available which may affect how the CPC can be activated.

No additional action is necessary if you intend to activate the CPC in a basic operating mode. But if you intend to activate the CPC, a reduction in the number of available CPs will reduce the number of logical processors you can assign to logical partitions.

Note: Activation of a logical partition will fail if the number of logical processors you attempt to assign exceeds the number of CPs available. To avoid a logical partition activation failure, verify the number of logical processors assigned to a logical partition does not exceed the number of CPs available.

Internal coupling facility processors (ICFs)
Displays the number of internal coupling facility processors (ICFs).

Integrated facilities for Linux (IFLs)
Displays the number of integrated facilities for Linux (IFLs) processors.

zEnterprise Application Assist Processors (zAAPs)

Displays the number of zEnterprise Application Assist Processors (zAAPs).

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

z Integrated Information Processors (zIIPs)
Displays the number of z Integrated Information Processors (zIIPs).

Defective processing units
Displays the number of defective processing units.

Display fenced book page
Check this option to display the Fenced window.

Fenced CPC drawer

This window allows you to determine how the available system processors would be assigned when a hardware problem occurs with one of the CPC drawers that causes the system to be fenced or become unavailable for use.

- **Number of available processors for Licensed Internal Code** indicates the number of processors that are available in your system.
- **Number of available processors when a CPC drawer is fenced** indicates the number of processors that your system can use when one system drawer is fenced from use.
- **Number of available processors when a XX processors drawer is fenced** where XX indicates the number of processors that your system can use when the specified processors drawer is fenced from use.

Processors assignment controls

Select a processor assignment option.

Determined by the system
Select this option if you want the system to determine how to assign all available processors when a drawer is fenced from use in your system.

Determined by the user
Select this option if you want to manually assign the processors to your system when a drawer is fenced from use.

Processor assignments

Display processor assignment when a XX processors drawer is fenced
Where XX indicates the number of processors fenced from use. Select this option to display the processor assignments

Processor type
Displays the physical processor assigned to the logical partitions logical processors

LICCC Definition
Displays the amount of licensed internal code installed in your system

Value used when CPC drawer is Fenced
Indicates how many processors have been assigned to the specified processor types.

Partitions

Use this window to customize a list of logical partitions to be activated and the order in which they are activated on the Central Processor Complex (CPC) activated by the profile.

To activate a logical partition, you must provide its name **and** activation order. Logical partitions with blank activation orders will not be activated and their names on this page will not be saved in the profile.

Partition
Specify the names of the logical partitions to activate.

Order
Specify the numeric positions of the logical partitions in the activation order.

Important: Logical partitions activated in coupling facility mode, if any, should be activated first.

For each logical partition to be activated, customize the information for activating it in its corresponding set of image pages. To display the image pages for a logical partition, select its pages from the profile tree view on the left side of the window.

Load

Use this window to customize information that controls loading a control program for the logical partition activated by the profile.

Use this window to customize information that controls loading a control program for the logical partition activated by the profile.

Note: The image pages do not include this additional page if the operating mode selected on the **General** image page is coupling facility or SSC mode.

Profile name

Specify or select the name of the profile you want to work with:

- To customize a new profile, specify a new name in the field.
- To view or customize an existing profile, select the list button beside the field to list the names of existing profiles. Then select a profile name from the list to display its information on the window.

A profile name is required to save the information on the window.

A profile name can be from 1 to 16 characters long. It cannot have special characters or imbedded blanks. Valid characters for a profile name are:

Characters 0 through 9
Decimal digits

Characters A through Z
Letters of the English alphabet

Note: Profile names are not case-sensitive. All alphabetic characters are saved in uppercase.

Description
Enter a brief note, up to 50 characters long, that describes the contents or the purpose of the profile. A description is recommended, but optional.

Load type
Select the type of load to perform for the logical partition. Optionally, select the clear main storage on the logical partition before loading. You would use the SCSI or NVMe dump option to do a standalone dump to a SCSI device or NVMe adapter.

Standard load
To perform the load on the logical partition, click **Standard load**.

Note: You must select this choice if you want to perform the **Store status** function and the **Store status** clear check box must be unchecked.

SCSI load
To IPL from a device that requires a SCSI load, click **SCSI load**.

SCSI dump
To IPL a standalone dump program from a device that requires a SCSI load, click **SCSI dump**.

NVMe load
To IPL from a device that requires a NVMe load, click **NVMe load**.

NVMe dump
To IPL a standalone dump program from a device that requires a NVMe load, click **NVMe dump**.

Clear the main memory on this partition before loading it
Select this to clear main memory storage on the logical partition before a load.

Note: Available when **Standard load**, **SCSI load**, or **NVMe load** are selected. Clearing partitions with larger amounts of main memory storage may take longer.

Enable Secure Boot for Linux
To verify the signature of the load program and distributor's signature match , select **Enable Secure Boot for Linux**.

Load address

Enter the address of the input/output (I/O) device that provides access to the control program to load. For a SCSI load, NVMe load, SCSI dump, or NVMe dump, this field has the device number of the device (for example, fibre channel adapter) that will be used to perform the SCSI load or NVMe load. This should contain four hexadecimal digits for NVMe load or five hexadecimal digits for SCSI load.

A load address is required.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device can store the control program or can be used to read the control program from a data storage medium.

Note: This field is applicable only when **Use dynamically changed address** check box is empty. Otherwise, if the check box displays a check mark, this field is unavailable.

Use dynamically changed address

To indicate whether the load address is dynamically determined by changes to the channel subsystem Input/Output definition (I/O), select **Use dynamically changed address**.

If this is selected, the load address is dynamically determined. Otherwise, this profile sets the load address. See the **Load address** field for the address set by this profile.

Load parameter

Specify the optional information, if any, to use to further control how the control program is loaded during activation. Valid characters for a load parameter are:

- At (@)
- Pound (#)
- Dollar ($)
- Blank character
- Period (.)
- Decimal digits 0 through 9
- Capital letters A through Z .

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Note: This field is applicable only when **Use dynamically changed parameter** is **not** selected. Otherwise, this field is unavailable.

Use dynamically changed parameter

To indicate whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition, select **Use dynamically changed parameter**

If this is selected, the load parameter is dynamically determined. Otherwise, this profile sets the load parameter. Enter the parameter for this profile in the **Load parameter** field.

Time-out value

Specify the amount of time to allow for the completion of the load.

The time-out value can be from 60 to 600 seconds. If the load operation cannot be completed within the specified time, the operation is canceled.

This field is unavailable if a load type of **SCSI load** or **SCSI dump** is selected.

Store status

The store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations. (This function is effective only when the status of the processor performing the load is **Stopped**.)

If the selected load type is **Standard load**, this check box indicates whether to perform the store status function before the load. If the selected load type is **SCSI load** or **SCSI dump**, the store status function cannot be performed.

If the selected load type is **Standard load**, click the check box to change the setting.

- A check mark indicates performing the store status function before the load.

- An empty check box indicates not performing the store status function before the load.

Worldwide port name

Specify the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI load or SCSI dump.

If the selected load type is **Standard load**, **NVMe load**, or **NVMe dump** this field is unavailable.

Logical unit number

Specify the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

If the selected load type is **Standard load**, **NVMe load**, or **NVMe dump** this field is unavailable.

Boot program selector

This field identifies the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30. This parameter provides the possibility of having up to 31 different boot configurations on a single disk device. This field should be set to 0 for optical media SCSI devices.

If the selected load type is **Standard load**, this field is unavailable.

Boot record logical block address

Specify the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

If the selected load type is **Standard load**, this field is unavailable.

Operating system specific load parameters

Specify a variable number of characters to be used by the program that is loaded during SCSI load, NVMe load, SCSI dump, or NVMe dump. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

If the selected load type is **Standard load**, this field is unavailable.

Image pages

This window displays an activation profile for activating a logical partition as an image. The window displays the image name.

Make a selection from the Profile Tree to view the image pages in the profile:

General
To describe the image profile and its purpose, and to identify the operating mode established for the logical partition activated by the profile, select **General**.

Processor
To customize information that assigns logical processors to the logical partition activated by the profile, select **Processor**.

Security
To customize settings that determine the extent of interaction between the logical partition activated by the profile and other logical partitions activated on the same CPC, click **Security**.

Storage
To set the amount of storage assigned to the logical partition activated by the profile, select **Storage**.

Options
To specify the image option for the processor values, select **Options**.

Load
To customize information that controls loading a control program for the logical partition activated by the profile, select **Load**.

Note: Not available when Coupling facility, Secure Service Container, or zAware are selected on the **General** image page.

"zAware" on page 789
To specify the image option for the zAware values, select **zAware**.

Note: This tab is only applicable for z13, zEC12, and zBC12.

"SSC" on page 792
To set up the IBM Secure Service Container (Secure Service Container), select **SSC**.

Crypto
To customize information that controls how the logical partition activated by the profile uses coprocessors and accelerators assigned to it, select **Crypto**.

Note: Not available when Coupling facility or zAware are selected on the **General** image page.

Time Offset
To set the logical partition's clock using an offset from the External Time Source's time of day, select **Time Offset**.

Note: Available when **Logical partition offset** is selected on the **General** image page.

General

Use this window to describe the image profile and its purpose and to identify the operating mode established for the logical partition activated by the profile.

Profile name

Specify the name of the profile you want to work with:

- To customize a new profile, enter a new name in the field.
- To view or customize an existing profile, select the arrow beside the field to list the names of existing profiles. Then select a profile name from the list to display its information.

A profile name is required to save the information.

A profile name can be from 1 to 8 characters long. It cannot have special characters or imbedded blanks. Valid characters for a profile name are:

Characters 0 through 9
Decimal digits

Characters A through Z
Letters of the English alphabet

Note: Profile names are not case-sensitive. All alphabetic characters are saved in uppercase.

Description

Specify a brief note, up to 50 characters long, that describes the contents or purpose of the profile.

Note: A description is recommended, but optional.

Partition identifier

Specify the two hexadecimal digits partition identifier to be used by the logical partition. The partition identifier can be from X'0' to X'7F' or X'0' to X'3F' (Hardware Management Console Version 2.12.1 and earlier).

The partition identifier must also be unique among the identifiers of other logical partitions activated by the reset profile. If necessary, check the partition identifier fields on the other **General** image pages to verify the partition identifier assigned to this image is unique.

Mode

Select the operating mode to establish during activation to support the type of control program that can operate on the logical partition.

The mode determines some of the other types of information included in the image profile. Different profile information is associated with each different mode.

Note: Changing mode discards information exclusively associated with it. For example, changing from any mode to coupling facility mode discards the profile page that contains the load information and the profile page that contains the crypto information.

Clock Type Assignment

Select a time source for setting the logical partition's time-of-day (TOD) clock.

The logical partition's clock is synchronized with the central processor complex time-of-day clock (CPC TOD clock). Ordinarily, the logical partition's clock is set to the same time as the CPC's time source (either the CPC TOD clock or an external time reference, such as a Server Time Protocol(STP). You can use this group box to select another source for setting the logical partition's clock.

Standard time of day
To set the logical partition's clock to the same time set for the CPC's time source (either the CPC TOD clock or an external time reference, such as the Server Time Protocol (STP), select **Standard time of day**.

Logical partition time offset
If the CPC uses a Sysplex Timer as its time source, select **Logical partition time offset** to set the logical partition's clock using an offset from the External Time Source's time of day. Then use the **Time Offset** window to set the offset.

Ensure that the image profile data conforms to the current maximum LICCC configuration

Select this option to ensure that the image profile data conforms to the current maximum Licensed Internal Code Configuration Control (LICCC) configuration. The data entered in the image profiles has to be compatible and supported by the LICCC. If image profile data changes, is imported, or the LICCC definition changes the profiles will be modified automatically to meet the new LICCC configuration. If this option is unchecked, the data entered for an image profile can be outside the valid LICCC configuration.

Note: It is recommended that image profile data conform to the current maximum LICCC configuration.

Processor

Use this window to customize information that determines the allocation and management of processor resources assigned to the logical partition activated by the profile.

Use the **Logical processor assignment** group box to customize the logical partition's logical processor assignment.

Note: The **Mode** list on the **General** image page lists the operating modes. The logical partition operates in the selected mode upon being activated with this profile. Depending on the selected mode and what processors are installed in your system will determine the allocation and management of the processor resources.

You can find more detailed help on the following elements of this window:

Group Name

To change the group profile name assigned to the logical partition, select the arrow beside the field to list the names of existing group profiles and select a new group or create your own group profile name. A logical partition can be assigned to only one group.

Note: If the group profile name is blank, then the logical partition is not assigned to a group.

Logical Processor Assignment (CPs - General and SSC modes)

Use these selections to customize the logical partition's logical processor assignment.

Note: The zAware mode is applicable for z13, zEC12, and zBC12.

Make a selection to choose the physical processors you want assigned to the logical partition's logical processors. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated central processors**

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated central processors**

Logical Processor Assignment (CPs/zAAPs/zIIPs - General mode)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the logical partition's logical processors. Enter the initial and reserved number of processors for your selection. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Notes:

1. If you have temporary processors that are installed for use on your system, you can specify an initial number of processors that does not exceed the number of physical processors configured plus the number of installed temporary processors even if the temporary processors are not currently activated. You will not be able to activate the image unless the temporary processors are activated or the LICCC has been permanently updated to include extra processors.
2. Unless you plan to have your LICCC updated, it is best to specify the number of initial processors that does not exceed the number of configured physical processors and specify the temporary processors as reserved. The image can be activated without having to activate the temporary processors. The reserved processors can be brought on-line after the temporary processors have been activated and configured off-line before deactivating the temporary processors.
3. If you have temporary processors of a given type, but no physical processors of the same type, you can specify up the number of temporary processors of that type. You will not be able to activate it unless the temporary processors are activated or until the LICCC has been permanently updated to include the new processor types.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated processors**.

Dedicated zEnterprise Application Assist Processors (zAAPs)
If zEnterprise Application Assist Processors (zAAPs) is supported by and installed in the Central Processor Complex (CPC), select **Dedicated processors**, then select **zEnterprise application assist processors** if you want to assign zAAPs to each logical processor.

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

Dedicated z Integrated Information Processors (zIIPs)
If z Integrated Information Processors (zIIPs) is supported by and installed in the Central Processor Complex (CPC), select **Dedicated processors**, then select **z integrated information processors** if you want to assign zIIPs to each logical processor.

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Central processors**.

Not dedicated zEnterprise Application Assist Processors (zAAPs)
If zEnterprise Application Assist Processors (zAAPs) are supported by and installed in the Central Processor Complex (CPC), select **zEnterprise Application Assist Processors** to assign not dedicated zAAPs (zAAPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

Not dedicated z Integrated Information Processors (zIIPs)
If z Integrated Information Processors (zIIP) are supported by and installed in the Central Processor Complex (CPC), select **z Integrated Information Processors** to assign not dedicated zIIPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Logical Processor Assignment (CPs/ICFs - Coupling facility mode)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the partition's logical processors. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated central processors**.

Dedicated internal coupling facility processors
If internal coupling facility processors are supported by and installed in the central processor complex (CPC), select **Dedicated internal coupling facility processors** if you want one dedicated to each logical processor.

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated central processors**.

Not dedicated internal coupling facility processors
If you want the logical processors to share *not dedicated internal coupling facility processors* (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated internal coupling facility processors**.

Not dedicated internal coupling facility processors and not dedicated central processors
If internal coupling facility processors are supported by and installed in the central processor complex (CPC), select **Dedicated internal coupling facility processors and not dedicated central processors** if you want to assign a combination of dedicated internal coupling facility processors *and* not dedicated central processors to the logical partition.

Note: This option is only available on the console for Version 2.10.2 and earlier.

Dedicated and not dedicated internal coupling facility processors
If internal coupling facility processors are supported by and installed in the CPC, select **Dedicated and not dedicated internal coupling facility processors and not dedicated central processors** if you want to assign a combination of dedicated internal coupling facility processors *and* not dedicated internal coupling facility processors to the logical partition.

Note: This option is only available on the console for Version 2.10.2 and earlier.

Logical Processor Assignment (CPs/IFLs - Linux only mode)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the logical partition's logical processors. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated central processors**.

Dedicated Integrated Facilities for Linux
If Integrated Facilities for Linux (IFL) is supported and installed in the Central Processor Complex (CPC), select **Dedicated Integrated Facilities for Linux** if you want an integrated facilities for Linux dedicated to each logical processor.

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated central processors**.

Not dedicated Integrated Facility for Linux
If you want the logical processors to share *Not dedicated integrated facilities for Linux* (integrated facilities for Linux processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated Integrated Facilities for Linux (IFLs)**.

Logical Processor Assignment (CPs/zAAPs/zIIPs/ICFs/IFLs - z/VM mode)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the logical partition's logical processors. Enter the initial and reserved number of processors for your selection. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Notes:

1. If you have temporary processors that are installed for use on your system, you can specify an initial number of processors that does not exceed the number of physical processors configured plus the number of installed temporary processors even if the temporary processors are not currently activated. You will not be able to activate the image unless the temporary processors are activated or the LICCC has been permanently updated to include extra processors.
2. Unless you plan to have your LICCC updated, it is best to specify the number of initial processors that does not exceed the number of configured physical processors and specify the temporary processors as reserved. The image can be activated without having to activate the temporary processors. The reserved processors can be brought on-line after the temporary processors have been activated and configured off-line before deactivating the temporary processors.
3. If you have temporary processors of a given type, but no physical processors of the same type, you can specify up the number of temporary processors of that type. You will not be able to activate it unless the temporary processors are activated or until the LICCC has been permanently updated to include the new processor types.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated processors**.

Dedicated zEnterprise Application Assist Processors (zAAPs)
If zEnterprise Application Assist Processors (zAAPs) is supported by and installed in the central processor complex (CPC), select **Dedicated processors**, then select **zEnterprise application assist processors** if you want to assign zAAPs to each logical processor.

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

Dedicated z Integrated Information Processors (zIIPs)
If z Integrated Information Processors (zIIPs) is supported by and installed in the central processor complex (CPC), select **Dedicated processors**, then select **z Integrated Information Processors** if you want to assign zIIPs to each logical processor.

Dedicated Internal Coupling Facility Processors
If internal coupling facility is supported by and installed in the central processor complex (CPC), select **Dedicated processors**, then select **Internal Coupling Facility Processors (ICFs)** if you want to assign *internal coupling facility processors* to each logical processor.

Dedicated Integrated Facilities for Linux
If integrated facilities for Linux is supported by and installed in the central processor complex (CPC), select **Dedicated processors**, then select **Integrated Facilities for Linux (IFLs)** if you want to assign *Integrated Facilities for Linux* to each logical processor.

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Central processors**.

Not dedicated zEnterprise Application Assist Processors (zAAPs)
If zEnterprise Application Assist Processors (zAAPs) are supported by and installed in the central processor complex (CPC), select **zEnterprise application assist processors** to assign not dedicated zAAPs (zAAPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

Not dedicated z Integrated Information Processors (zIIPs)
If z Integrated Information Processors (zIIPs) are supported by and installed in the central processor complex (CPC), select **z Integrated Information Processors** to assign not dedicated zIIPs (zIIPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated Internal Coupling Facility Processors
f internal coupling facility processors are supported by and installed in the central processor complex (CPC), select **Internal Coupling Facility Processors (ICFs)** to assign not dedicated internal coupling facility processors (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated Integrated Facilities for Linux
If Integrated Facilities for Linux are supported by and installed in the Central Processor Complex (CPC), select **Integrated Facilities for Linux (IFLs)** to assign not dedicated integrated facilities for Linux (integrated facilities for Linux processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Number of processors (General, Coupling facility, Linux only, and SSC modes)

This field represents the number of processors that are used each time you activate a partition.

Note: The zAware mode is applicable for z13, zEC12, and zBC12.

A *logical processor* is the processor resource defined to operate in a logical partition as a physical processor. A logical partition's control program uses its logical processors to perform jobs for the logical partition.

Initial
Specify the number of logical processors to assign to the logical partition.

The number of processors can be from one to the maximum number of physical processors available to the logical partition. The maximum number of processors available is limited by:

- The number of physical processors configured and available.
- The number of processors supported by the operating mode selected on the **General** image page.
- The number of processors that are not already dedicated to another active logical partition at the time of the next activation.
- The number of processors supported by the control program at the time of the next activation.

Reserved
Specify the number of reserved processors available that you want assigned to the logical partition.

Reserved processors can be configured online at a later time. Reserved processors can be defined at partition activation time, but are not used during partition activation. Instead, they are configured offline during activation automatically, and can be manually configured online. The reserved processor

may or may not be available when the system is activated. If it is not available when the system is activated, it can become available during concurrent upgrade.

The ability to add and remove dedicated processors does not require deactivating/activating the partitions. This support is not restricted to concurrent upgrade purposes.

Notes:

1. This field is applied only when the following selection is made:
   - **Dedicated Central Processors**
   - **Not dedicated Central Processors**
   - **Dedicated Internal Coupling Facility processors**
   - **Not dedicated Internal Coupling Facility processors**
   - **Dedicated Integrated Facility for Linux**
   - **Not dedicated Integrated Facility for Linux**
2. If you have temporary processors that are installed for use on your system, you can specify an initial number of processors that does not exceed the number of physical processors configured plus the number of installed temporary processors even if the temporary processors are not currently activated. You will not be able to activate the image unless the temporary processors are activated or the LICCC has been permanently updated to include extra processors.
3. Unless you plan to have your LICCC updated, it is best to specify the number of initial processors that does not exceed the number of configured physical processors and specify the temporary processors as reserved. The image can be activated without having to activate the temporary processors. The reserved processors can be brought on-line after the temporary processors have been activated and configured off-line before deactivating the temporary processors.
4. If you have temporary processors of a given type, but no physical processors of the same type, you can specify up the number of temporary processors of that type. You will not be able to activate it unless the temporary processors are activated or until the LICCC has been permanently updated to include the new processor types.

Processor type (General, z/VM, and Coupling facility modes)

This field represents the number of processors that are used each time you activate a partition.

A *logical processor* is the processor resource defined to operate in a logical partition as a physical processor. A logical partition's control program uses its logical processors to perform jobs for the logical partition.

Initial
Specify the number of logical processors to assign to the logical partition.

The number of processors can be from one to the maximum number of physical processors available to the logical partition. The maximum number of processors available is limited by:

- The number of physical processors configured and available.
- The number of processors supported by the operating mode selected on the **General** image page.
- The number of processors that are not already dedicated to another active logical partition at the time of the next activation.
- The number of processors supported by the control program at the time of the next activation.

Reserved
Specify the number of reserved processors available that you want assigned to the logical partition.

Reserved processors can be configured online at a later time. Reserved processors can be defined at partition activation time, but are not used during partition activation. Instead, they are configured offline during activation automatically, and can be manually configured online. The reserved processor may or may not be available when the system is activated. If it is not available when the system is activated, it can become available during concurrent upgrade.

The ability to add and remove dedicated processors does not require deactivating/activating the partitions. This support is not restricted to concurrent upgrade purposes.

Note: This field is applied only when the following selection is made:

- **Dedicated internal coupling facility processors and not dedicated central processors**

  Note: This option is only available on the console for Version 2.10.2 and earlier
- **Dedicated and not dedicated internal coupling facility processors**

  Note: This option is only available on the console for Version 2.10.2 and earlier.

Not Dedicated Processor Details (General, Coupling facility, Linux only, z/VM, and SSC modes)

Use this section to specify initial processing weight, minimum and maximum processing weight, select whether or not to enable initial capping and workload manager, and to specify absolute capping.

Note: The zAware mode is applicable for z13, zEC12, and zBC12.

Initial processing weight

Specify the logical partition's processing weight for sharing the not dedicated processors.

The *not dedicated* processors are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *processing weight* is its share of the not dedicated processors. The processing weight can be from 1 to 999.

The exact percentage of the not dedicated processors allocated to the logical partition depends upon the processing weights of other logical partitions defined and activated on the same Central Processor Complex (CPC). That percentage is calculated by dividing the logical partition processing weight by the sum of the processing weights of all active logical partitions on the CPC.

A processing weight is a target, not a limit. It represents the share of the not dedicated processor resources guaranteed to a logical partition when all the resources are in use. When resources are available, this logical partition can borrow them if necessary. When this logical partition is not using its share of the resources, other logical partitions can use those resources.

Notes:

1. While excess resources are available, processing weights have no effect on how those resources are used. Weights take effect when the number of logical processors requiring a timeslice is greater than the number of not central processors.
2. This field is available only when either of the following selections are made:
   - **Not dedicated central processors**
   - **Not dedicated internal coupling facility processors**
   - **Dedicated internal coupling facility processors and not dedicated central processors**

     Note: This option is only available on the console for Version 2.10.2 and earlier.
   - **Not dedicated integrated facility for Linux**
   - **zEnterprise Application Assist Processors (zAAPs)**

     Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
   - **Not dedicated z Integrated Information Processors (zIIPs)**

   Otherwise, this field is unavailable.

Initial capping

You can specify whether the logical partition is prevented from using the not dedicated processors in excess of its processing weight.

To indicate the logical partition *cannot* use the not dedicated processors in excess of its processing weight, select **Initial capping**. That is, the processing weight is capped.

Otherwise, it indicates it can use the not dedicated processors in excess of its processing weight when the resources are not in use by another logical partition. That is, the processing weight is not capped.

The *Not dedicated processors* are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *processing weight* is its share of the not dedicated processors. Ordinarily, a processing weight is a target, not a limit. When the processing weight is *capped*, it is a limit.

Notes:

1. If this logical partition's share of the not dedicated processors is capped, it does not affect the shares set for other activated logical partitions.
2. This field is available only when the **Enable workload manager** check box is not checked and either of the following selections are made:
   - **Not dedicated central processors**
   - **Not dedicated integrated coupling facility processors**
   - **Dedicated integrated coupling facility processors and not dedicated central processors**

     Note: This option is only available on the console for Version 2.10.2 and earlier.
   - **Dedicated and not dedicated internal coupling facility processors**

     Note: This option is only available on the console for Version 2.10.2 and earlier.
   - **Not dedicated Integrated Facility for Linux**
   - **Not dedicated zEnterprise Application Assist Processors (zAAPs)**

     Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
   - **Not dedicated z Integrated Information Processors (zIIPs)**. Otherwise, this field is unavailable.

Enable workload manager

You can select either **Enable workload manager** or **Initial capping**, but not both. However, you do not have to select either one.

To enable the Workload Manager Intelligent Resource (IRD) weight management function, select **Enable workload manager**. Selecting WLM from one processor details automatically selects WLM from the other processor details and conversely. Specify the minimum and maximum processing weights. Changes to LPAR management weights based on customer Workload Management policies and current work loads. For more information, refer to *z/OS MVS Planning: Workload Management* for the release of z/OS that you are using.

Minimum processing weight
Minimum processing weight is the lowest weight that IRD weight management can use. The value must be less than or equal to the initial processing weight.

Maximum processing weight
Maximum processing weight is the highest weight that IRD weight management can use. Maximum processing weight must be greater than or equal to the initial processing weight.

Note: This field is available only when the **Initial capping** check box is not checked for any of the processor types and either of the following selections are made:

- **Not dedicated integrated facility for Linux**
- **Not dedicated central processors**
- **zEnterprise Application Assist Processors (zAAPs)**

  Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
- **Not dedicated z Integrated Information Processors (zIIPs)**

Otherwise, this field is unavailable.

Absolute Capping

You can specify whether the logical partition can use the not dedicated processors absolute capping.

To indicate the logical partition *can* use the not dedicated processors absolute capping, select **Absolute capping** to specify an absolute number of processors to cap the logical partition's activity. The absolute capping value can either be None or a number of processors value from 0.01 to 255.0 can be specified.

Otherwise, it indicates the logical partition *cannot* use the not dedicated processors absolute capping when the resources are in use by another logical partition. That is, the processing absolute number is not capped.

The *Not dedicated processors* are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *absolute capping* is its share of the not dedicated processors. When the absolute processing number is *capped*, it is a limit.

Notes:

1. If this logical partition's share of the not dedicated processors is capped, it does not affect the shares set for other activated logical partitions.
2. This field is available only when either of the following selections are made:
   - **Not dedicated central processors**
   - **Not dedicated integrated coupling facility processors**
   - **Not dedicated integrated facility for Linux**
   - **Central processors**
   - **Not dedicated zEnterprise Application Assist Processors (zAAPs)**

     Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
   - **Not dedicated z Integrated Information Processors (zIIPs)**

   Otherwise, this field is unavailable.

Security

Use this window to customize settings that determine the extent of interaction between the logical partition activated by the profile and other logical partitions activated on the same Central Processor Complex (CPC).

Partition Security Options

Use this section to specify the security options for the logical partitions activated by the profile.

Global performance data control
To indicate whether the logical partition can be used to view the processing unit activity data for all other logical partitions activated on the same CPC, select **Global performance data control**.

Input/output (I/O) configuration control

To indicate whether the logical partition can be used to read and write any Input/Output Configuration Data Set (IOCDS) in the configuration, select **Input/Output (I/O) configuration control**.

Selecting this option indicates the logical partition can also be used to change the input/output (I/O) configuration dynamically and controls whether or not a logical partition can enter config mode.

Additionally, this control allows the OSA Support Facility to control OSA configuration for other LPs and allows access to certain STP data.

Cross partition authority
To indicate whether the logical partition can be used to issue control program instructions that reset or deactivate other logical partitions, select **Cross partition authority**.

Logical partition isolation

To indicate whether reconfigurable channel paths assigned to the logical partition are reserved for its exclusive use, select **Logical partition isolation**.

When selected, channel paths are configured off; they will not become available to other logical partitions.

When not selected, reconfigurable channel paths assigned to this logical partition are not reserved for its exclusive use. Its channel paths can be configured off and reassigned to other logical partitions.

BCPii Permissions

Use this section to enable the Base Control Program internal interface (BCPii) permissions for the selected logical partition activated by the profile.

Enable the partition to send commands
To enable the selected partition to send BCPii commands, select **Enable the partition to send commands**. When selected, the active logical partition can send BCPii commands to other active logical partitions.

Enable the partition to receive commands from other partitions
To enable the selected partition to receive BCPii commands from other partitions, select **Enable the partition to receive commands from other partitions**. When selected, the active logical partition can receive BCPii commands from other active logical partitions.

All partitions
Select this option if you want the selected logical partition to receive BCPii commands from all the active logical partitions.

“Add partition” on page 787 (Selected partitions)
Select this option if you want to remove or add selected logical partitions to receive BCPii commands from the logical partition.

Add
To add a system and logical partition to receive BCPii commands from the logical partition, click **Add**.

Remove
To remove a selected logical partition to receive BCPii commands from the logical partition, click **Remove**.

Counter Facility Security Options

Use this section to specify the counter facility security options for the logical partitions activated by the profile.

Basic counter set authorization control
To indicate whether authorization is allowed to use the basic counter set, select **Basic counter set authorization control**. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

Problem state counter set authorization control
To indicate whether authorization is allowed to use the problem-state counter set, select **Problem state counter set authorization control**. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

Crypto activity set authorization control
To indicate whether authorization is allowed to use the crypto-activity counter set, select **Crypto activity counter set authorization control**. The set can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

Extended counter set authorization control
To indicate whether authorization is allowed to use the extended counter set, select **Extended counter set authorization control**. The counters of this set are model dependent.

Coprocessor group counter sets authorization control
Indicates whether authorization is allowed to use the coprocessor-group counter sets. This set can be used to count the crypto activities of a coprocessor.

Note: This option is available on the Hardware Management Console Version 2.11.1 and earlier.

Sampling Facility Security Options

Use this section to specify the sampling facility security options for the logical partitions activated by the profile.

Basic sampling authorization control
To indicate whether authorization is allowed to use the basic-sampling function, select **Basic sampling authorization control**. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

Diagnostic sampling authorization control

Note: This option is available if the **Basic sampling authorization control** option has been selected. However, if this option is selected the **Basic sampling authorization control** option cannot be deselected.

To indicate whether authorization is allowed to use the diagnostic-sampling function, select **Diagnostic sampling authorization control**. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

CP Assist for Cryptographic Functions

Use this section to specify the CP Assist Cryptographic Functions (CPACF) for the logical partitions activated by the profile.

Note: The default setting is to permit.

Permit AES key import functions

To change the current Advanced Encryption Standard (AES) key import functions setting for CPACF when the logical partition is activated, select **Permit AES key import functions**.

Permit DEA key import functions
To change the current Data Encryption Algorithm (DEA) key import functions setting for CPACF when the logical partition is activated, select **Permit DEA import key functions**.

Permit ECC key import functions
To change the current Elliptical Curve Cryptography (ECC) key import functions setting for CPACF when the logical partition is activated, select **Permit ECC import key functions**.

Add partition

Use this window to specify the partitions from which the target partition can receive BCPii commands.

Enter system and partition manually
System: Enter the system name for the logical partition from which the target partition can receive BCPii commands.

Netid: Enter the Netid name for the selected system.

Partition: Enter the logical partition name from which the target partition can receive BCPii commands.

Select a system and partition
System: Select from the drop-down menu the system for the logical partition from which the target partition can receive BCPii commands.

Netid: The Netid displays for the selected system.

Partition: Select from the drop-down menu the active logical partition from which the target partition can receive BCPii commands.

Additional functions on this window include:

Add
To add a selected system and partitions, click **Add**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Storage

Use this window to set the amount of central storage and virtual flash memory assigned to the logical partition activated by the profile.

Central Storage

Use this section to customize information that determines the amount and starting position of central storage allocated to the logical partition.

Amount in:
Displays the amount of storage is that is installed in the selected partition. Use the down arrow to change the amount of storage in Gigabytes, Megabytes, or Terabytes.

Initial
Enter the amount of central storage to allocate to the logical partition upon activation.

Initial storage is allocated to a logical partition in a contiguous block of one Gigabyte (GB) units. The logical partition has exclusive use of its initial storage. That is, it is not shared with other active logical partitions.

You must allocate at least 1 GB of initial storage for all operating modes.

Reserved
Enter the amount of central storage that can be reconfigured dynamically to the logical partition after activation. This field is only active if the operating mode selected on the **General** image page is **General**, **LINUX only**, or **z/VM** mode. It is not available in coupling facility mode.

Reserved storage is allocated to a logical partition in a contiguous block of one Gigabyte (GB) units, and is contiguous to an located above its initial storage. But, unlike its initial storage, the logical partition does not have exclusive use of its reserved storage. The reserved storage provides the logical partition with an additional amount of storage to use only if it is not already being used by another active logical partition.

There is no minimum for reserved storage. Zero gigabytes (0 GB) is a valid amount of reserved storage.

Storage origin
Use these selections to indicate how the central storage origin is determined.

The central storage origin of a logical partition is the storage location from which its central storage allocation begins. The origin can be any location that provides sufficient, contiguous space for allocating the total central storage for the logical partition.

Determined by the system
To have the Central Processor Complex (CPC) determine the central storage origin, select **Determined by the system**.

The CPC allocates central storage, wherever sufficient, contiguous space is available.

Determined by the user
To have this profile set the central storage origin, select **Determined by the user**, then specify the origin in the **Origin** field.

Origin
If you select to have this profile set the central storage origin, enter the origin here. The origin is an offset, not an address. Enter the offset number from where available CPC central storage begins, to where you want logical partition central storage to begin.

When this profile is used to activate a logical partition, sufficient and contiguous space must be available from the origin for the amount of central storage specified. Logical partition activation fails if sufficient storage is not available from the origin, regardless of whether the origin is determined by the system or by the user through this profile.

Virtual Flash Memory

Use these selections to customize information that determines the amount and virtual flash memory storage allocated to the logical partition. The virtual memory increments in 16 GB amounts with a maximum of 6144 GB. This field is only active if the operating mode selected on the **General** image page is **General**, **LINUX only**, or **z/VM** mode. It is not available in coupling facility mode.

Initial
Use the number spinner to increment or decrement the initial amount of virtual flash memory for the selected partition in 16 GB increments.

Maximum
Use the number spinner to increment or decrement the maximum amount of virtual flash memory to a allow for the selected partition.

Options

Specify the image options for the processor values on this window:

Minimum and Maximum I/O priority values can be specified at a partition level. These minimum and maximum I/O priority values can both be set at partition activation time or dynamically (post partition activation).

Minimum I/O priority

The minimum value must be less than or equal to the maximum value entered. This value can range from 0 to the maximum I/O priority allowed for that processor.

The minimum default is a priority value of 0.

Maximum I/O priority

This maximum processor I/O priority is obtained from new System Information support.

The maximum default is a priority value of 0.

Defined capacity
The measure of processor resource consumption for a logical partition, expressed in millions of service units (MSU) per hour.

CP management cluster name
The name specified for the CP management cluster.

zAware

Note: This tab is only applicable for z13, zEC12, and zBC12.

Use this window to customize zAware configuration settings for the selected zAware logical partition.The zAware configuration settings are:

Master user ID
Use this field to specify the master user ID for the selected zAware logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a master user ID name is numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Use this field to specify the master password for the master user ID you specified.

A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Use this field to specify again the same master password you specified in the **Master password** field.

Host name
Use this field to specify the host name for the selected zAware logical partition.

A host name can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a host name are alphanumeric characters, periods (.), colons (:), and hyphens (-).

Default gateway
Use this field to specify the default gateway IPv4 or IPv6 address.

You can find more detailed help on the following elements of this window:

Network Adapters

Use the Network Adapter table to view and change an IP address type and detail settings for the selected network adapters. You can add, edit, or remove the IP address type and detail settings using the **Select Action** list from the table tool bar. A maximum of 100 network adapters can be specified.

CHPID
Displays the CHPID for the selected zAware logical partition.

VLAN
Displays the VLAN for the selected zAware logical partition.

IP address
Displays the IPv4 or IPv6 address for the selected zAware logical partition. Also, indicates DHCP or Link Local if that is the specific IP address type.

Mask/Prefix
Displays the Mask/Prefix for the IPv4 or IPv6 address specified.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Add...
Select this operation to add a new IP address type and CHPID/VLAN details for the selected zAware logical partition.

Edit...
Select this operation to edit the selected IP address type and CHPID/VLAN details for the selected zAware logical partition.

Delete
Select this operation to delete the selected IP address type and CHPID/VLAN details for the selected zAware logical partition.

The icons perform the following functions in the Network Adapters table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

DNS Servers

The DNS Servers table displays the IPv4 or IPv6 address for the selected zAware logical partition. You can add, edit, or remove the IP address using the **Select Action** list from the table tool bar. A maximum of 2 DNS addresses can be specified.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.jkltoys.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all host names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

IP address
Displays the current IPv4 or IPv6 address for the selected zAware logical partition.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Add...
Select this operation to add a new IPv4 or IPv6 address to the selected zAware logical partition.

Edit...
Select this operation to edit the selected IPv4 or IPv6 address specified for the selected zAware logical partition.

Remove
Select this operation to remove the selected IPv4 or IPv6 address for the selected zAware logical partition.

The icons perform the following functions in the DNS Servers table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

SSC

Use this window to customize IBM Secure Service Container (Secure Service Container) configuration settings for the selected logical partition in Secure Service Container mode.

Note: Cryptographic (Crypto) options can be selected for Secure Service Container partitions.

The Secure Service Container configuration settings include the following:

Boot selection
Before a Secure Service Container partition is restarted for the first time, all fields of activation profiles can be updated or saved.

Secure Service Container installer
This option is selected until the Secure Service Container partition is restarted and the input fields contain information that was previously defined.

Secure Service Container
This option is selected after the Secure Service Container partition is restarted. The **Reset Logon Settings** and **Reset Network Settings** can be updated after the restart.

Reset Logon Settings
To reset the logon settings after the Secure Service Container partition is restarted, click **Reset Logon Settings**. Click **Yes** to proceed with resetting the master logon settings, then provide new information in the logon input fields.

Note: The input areas are pre-filled with the old settings.

Reset Network Settings
To reset the network settings after the Secure Service Container partition is restarted, click **Reset Network Settings**. Click **Yes** to proceed with resetting the master logon settings, then provide new information in the network input fields.

Note: The input areas are predefined with the old settings.

Master user ID
Use this field to specify the master user ID for the selected Secure Service Container logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or embedded blanks. Valid characters for a master user ID name are numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Use this field to specify the master password for the master user ID you specified.

A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Use this field to specify again the same master password you specified in the **Master password** field.

Host name
Use this field to specify the host name for the selected Secure Service Container logical partition.

A host name can be from one to 32 characters long. It cannot have special characters or embedded blanks. Valid characters for a host name are alphanumeric characters, periods (.), colons (:), and hyphens (-).

IPv4 gateway
Use this field to specify the default gateway IPv4 address.

IPv6 gateway
Use this field to specify the default gateway IPv6 address.

Network Adapters

Use the Network Adapter table to view and change an IP address type and detail settings for the selected network adapters. You can add, edit, or remove the IP address type and detail settings using the **Select Action** list from the table tool bar. A maximum of 100 network adapters can be specified.

CHPID
Displays the CHPID for the selected Secure Service Container logical partition.

VLAN
Displays the VLAN for the selected Secure Service Container logical partition.

Port
Displays the Port 0/1 parameter for the selected Secure Service Container logical partition.

IP address
Displays the IPv4 or IPv6 address for the selected Secure Service Container logical partition. Also, indicates DHCP or Link Local if that is the specific IP address type.

Mask/Prefix
Displays the Mask/Prefix for the IPv4 or IPv6 address specified.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Add...
Select this operation to add a new IP address type and CHPID/VLAN details for the selected Secure Service Container logical partition.

Edit...
Select this operation to edit the selected IP address type and CHPID/VLAN details for the selected Secure Service Container logical partition.

Delete
Select this operation to delete the selected IP address type and CHPID/VLAN details for the selected Secure Service Container logical partition.

The icons perform the following functions in the Network Adapters table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

DNS Servers

The DNS Servers table displays the IPv4 or IPv6 address for the selected Secure Service Container logical partition. You can add, edit, or remove the IP address using the **Select Action** list from the table tool bar. A maximum of 2 DNS addresses can be specified.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.jkltoys.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map

all host names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

IP address
Displays the current IPv4 or IPv6 address for the selected Secure Service Container logical partition.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Add...
Select this operation to add a new IPv4 or IPv6 address to the selected Secure Service Container logical partition.

Edit...
Select this operation to edit the selected IPv4 or IPv6 address specified for the selected Secure Service Container logical partition.

Remove
Select this operation to remove the selected IPv4 or IPv6 address for the selected logical partition.

The icons perform the following functions in the DNS Servers table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Add/Edit Network Adapters Entry

Use this window to add or edit the CHPID, VLAN, or Port for the selected secure service container logical partition. If the IP address selected is a static IPv4 or IPv6, you can edit or add the corresponding IP address.

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add/Edit DNS Entry

Use this window to add or edit the static IPv4 or IPv6 address configured for the selected secure service container logical partition.

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Load

Use this window to customize information that controls loading a control program for the logical partition activated by the profile.

Note: The image pages do not include this additional page if the operating mode selected on the **General** image page is coupling facility.

Load during activation

To indicate whether the load is performed during activation, select **Load during activation**.

If it has been selected it indicates a load is performed. The other information on the window is used to perform the load. Otherwise, a load is not performed.

Load type
Select the type of load to perform for the logical partition. Optionally, select the clear main storage on the logical partition before loading. You would use the SCSI or NVMe dump option to do a standalone dump to a SCSI device or NVMe adapter.

Standard load
To perform the load on the logical partition, click **Standard load**.

SCSI load
To IPL from a device that requires a SCSI load, click **SCSI load**.

SCSI dump
To IPL a standalone dump program from a device that requires a SCSI load, click **SCSI dump**.

NVMe load
To IPL from a device that requires a NVMe load, click **NVMe load**.

NVMe dump
To IPL a standalone dump program from a device that requires a NVMe load, click **NVMe dump**.

Enable Secure Boot for Linux
To verify the signature of the load program and distributor's signature match, select **Enable Secure Boot for Linux**.

Load address

Enter the address of the input/output (I/O) device that provides access to the control program to load. For a SCSI load, NVMe load, SCSI dump, or NVMe dump, this field has the device number of the device (for example, fibre channel adapter) that will be used to perform the SCSI load or NVMe load. This should contain four hexadecimal digits for NVMe load or five hexadecimal digits for SCSI load.

A load address is required.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device can store the control program or can be used to read the control program from a data storage medium.

Note: This field is applicable only when **Use dynamically changed address** check box is empty. Otherwise, if the check box displays a check mark, this field is unavailable.

Use dynamically changed address

To indicate whether the load address is dynamically determined by changes to the channel subsystem Input/Output definition (I/O), select **Use dynamically changed address**.

If this is selected, the load address is dynamically determined. Otherwise, this profile sets the load address. See the **Load address** field for the address set by this profile.

Specify the address in the **Load address** field.

Load parameter

Specify the optional information, if any, to use to further control how the control program is loaded during activation. Valid characters for a load parameter are:

- At (@)
- Pound (#)
- Dollar ($)
- Blank character
- Period (.)
- Decimal digits 0 through 9
- Capital letters A through Z .

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Note: This field is applicable only when **Use dynamically changed parameter** is **not** selected. Otherwise, this field is unavailable.

Use dynamically changed parameter

To indicate whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition, select **Use dynamically changed parameter**

If this is selected, the load parameter is dynamically determined. Otherwise, this profile sets the load parameter. Enter the parameter for this profile in the **Load parameter** field.

Time-out value

Specify the amount of time to allow for the completion of the load.

The time-out value can be from 60 to 600 seconds. If the load operation cannot be completed within the specified time, the operation is canceled.

This field is unavailable if a load type of **SCSI load** or **SCSI dump** is selected.

Worldwide port name

Specify the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI load or SCSI dump.

If the selected load type is **Standard load** or **NVMe load**, this field is unavailable.

Logical unit number

Specify the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

If the selected load type is **Standard load** or **NVMe load**, this field is unavailable.

Boot program selector

This field identifies the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30. This parameter provides the possibility of having up to 31 different boot configurations on a single disk device. This field should be set to 0 for optical media SCSI devices.

If the selected load type is **Standard load**, this field is unavailable.

Boot record logical block address

Specify the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is

assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

If the selected load type is **Standard load**, this field is unavailable.

Operating system specific load parameters

Specify a variable number of characters to be used by the program that is loaded. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

If the selected load type is **Standard load**, this field is unavailable.

Crypto

Use this window to customize information that controls how the logical partition activated by the profile uses the coprocessors and accelerators assigned to it. The settings are referred to here as *cryptographic controls*, and apply to the logical partition only if it is customized for using coprocessors and accelerators. This window allows you to:

- Add unassigned crypto(s) domain(s) to a logical partition for the first time.
- Edit assigned crypto(s) and domain(s) types to a logical partition already using cryptos and domains.
- Remove crypto(s) and domain(s) from a logical partition.

The assigned cryptographic domain index table displays the control domain and control and usage domain indexes which can be modified in the logical partition.

Control Domain

A logical partition's *control domains* are those cryptographic domains for which remote secure administration functions can be established and administered from this logical partition.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Control and Usage Domain

A logical partition's *control and usage domains* are domains in the cryptos that can be used for cryptographic functions. The usage domains cannot be removed if they are online.

A logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

The assigned cryptos index table displays the cryptographic candidate list and cryptographic online list settings which can be modified in the logical partition.

Cryptographic Candidate List

The candidate list identifies which cryptos will be assigned to the logical partition. Cryptos cannot be removed if they are online.

Cryptographic Online List (from profile)

The online list identifies which cryptos will be brought online at the next activation. Changes to the online list do not affect the running system. You must activate the partition to bring the coprocessor or accelerators online.

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Edit
Allows you to "Edit Domains" on page 798 or "Edit Cryptos" on page 799 for the selected activation profile.

Remove
Allows you to remove selected control and usage domain settings or selected crypto candidate and online settings for the selected activation profile.

Add
Allows you to "Add Domains" on page 799 or "Add Cryptos" on page 799 for unassigned domains or unassigned crypto candidates for the selected activation profile.

The icons perform the following functions in the Assigned domains or crypto tables:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

You can find more detailed help on the following elements of this window:

Edit Domains

Use this window to change the domain type for the assigned domains in this activation profile.

Select the domain type you want to change for this activation profile.

Control
Identifies the control domain you want to change the cryptographic functions for the logical partition.

Control and usage
Identifies the control and usage domains that you want to change the cryptographic functions for the logical partition.

Additional functions on this window include:

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Domains

Use this window to select the unassigned domains and domain type to add to this activation profile. You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Select the domain type for this activation profile.

Control
Identifies the control domain that can use the cryptographic functions for the logical partition.

Control and usage
Identifies the control and usage domains that can use the cryptographic functions for the logical partition.

Additional functions on this window include:

OK
To add the selected unassigned domains to this activation profile, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Cryptos

Use this window to change the crypto type for the assigned cryptos in this activation profile.

Select the crypto type you want to change for this activation profile.

Candidate
Identifies which cryptos will be assigned to the logical partition.

Candidate and online
Identifies which cryptos will be assigned and brought online at the next activations

Additional functions on this window include:

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Cryptos

Use this window to select the unassigned cryptos and crypto type to add for this activation profile. You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Select the crypto type for this activation profile.

Candidate
Identifies which cryptos will be assigned to the logical partition.

Candidate and online
Identifies which cryptos will be assigned and brought online at the next activations

Additional functions on this window include:

OK
To add the selected unassigned cryptos and crypto type for this activation profile, click **OK**.

Cancel

To exit the current window without saving changes, click **Cancel**.

Help

To display help for the current window, click **Help**.

Time Offset

If the Central Processor Complex (CPC) uses an External Time Source such as an Server Time Protocol (STP) as its time source, and you chose to set the logical partition's clock using an offset from the External Time Source's time of day, use this window to set the offset and to choose how you want it applied when the logical partition's clock is set.

Note: The image profile includes this window only if the clock type selected on the **General** page of the logical partition's image profile is **Logical partition time offset**.

Offset

Specify or select the number of days, hours, and minutes you want to set for the offset from the External Time Source's time of day. You can set an offset within the following range:

- 0 to 999 days
- 0 to 23 hours
- 0, 15, 30, or 45 minutes

days

Specify or select the number of days, from 0 to 999, that you want to set for the offset from the External Time Source's time of day.

hours

Specify or select the number of hours, from 0 to 23, that you want to set for the offset from the External Time Source's time of day.

minutes

Specify or select the number of minutes, 0, 15, 30, or 45, that you want to set for the offset from the External Time Source's time of day.

Decrease system time value by the amount shown

To set the logical partition's clock *back* from the External Time Source's time of day by the number of days, hours, and minutes in the offset, select **Decrease system time value by the amount shown**. Use this setting to provide a local time zone WEST of GMT.

Increase system time value by the amount shown

To set the logical partition's clock *ahead* of the External Time Source's time of day by the number of days, hours, and minutes in the offset, select **Increase system time value by the amount shown**. Use this setting to provide a local time zone EAST of GMT or a date and time in the future.

Group page

This window displays a group profile name, group description, group capacity, and absolute capping value that can be customized in determining the allocation and management of processor resources assigned to the logical partition in the group.

In the processor type table, the absolute capping can be None or a number of processors value from 0.01 to 255.0. To change an absolute capping for a processor type in the group profile, select the current absolute capping setting in its field, then use the Customize Group Profiles window to specify the absolute capping for the selected processor type to indicate the new setting.

Group name

Use this entry field to enter a group name for logical partition(s) in the group.

Specify the group name that you want to work with:

- To customize a group name, enter a new name in the field.
- To view or customize an existing group name, select the arrow beside the field to list the names of existing group names. Then select a group name from the list to display its information.

Requirements for group names: A group name is required to save the information.

Group description
Use this entry field to specify a brief note, up to 50 characters long, that describes the contents or purpose of the profile.

Note: A description is recommended, but optional.

Group capacity
Use this entry field to specify a group capacity for all profiles belonging to this group.

Note: If you add a new logical partition member to the group, a new group capacity value does not take affect if other logical partition members of the group are active. All logical partition members of the group must be deactivated first before the new group capacity value can take affect. You can use the **Change LPAR Group Controls** task to change the group capacity value to the running system immediately.

Customize Group Profiles
Use this window to specify the absolute capping for the selected processor type assigned in the group profile.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes you made and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Make a selection from the Profile Tree to view the group pages in the profile.

Customize Group Profiles

Use this window to specify the absolute capping for the selected processor type assigned in the group profile.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes you made and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Deactivate

Accessing the Deactivate task when targeting one or more CPCs or objects

Notes:

- This task is not available when one or more managed systems have DPM enabled.
- Deactivate is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task stops the operating system, deallocates resources, and clears associated hardware for all selected CPCs or CPC images. In addition, if a CPC or a CPC image that represents a non-LPAR system is selected, the deactivate task will perform a power off.

To start deactivation:

1. Select one or more CPCs or CPC images.
2. Open the **Deactivate** task. The Deactivate Task Confirmation window is displayed.

   Note: If one or more of the selected CPCs have associated secondary objects (for example, an image or coupling facility image), a Secondary Object Notification for Disruptive Task message window is displayed with a list of the active secondary objects. Review the list before proceeding. If you click **Yes** to proceed, the Deactivate Task Confirmation window is displayed. If you click **Yes** to proceed the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
3. Review the information on the window to verify that the object(s) you will deactivate is the correct one. If you want to continue this task, click **Yes**. If you want to end the task, click **No**. If you click **Yes**, the Deactivate Progress window is displayed.
4. The Deactivate Progress window is displayed indicating the progress of the deactivation and the outcome. Click **OK** to close the window when the deactivation completes successfully.

   Otherwise, if the deactivation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Delete Partition

Accessing the Delete Partition task

Use this task to delete one or more Dynamic Partition Manager (DPM) partitions.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

Before proceeding with this task, consider the following conditions:

- The partition cannot be part of an automatically started group, or part of an automatically started list.
- The partition cannot be part of a capacity group.
- The system must be active for the partition to be deleted.
- Only the partition can be stopped.

To delete one or more partitions:

1. Select one or more partitions that you want to delete.
2. Review the table that displays the partitions that you requested to delete.
3. Click **Delete** to proceed with this task. A progress bar displays as the partitions are deleted.
   a. If the task successfully deleted the requested partitions, a validation dialog is displayed. Click **Close** to complete the task.
   b. If the task did not successfully delete the requested partitions, review the table and the reasons why the partitions were not deleted.
4. Or, you can click **Cancel** to end this task without deleting any partitions.

Delete Partition

Use this task to delete one or more Dynamic Partition Manager (DPM) partitions. Before proceeding with this task, consider the following conditions:

- The partition cannot be part of an automatically started group, or part of an automatically started list.
- The partition cannot be part of a capacity group.
- The system must be active for the partition to be deleted.
- Only the partition can be stopped.

After you select one or more partitions to be deleted, review the table that displays the target partitions that are valid and those partitions that will be deleted. The table columns include the following information.

Partition
Specifies the name of the partition. It is a hyperlink that opens the Partition Details task.

Status
Specifies the current partition status.

Description
Specifies the user-defined description of the partition.

Additional functions for this window include the following items.

Delete
To continue with the removal of the partitions, click **Delete**. The Progress bar is displayed with no option to cancel.

If the deletion completes successfully, the validation window is displayed. Click **Close** when you are done viewing this message.

If the deletion cannot be completed successfully for all the partitions, then a new table is displayed.

Results
Specifies whether the partition was deleted.

Reason
Indicates why the partition was not deleted. If a reason is not identified, then the partition was deleted.

Click **Close** when you are done viewing this message.

Cancel
To exit this task without deleting any partitions, click **Cancel**.

Help
To display help for the current window, click **Help**.

Display Adapter ID

Accessing the Display Adapter ID task

Use this task to display the adapter ID, location, and fanout type assigned to the InfiniBand channels.

To display the InfiniBand adapter ID:

1. Open the **Display Adapter ID** task.
2. The Display Assigned Adapter ID window lists the InfiniBand cage-card slot, location, fanout type and assigned adapter ID.
3. Click **OK** to exit the window.

Disruptive Task Confirmation

Disruptive Task Confirmation

This window is used to inform you that a disruptive task is about to be performed on a targeted object. The window displays the objects that are affected by the task, along with information about what happens to each of these objects.

Note: If necessary, you might be required to provide confirmation text input for each object and you might also be required to provide your password. These additional requirements ensure that you want to perform the disruptive task.

Affect object list
This list displays the set of objects that are affected by the disruptive task. It is possible for this list to contain more objects than those selected by you as targets for the task. If this is the case, it means that performing the task also affects these additional objects due to some relationship between the set of targets chosen by you and these additional objects.

It is important for you to review the affect this task has on all the listed targets to make sure the execution of the task has the expected results.

The following information is provided in the table:

System Name
Specifies the name of the object that is being disrupted by the task that is being executing.

Type
Specifies the type of the profile of the affected object.

OS Name
Specifies the associated operating system name of the affected object.

Note: You can have an object that is operating but does not have an operating system installed on it. In this case, the **OS Name** is blank. The **OS Name** can also be blank for non-LPAR virtual servers.

Status
Specifies the status of the affected object.

Confirmation Text
Describes the results of proceeding with the task for the affected object.

Confirmation text input
Provide the operating system name (preferred, if available) or the system name as input to the **Confirmation Text** fields. You can type the name in the field or copy the name from the table and paste it into the input area, then click **Confirm** to continue.

When you have provided the correct information, the affected object list indicates that your entries have been confirmed in the **Confirmation Status** column.

Note: If your user ID does not require additional confirmation text to perform the disruptive task then this input field is not available.

Password confirmation input
Use this input field to specify your user ID password which allows you to perform the disruptive task.

Note: If your user ID does not require a password to perform the disruptive task then this input field is not available.

Performing a disruptive task can have severe affects, therefore, you are required to confirm the execution of the task by specifying your user ID password in this input field. Once you provide the correct password, **Yes** is enabled and you can proceed with the disruptive task.

Yes
To continue with the execution of the disruptive task, click **Yes**.

No
To exit this window without continuing the execution of the disruptive task, click **No**.

Confirm
To continue with the execution of the disruptive task after providing confirmation text for each object, click **Confirm**.

Cancel
To exit this window without providing confirmation text or continuing the execution of the disruptive task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Domain Security

Accessing the Domain Security task

This task provides a method for you to maintain the security of a processor complex by controlling the access of the Hardware Management Consoles to the system Support Elements. Hardware Management Consoles can only communicate with system Support Elements that have the same domain name and domain password as the Hardware Management Console. Assigning a unique domain name and password to a Hardware Management Console and the systems that are defined to it will isolate those systems from any other Hardware Management Console connected to the same Local Area Network (LAN).

To define the domain security:

1. Open the **Domain Security** task. The Domain Security window is displayed.
2. Specify a domain name and domain password. Select the option with which you want the domain to apply.
3. Click **OK** to proceed with the change.

Domain Security

Use this window to change the name or password of the domain of this Hardware Management Console, and also to indicate whether to change them for the defined objects in the current domain.

The “Current domain name” on page 806 is displayed on the window. If **NOT SET** is displayed, it indicates that default domain security is in effect for this console.

The “Current password status” on page 806 indicator is displayed on the window. The password itself is not displayed. If **SET** is displayed, it indicates that the password has been set for this console. If **NOT SET** is displayed, it indicates that the password has not been set for this console.

Important: See Important domain security information about using this task correctly, and about the consequences of applying a customized domain name or password to this console or its defined objects.

Default domain security is the type of domain security that is initially set for new Hardware Management Consoles and for new, undefined objects.

The intent of default domain security is to allow connecting Hardware Management Consoles and objects to a Local Area Network (LAN) that might attach other systems and devices, yet provide secure communications between the consoles and the objects that prevents other systems and devices on the same LAN from being used to control the objects.

Default domain security provides complete domain security for a Parallel Sysplex® while only one Hardware Management Console is attached to the LAN. Only that console can be used to control the objects in the sysplex. If more than one Hardware Management Console is attached to the same LAN, either as alternate consoles for the same sysplex, or as primary or alternate consoles for other sysplexes, default domain security still provides communication with their objects that is secure from other systems and devices on the LAN. However, under default domain security, any Hardware Management Console on a LAN can communicate with any object in any sysplex on the same LAN. You must establish customized

domain security to provide communication between particular consoles and objects that is secure from other consoles on the LAN.

Customized domain security is a type of domain security you can set for a Hardware Management Console and its defined objects. The intent of customized domain security is the same as that of default domain security, but with an extra level of security.

Like default domain security, it allows connecting a Hardware Management Console and its objects to a LAN that might attach other systems and devices. It also provides secure communications between the console and its objects that prevents other systems and devices on the same LAN from being used to control the objects. Unlike default domain security, it provides secure communications between the console and its defined objects that prevents other Hardware Management Consoles on the same LAN from being used to control its objects.

Customized domain security can provide complete domain security within a parallel sysplex while one or more Hardware Management Consoles are attached to the same LAN as alternate consoles for the sysplex and while one or more Hardware Management Consoles are attached to the same LAN as primary and alternate consoles for other sysplexes.

Current domain name

Displays the name that is currently assigned to the domain of the console.

The domain of the Hardware Management Console is the set of objects the console can be used to manage. The current domain of this console includes all the objects currently under **Systems Management**.

This current domain name displays one of the following:

NOT SET
Indicates that default domain security currently is in effect for the console.

Any other *name*
Indicates that customized domain security currently is in effect for the console. The current name of the domain is *name*.

Domain Name

Use this field to specify a new name for the domain of this Hardware Management Console.

The domain of a Hardware Management Console is the set of objects the console can be used to manage. The current domain of this console includes all the objects currently under **Systems Management**.

The domain name and password of the console authorize its communication with the objects in its domain. They prevent unauthorized sources that are attached to the same LAN from communicating with the objects.

Requirements for a domain name
A new domain name is optional. But to change domain security, you must change either the domain name or password, or both. To keep the current domain name and change only the domain password, leave this field blank.

A domain name can be from 1 to 8 characters long. It cannot have special characters or embedded blanks. Valid characters for a domain name are numbers **0** through **9** and alphabetic letters **A** through **Z**.

Note: Domain names are not case-sensitive. All alphabetic characters are saved in uppercase.

Current password status

Indicates whether the password is set for the domain of the console. The password itself is not displayed.

This current password status displays one of the following:

SET
Indicates that the password has been set for the domain of the console.

NOT SET
Indicates that the password has not been set for the domain of the console.

New password

Use this field to specify the new password to the domain of this console.

Note: The password is not displayed as you specify it; asterisks display instead.

The domain name and password of the console authorize its communication with the objects in its domain. They prevent unauthorized sources that are attached to the same LAN from communicating with the objects.

Requirements for a domain password of eight or fewer characters
A new domain password is optional. But to change domain security, you must change either the domain name or password, or both. To keep the current domain password and change only the domain name, leave this field blank.

A password can be 6 - 8 characters long. It cannot have special characters or embedded blanks. Valid characters for a password are numbers **0** through **9** and alphabetic letters **A** through **Z**.

Note: Passwords are not case-sensitive. All alphabetic characters are saved in uppercase.

The first and last character of a password must be a letter.

A password must include at least one number, but it cannot be the first or last character in the password.

A password cannot include a sequence of 3 characters that are the same.

Requirements for a domain password of nine or more characters
A domain that uses this longer password format cannot include Version 2.13.1 and prior HMC consoles or defined objects.

A new domain password is optional. But to change domain security, you must change either the domain name or password, or both. To keep the current domain password and change only the domain name, leave this field blank.

A password can be from nine to 64 characters long. It can have special characters that include:

` ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ' " , . < > / ?

It cannot have embedded blanks. In addition to the special characters listed, valid characters for a password are numbers **0** through **9** and uppercase and lowercase alphabetic letters **A** through **Z**.

Note: Passwords are case-sensitive.

Verify password

Use this field to specify again the same password you specified in the **New password** field.

Note: The password is not displayed as you specify it; asterisks display instead.

Important: You do not need to write down or remember the domain password. After it is applied, it is used only for internal communication between this console and the objects in its domain. You are required to know the password to perform any other tasks at this console. If you need to assign the same password to other consoles you want in the same domain, it is recommended you do so promptly.

Apply to the Hardware Management Console

To assign the domain name and password to this console only, select **Apply to the Hardware Management Console**.

Note: Changing the name and password for the domain of only this console removes it from the current domain of its defined and undefined objects. This might strand the objects outside the domain of any console, effectively isolating them from your control. For more information about stranding objects, and how to avoid it, see Important domain security information.

Apply to defined objects and the Hardware Management Console

To assign the domain name and password to this console and all objects that are currently defined under **Systems Management**, select **Apply to defined objects and the Hardware Management Console**.

Note: If you attempt to apply a domain password of 9 or more characters to a Version 2.13.1 or prior defined object, it results in an error message. In this case, the new domain information is not applied to the HMC or to any of its defined objects.

The length of time this task takes depends on the number of defined objects and whether a problem exists. If a problem exists, these changes are not applied to any of the defined objects or the Hardware Management Console (HMC). Avoid ending this task or restarting the application or console so that all the defined objects and the Hardware Management Console can be processed together.

Note: Changing the name and password for the domain of this console and its defined objects remove the console from the current domain of its undefined objects. This might strand the objects outside the domain of any console, effectively isolating them from your control. For more information about stranding objects, and how to avoid it, see Important domain security information.

Reset to manufacturing default domain name and password

The manufacturing default domain is the type of domain security that is initially set for new consoles and for new, undefined objects. To reset the domain name and password to the default domain name and password, select **Reset to manufacturing default domain name and password**.

Note: This option appears if you are using the SERVICE default user ID or a user ID that is assigned Service Representative roles.

Additional options on this window are available:

OK
To assign the new domain name and password to the selected objects you want to include in the new domain or to reset the domain name and password to the default, click **OK**.

Cancel
To close the window without changing the current settings for domain security, click **Cancel**.

Help
To display help for the current window, click **Help**.

Important domain security information

Consequences of customizing domain security

- Changing the domain of a Hardware Management Console will remove it from its current domain, regardless of whether its current domain still includes objects. This may strand the objects outside the domain of any console, effectively isolating them from your control. For more information about stranding objects, and how to avoid it, see **Stranding objects**.
- Applying a customized domain name or password to consoles or defined objects currently in the default domain removes them from the default domain. Afterwards, you must contact the support system for assistance if you want to move consoles or objects from a customized domain back into the default domain.

When to use this task

It is recommended you **not** change the domain of this Hardware Management Console when it is the only console serving a single Parallel Sysplex. Domain security is already provided for this configuration by default domain security.

Use this task only when you want customized domain security. Customize domains to establish and maintain different domains for **multiple** Hardware Management Consoles attached to the same LAN. Multiple consoles can be on the same LAN for two reasons:

- For a single sysplex served by a primary console and one or more alternate consoles.
- For multiple sysplexes attached to the same LAN, with each sysplex served by a primary console and any number of alternate consoles.

Stranding objects

Stranding objects is a potential pitfall of establishing customized domain security.

Stranded objects are objects in a domain that does not include any Hardware Management Consoles. Consoles cannot communicate with a stranded object, so the object can never be defined to a console. And not being able to define an object isolates it from all other console tasks.

How objects become stranded

There are two ways objects can become stranded:

1. Undefined objects in a domain with only one Hardware Management Console **and** a new name or password is applied to the domain of the console and its defined objects.
2. All objects are in a domain with only one Hardware Management Console **and** a new name or password is applied to the domain of the console only.

   Note: It does not matter whether the objects are defined or undefined at the time.

How to avoid stranding objects

To avoid stranding objects, never assign a new name or password to the domain of a console and its defined objects when it is the only console in the domain and there are undefined objects in the domain. Before assigning a new name or password to the domain of a console and its defined objects, either define all undefined objects, or make sure at least one other console will remain in the current domain with the undefined objects.

Never assign a new name or password to the domain of a console only when it is the only console in the domain of its defined and undefined objects. Before assigning a new name or password to the domain of a console only, make sure all defined objects and undefined objects are in the domain of at least one other console. Make sure at least one other console will remain in the current domain with the defined and undefined objects.

How to recover stranded objects

If you know the domain name and password of the stranded objects, then simply assign the same name and password to any available Hardware Management Console. This moves the console into the domain of the stranded objects.

If you do not know the domain name or password of the stranded objects, then you must report the problem to the support system.

Dump

Accessing the Dump task

Use this task to dump the memory attached to a partition that resides on a Dynamic Partition Manager (DPM)-enabled system. To use this task, you need to set up a dump program on a storage volume. The dump program must be a stand-alone dump tool for the operating system that the partition hosts; for example, the DASD dump tool for Linux.

Note: This task is available only when one or more managed systems have DPM enabled.

You can access this task from the main console page by selecting **Dump** in the Tasks index, or by completing the following steps.

1. Expand the **Systems Management** node.
2. Select the **Partitions** tab.
3. Select a partition that resides on a DPM-enabled system. The partition must have one of the following status values: Active, Degraded, Terminated, or Paused.
4. Open the task by selecting **Dump** either from the context menu next to the partition name, or from the Recovery task group. The Dump window opens.
5. When you are ready to close the task, click **X** on the Dump tab.

Dump

Use this task to dump the memory attached to a partition that resides on a Dynamic Partition Manager (DPM)-enabled system. To use this task, you need to set up a dump program on a storage volume and, if you are not using default dump parameters, you need to know which parameters to specify for the dump program. You also need to identify the volume on which the dump program resides. The dump program must be a stand-alone dump tool for the operating system that the partition hosts; for example, the DASD dump tool for Linux.

Before you begin

- Set up the stand-alone dump program on a bootable storage volume that is large enough for the dump program plus the maximum amount of memory that is allocated to the partition. To determine the required volume capacity, go to the Memory section of the **Partition Details** task, and add 10 MB to the maximum value shown in the Installed Memory bar chart.
- Go to the Storage section of the **Partition Details** task and assign the volume containing the dump program to the partition. How you assign that volume depends on the version of DPM that is applied on the system.
  - When the system has the DPM R3.1 storage management feature or a later DPM version applied, attach the storage group that contains the boot volume. The storage group can be one of the following types:
    - FCP (Fibre Channel Protocol)
    - FICON (Fibre Connection)
    - NVMe (Non-Volatile Memory Express)
  - When the system has DPM R3.0 or an earlier version applied, define a host bus adapter (HBA) to access the storage device on which the stand-alone dump program resides.
- Make sure you can identify the volume that contains the dump program.
  - If you assigned the volume through a storage group, you need to know the universally unique ID (UUID) if the volume is an FCP volume, or the volume ID if the volume is a FICON volume, or the volume serial number of the NVMe solid state drive (SSD). The ID or volume serial number is shown in the **Dump** task display when you select and expand a storage group.

– If you assigned the volume through an HBA, you need to know the 64-bit worldwide port number (WWPN) of the storage subsystem, and the 64-bit hexadecimal logical unit number (LUN) of the volume that contains the dump program.

Procedure

1. On the **Partitions** tab of the System Management view, select a partition that resides on a DPM-enabled system. The partition must have one of the following status values: Active, Degraded, Terminated, or Paused.
2. Open the task by selecting **Dump** either from the context menu next to the partition name, or from the Recovery task group. The Dump window opens.

   The Dump window displays a Boot Device table or a Storage Group table, depending on the version of DPM that is applied on the system. Follow the instructions that correspond to the type of table displayed on the page.

   Boot Device table

   a. From the boot device table, select the host bus adapter (HBA) that is used for the dump program boot. By default, the initially selected row defines the HBA that is used for the dump program boot.

   b. Provide the Target WWPN and the Target LUN.

   Target WWPN
   This required field is a 16-digit hex string (64-bit binary number) which identifies the Fibre Channel port of the target SCSI disk.

   Target LUN
   This required field defines the 64-bit boot target logical unit address. It is a 16-digit hex string that designates the unit number of the target SCSI disk.

   c. Optionally provide additional dump program parameters.

   Boot program selector (0-30)
   This optional field can have a value in the range 0 - 30, with the default value of 0. The parameter specifies the dump configuration number that is to be booted; the number corresponds to the menu of IPL/dump entries in the zipl configuration file.

   Boot record logical block address
   This optional field defines the 64-bit load block address. It is a 16-digit hexadecimal string. If a value is not defined, it is defaulted to an empty string for display (even if its defaulted model value is 0).

   Dump program parameters
   This optional field defines the parameters of the dump program that you are using. Its value is a string. If a value is not defined, it is defaulted to an empty string.

   Use this field to overwrite or add to (concatenate) existing dump parameters that have been configured, such as the dump mode setting. For example: `dump_dir=/mydumps dump_compress=gzip`

   Storage Group table

   a. In the Storage Group table, select a storage group. If only one storage group is available, DPM automatically selects it. The table entry expands to show the volumes that are attached to the selected storage group. If a selected FCP or FICON storage group is in Pending state, some volume UUIDs or volume IDs might not be available.

   b. Select the boot volume on which the dump program resides.

   - If only one boot volume is available, DPM automatically selects it. Otherwise, check the Type column to look for boot volumes. If no boot volumes are shown, you need to go to **Partition Details** and select a storage group that has a boot volume containing the stand-alone dump program.

- For each boot volume, check the Capacity column to determine whether the volume is large enough to contain the amount of partition memory to be dumped. If you have selected a FICON storage group, the volume must be at least 1 gibibyte (GiB) in size.
- When you select an NVMe volume, note that NVMe namespace management is not supported, so you can boot programs only from namespace ID=1.

c. Optionally provide additional dump program parameters in the Volume Settings section. The fields in this section vary, depending on the type of storage group that you selected.

Boot program selector (0-30)
This optional field can have a value in the range 0 - 30, with the default value of 0. The parameter specifies the dump configuration number that is to be booted; the number corresponds to the menu of IPL/dump entries in the zipl configuration file. This field is displayed only when you select an FCP or NVMe volume.

Boot record logical block address
This optional field defines the 64-bit load block address. It is a 16-digit hexadecimal string. If a value is not defined, it is defaulted to an empty string for display (even if its defaulted model value is 0). This field is displayed only when you select an FCP or NVMe volume.

IPL load parameter
This optional field can contain initial program load (IPL) parameters to be passed to the dump program. You can specify a maximum of eight alphanumeric characters.

OS load parameter
This optional field can contain operating system-specific parameters to be passed to the hypervisor or operating system while the dump program is booting. You can specify a maximum of 256 alphanumeric characters. This field is displayed only when you select an FCP or NVMe volume.

Time-out value
This optional field specifies a time-out value for the boot process. By default, the value is the minimum value of 60 seconds. The maximum time-out value is 600 seconds.

3. To proceed with the task, select **OK**. Otherwise, select **Cancel** to end the task.

Edit Frame Layout

Accessing the Edit Frame Layout task

This task provides a graphic view of the physical location of the hardware objects that are defined to this Hardware Management Console. Each object is shown with its frame designation and position within the frame. By opening (double-clicking on) the object, additional information is provided:

- Machine type
- Model
- Serial number
- Device location

This task also shows the locations in the frames that are available for adding or moving a device. In addition to adding or moving devices, the service representative can also remove devices or add frames.

To add, remove, or move hardware objects that are defined to the Hardware Management Console:

1. Select an object.
2. Open the **Edit Frame Layout** task. The Edit Frame Layout window is displayed.

   Note: If you select more than one object, the Object Selection window is displayed prompting you to select a single CPC on which to perform the task.
3. Click **Save** when you have completed the task and want to save your changes.

Edit Frame Layout

This window displays graphically the current hardware configuration information for a machine.

Use this window after changing the actual hardware configuration of a machine to update its hardware configuration information.

Changing configuration information

Use the menus from the window to change the hardware configuration information for the frame, device, or open area you changed in the actual hardware configuration.

For step-by-step instructions about changing configuration information, select the change you made to the actual hardware configuration from the following:

- Installed a new device
- Installed a new frame
- Moved a device
- Removed a device
- Removed a frame

Frame and device graphics

Frame and device graphics indicate the layout of frames, and the location and size of devices, as described by the current hardware configuration information for the machine.

Use the mouse to select graphics and to display the menus of actions you can use on the selected graphic.

Frame
Represents an actual frame and its location in the machine.

Using the left mouse button, click any open area in the frame to display a menu of frame actions.

Device
Represents an actual device, and its size and location in a frame.

Using the left mouse button, click on a device to display a menu of device actions.

Using the left mouse button, double-click on a device to display the current, detailed hardware configuration information for the device.

Open area
Represents the size and location of empty space in a frame.

Using the left mouse button, click on an empty space to display a menu of frame actions.

Additional functions on this window include:

Machine Type
Displays the machine type of the machine.

Machine Model
Displays the model number of the machine.

Serial Number
Displays the serial number of the machine.

Save and Exit
To save the hardware configuration information represented by the frame layout currently displayed, to close the window, and to end this task, click **Save and Exit**.

Hardware configuration information for each Central Processor Complex (CPC) is stored on its Support Element.

Hardware configuration information for each device is stored on the support element of the CPC associated with the device.

Add Frame...
To add a frame to the hardware configuration, click **Add Frame...**.

Cancel
To close the window without saving changes you made to the frame layout, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installed a new device

Follow this procedure to add information about a new device you installed.

On the **Edit Frame Layout** window:

1. Using the left mouse button, click on the open area of the frame where you installed the device.

   The selected open area flashes, and the frame actions menu is displayed.
2. Verify whether the flashing open area includes the location where you installed the new device, then:

   a. If the flashing open area includes the new device location, continue to the next step.

   b. Otherwise, select **Deselect open area**, then start again with step 1.
3. Select **Add device** from the menu.

   The first of two **Add device** windows is displayed.
4. Use the windows to provide information about the exact location of the device you added, and its specific product information.

   Request help for the windows for additional information about using them to complete this step and to add the device to the frame layout.

   The **Edit Frame Layout** window is displayed again. The updated frame layout is displayed the device you added to the selected open area.
5. Click **Save and Exit** on the **Edit Frame Layout** window to save the new device information with the hardware configuration information for the machine.

Installed a new frame

Follow this procedure to add information about a new frame you installed.

On the **Edit Frame Layout** window:

1. Click **Add Frame...**.

   The **Add Frame** window is displayed.
2. Use the window to specify the frame label.

   Request help for the window for additional information about using it to complete this step and to add the frame to the frame layout.

   The **Edit Frame Layout** window is displayed again. The updated frame layout displays the frame you added to the machine.
3. Select **Save and Exit** on the **Edit Frame Layout** window to save the new frame information with the hardware configuration information for the machine.

Moved a device

Follow this procedure to change information about the location of a device you moved.

On the **Edit Frame Layout** window:

1. Using the left mouse button, click on the device you moved.

The selected device flashes, and the device actions menu is displayed.

2. Select **Move device** from the menu.

   The first of two **Move device** windows is displayed.

3. Use the windows to specify which frame you moved the device to, and the exact location of the device in that frame.

   Request help for the windows for additional information about using them to complete this step and to move the device within the frame layout.

   The **Edit Frame Layout** window is displayed again. The updated frame layout displays the device in its new location.

4. Select **Save and Exit** on the **Edit Frame Layout** window to save the new device location with the hardware configuration information for the machine.

Removed a device

Follow this procedure to delete information about a device you removed.

On the **Edit Frame Layout** window:

1. Using the left mouse button, click on the device you removed.

   The selected device flashes, and the device actions menu is displayed.

2. Select **Delete device** from the menu.

   A message is displayed to identify the device you selected to delete.

3. Use the message to confirm your request to delete the selected device.

   The **Edit Frame Layout** window is displayed again. The updated frame layout no longer is displayed the device you removed.

4. Select **Save and Exit** on the **Edit Frame Layout** window to delete the device information from the hardware configuration information for the machine.

Removed a frame

Follow this procedure to delete information about a frame you removed.

On the **Edit Frame Layout** window:

1. A frame must be empty before you can delete it. Delete all devices in the frame.

   Note: Delete a device after you removed the device from the actual frame.

2. Using the left mouse button, click on the open area of the empty frame you removed.

   The selected open area flashes, and the frame actions menu is displayed.

3. Select **Delete empty frame** from the menu.

   A message is displayed to identify the frame you selected to delete.

4. Use the message to confirm your request to delete the selected frame.

   The **Edit Frame Layout** window is displayed again. The updated frame layout no longer displays the frame you removed.

5. Select **Save and Exit** on the **Edit Frame Layout** window to delete the frame information from the hardware configuration information for the machine.

Device actions

Use this menu to select an action for working with the selected device.

A device flashes to indicate it is currently selected.

Menu choices

Move device
To change the location of the selected device, select this menu choice.

Change the location of a device in the frame layout only after you moved the device within the actual machine.

Delete device
To delete the selected device from the frame layout, select this menu choice.

Delete a device from the frame layout only after you removed the device from the actual frame.

Device details
To display the current, detailed hardware configuration information for the selected device, select this menu choice.

Note: Double-click the left mouse button on a device for another way to display its hardware configuration information.

Deselect device
To close the device actions menu and deselect the selected device, select this menu choice.

Add Fibre Trunk
To add a Fibre Trunk to the machine, select this menu choice.

Update Fibre Trunk
To change the location or serial number of a Fibre Trunk, or to view the Fibre Trunks in the system, select this menu choice.

Delete Fibre Trunk
To delete a Fibre Trunk and deselect the selected device, select this menu choice.

Frame actions

Use this menu to select an action for working with either:

- The selected empty frame
- The selected open area in a frame

An open area flashes to indicate it is currently selected.

Menu choices

Add device
To add a device to the selected open area of a frame, select this menu choice.

Add a device to the frame layout only after you installed a new device in the actual frame.

Delete empty frame
To delete a frame from the frame layout, select this menu choice.

Note: This choice is available only when the frame is empty.

Delete a frame from the frame layout only after you removed the frame from the actual machine.

Deselect open area
To close the frame actions menu and deselect the selected open area, select this menu choice.

Add Fibre Trunk
To add a Fibre Trunk to the machine, select this menu choice.

Update Fibre Trunk
To change the location or serial number of a Fibre Trunk, or to view the Fibre Trunks in the system, select this menu choice.

Delete Fibre Trunk
To delete a Fibre Trunk and deselect the selected device, select this menu choice.

Device actions

Use this menu to select an action for working with the selected device.

A device flashes to indicate it is currently selected.

Menu choices

Move device
To change the location of the selected device, select this menu choice.

Change the location of a device in the frame layout only after you moved the device within the actual machine.

Delete device
To delete the selected device from the frame layout, select this menu choice.

Delete a device from the frame layout only after you removed the device from the actual frame.

Device details
To display the current, detailed hardware configuration information for the selected device, select this menu choice.

Note: Double-click the left mouse button on a device for another way to display its hardware configuration information.

Deselect device
To close the device actions menu and deselect the selected device, select this menu choice.

Add Fibre Trunk
To add a Fibre Trunk to the machine, select this menu choice.

Update Fibre Trunk
To change the location or serial number of a Fibre Trunk, or to view the Fibre Trunks in the system, select this menu choice.

Delete Fibre Trunk
To delete a Fibre Trunk and deselect the selected device, select this menu choice.

Add Frame

Use this window to specify the label and the type of the frame added to the hardware configuration of the machine you are working with.

Select the frame label and frame type from those displayed, and enter the serial number of the frame, then click **Add Frame**.

Frame label
To choose the label of the frame added to the hardware configuration of the machine, use the down arrow to select a **Frame label**.

Frame Types
Select a frame type from the list provided.

Serial number

Specify the serial number assigned to the frame.

Add Frame
To add the specified frame to the frame layout of the machine, click **Add Frame**.

Add a frame to the frame layout only after you installed a new frame in the actual machine.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the frame information with the hardware configuration information for the machine.

Cancel
To close the window and not add a frame, click **Cancel**.

Help
To display help for the current window, click **Help**.

Frame Details

Use this window to verify the detailed hardware configuration information for a selected frame. This window also provides the ability to change the detailed hardware configuration information.

Frame label
Displays the name or identity of the frame.

Description
Displays the description of the frame.

Serial number
Displays the serial number of the frame.

Change Frame Details...
To change the frame details from the information that is displayed, click **Change Frame Details...**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Frame Details

Use this window to verify or change the detailed hardware configuration information for a selected frame.

Frame label
Displays the name or identity of the frame.

Description
Displays the current description of the frame.

Description (new)
Specify the new description of the frame.

Serial number
Displays the current serial number of the frame.

Serial number (new)
Specify the new serial number of the frame.

Save
To change the frame details to the information you entered, click **Save**.

Cancel
To close the window without changing the frame details, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Cage

Use this window to define a cage in your hardware configuration layout. Select a cage from the table, then click **Add Cage**.

Cage table
Use this window to define a cage in your configuration layout. This table lists the available cages by description and device UPC card serial number.

Select one, then click **Add Cage...** to define that cage in your configuration layout.

Add Cage...
To define the selected cage in your hardware configuration, click **Add Cage...**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Cage

Use this window to add a cage to the hardware configuration. Select the location of the cage, then click **Add Cage**.

Cage Addresses
This table displays the addresses of the cages available to add to the hardware configuration. Select a cage to add to the hardware configuration and specify the serial number of the device, then click **Add Cage**.

Serial number
Specify the serial number of the device.

Add Cage
To add the selected cage to the hardware configuration, click **Add Cage**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Device

Use this window to select the device added to the hardware configuration of the machine you are working with.

Select the device you added, then click **Add Device...**.

Device table
This table displays a list of devices that were recently added to your hardware configuration by description, device serial number, and associated CPC name and location.

Select a device, then click **Add Device...**.

Add Device...
To add the selected device to the fame layout of the machine, click **Add Device...**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Device

Use this window to select the device added to the hardware configuration of the machine you are working with.

Select from the list the device you added, then click **Add Device...**. Another window is displayed for you to provide specific hardware configuration information about the device.

Machine type
Displays the machine type of the machine you added a device to.

Machine model
Displays the model number of the machine you added a device to.

Devices
Displays the name, or type, and description of devices that can be added to the machine.

Add Device...
To add the selected device to the frame layout of the machine, click **Add Device...**.

Cancel
To close the window and not add the device to the frame layout, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Device

Use this window to provide product and location information about a device added to the hardware configuration.

Device
Displays the name, or type, and description of the device added to the machine.

Serial number
Specify the serial number of the device.

Frame
Displays the label of the frame you added the device to.

Exact location
Select the location of the device. Device locations are identified by four characters.

The first character of a device location identifies the frame label.

The next two characters identify the vertical location of the device, relative to the bottom of the frame. Vertical locations are identified by two digits, decimal numbers from bottom to top, beginning with the number 01.

The last character identifies the horizontal location of the device, relative to the left side of the front of the frame. Horizontal locations are identified by letters from left to right, beginning with the letter A.

Associated CPC
Select the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the support elements of its CPCs. A support element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the support element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

Add Device
To add the device to the frame layout for the machine, click **Add Device**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the device information with the hardware configuration information for the machine.

Cancel
To close the window and not add the device to the frame layout, click **Cancel**.

Help
To display help for the current window, click **Help**.

Device Details

Use this window to view device details. Detailed hardware configuration information for a selected device is displayed.

To change the device details, specify the device serial number and select the associated CPC, then click **Change Device Details**.

Device
Displays the name or type of the device.

Description
Displays a brief description of the device.

Location
Identifies the location of the device.

Serial number
Displays the serial number of the device. You can also specify another serial number.

Associated CPC
Displays the name and location of the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the support elements of its CPCs. A support element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the support element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

Associated devices

This table displays the name and location of devices associated with the Central Processor Complex (CPC).

Change Device Details
To change the device details to the device information currently displayed, click **Change device details**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Hardware configuration information for each Central Processor Complex (CPC) is stored on its support element.

Hardware configuration information for each device is stored on the support element of the CPC associated with the device.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Move Device

Use this window to specify a label of the frame where you installed a device removed from another location in the machine.

Use the drop downs choices to select the frame information, then select **Move Device**.

Device
Displays the name or type of the device you moved.

Description
Displays a brief description of the device you moved.

Previous location
Displays the location of the device currently stored in the hardware configuration information.

Frame
From the drop down choices, select the label of the frame where you reinstalled the device you moved.

Exact location
Select the location in the frame, in the lower, left-hand corner, where you reinstalled the device you moved.

Device locations are identified by four characters.

The first character of a device location identifies the frame label.

The next two characters identify the vertical location of the device, relative to the bottom of the frame. Vertical locations are identified by two digits, decimal numbers from bottom to top, beginning with the number 01.

The last character identifies the horizontal location of the device, relative to the left side of the front of the frame. Horizontal locations are identified by letters from left to right, beginning with the letter A.

Move device
To delete the device from its current frame in the frame layout, and to add it to its new frame, select **Move device**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Cancel
To close the window and not change the location of the device, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Support Element

Use this window to add a Support Element to the hardware configuration. Select a support element and the location of the Support Element as you want it identified in the hardware configuration, then click **Add Support Element**.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Support Elements
Select a Support Element from this table, then select the location as you want it identified in the hardware configuration.

Available support element locations
Select a Support Element, then select from this table the location as you want it identified in the hardware configuration.

Serial number
Specify the serial number of the machine.

Add Support Element
To add the selected Support Element to your hardware configuration, click **Add Support Element**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Support Element Details

Use this window to confirm the Support Elements listed by description, serial number, and location and associated with a specific CPC.

To confirm the support elements, click **OK**.

Support Element(s) table
This table displays the current Support Elements by description, serial number, and location.

Associated CPC
This is the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the Support Elements of its CPCs. A Support Element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

OK
To confirm the Support Elements listed with the associated CPC, click **OK**.

Help
To display help for the current window, click **Help**.

Update Support Element

Use this window to select a Support Element you want updated in the hardware configuration of the specified machine, then click **Update Support Element...**.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Associated CPC
Displays the central processor complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the Support Elements of its CPCs. A Support Element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

Current Support Element(s) table
This table displays current Support Elements by description, serial number, and location.

Select the Support Element you want updated in the hardware configuration of the specified machine, then click **Update Support Element...**.

Update Support Element...
To update the Support Element you selected, click **Update Support Element...**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update Support Element

Use this window to select a Support Element type you want to change in the hardware configuration of the specified machine, then select **Update Support Element**.

Note: Updates to this window will overwrite the current Support Element configuration data.

Current support element
Specifies the name of the current Support Element.

Serial number
Specifies the current serial number of the Fibre Trunk selected for updating.

Location

Specifies the current location of the Fibre Trunk selected for updating.

Support element types
This table displays the support element types for the machine specified.

Select one and update the machine serial number, then click **Update Support Element**.

Updated serial number
Use this field to update the machine serial number.

Note: Updating this field will overwrite the current Support Element configuration data.

Update Support Element
To update the support element you selected, click **Update Support Element**.

Note: Updates to this window will overwrite the current Support Element configuration data.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Delete Support Element

Use this window to delete a Support Element from the hardware configuration of the specified machine, then click **Delete Support Element**.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Associated CPC
Displays the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the Support Elements of its CPCs. A Support Element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

Current Support Element(s) table
This table displays current Support Elements by description, serial number, and location.

Select the Support Element you want deleted from the hardware configuration of the specified machine, then click **Delete Support Element**.

Delete Support Element
To delete the Support Element you selected, click **Delete Support Element**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Fibre Trunk

Use this window to add Fibre trunks to the current hardware configuration for the machine.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Fibre trunk locations
Select the location of the lower, left-hand corner of the Fibre Trunk.

Serial number
Specify the serial number of the Fibre Trunk.

Add Fibre Trunk
To add a Fibre Trunk to the system with the information currently displayed, click **Add Fibre Trunk**.

Note: This unit is not displayed graphically. In order to view the Fibre Trunk configuration at a later time, select **Update Fibre Trunk** from the list of options.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Cancel
To close the window without adding a Fibre Trunk, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update Fibre Trunk

Use this window to update Fibre Trunk information currently in the hardware configuration for the machine.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Fibre trunk locations
Select the location and serial number that correspond to the Fibre Trunk you want to update.

Update Fibre Trunk...
To update the currently selected Fibre Trunk location or serial number, click **Update Fibre Trunk...**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration for the machine.

Cancel
To close the window without updating a Fibre Trunk, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update Fibre Trunk

Use this window to update Fibre Trunk information currently in the hardware configuration for the machine.

Machine Type
Displays the machine type of the machine.

Machine Model
Displays the model number of the machine.

Current location
Specifies the current location of the Fibre Trunk selected for updating.

Current serial number
Specifies the current serial number of the Fibre Trunk selected for updating.

Fibre trunk locations
Select the location of the Fibre Trunk.

Serial number
Specify the serial number of the Fibre Trunk.

Update Fibre Trunk
To update the specified Fibre Trunk with the new data specified on this panel, click **Update Fibre Trunk**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Cancel
To close the window without updating a Fibre Trunk, click **Cancel**.

Help
To display help for the current window, click **Help**.

Delete Fibre Trunk

Use this window to delete Fibre Trunks from the current hardware configuration for the machine.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Fibre Trunk locations
Select the location and serial number that correspond to the Fibre Trunk you want to remove.

Delete Fibre Trunk
To delete the currently selected Fibre Trunk from the system, click **Delete Fibre Trunk**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Cancel
To close the window without deleting a Fibre Trunk, click **Cancel**.

Help
To display help for the current window, click **Help**.

Devices mounted in rear of frame

This window displays the current devices mounted in the rear of the frame.

Enable FTP Access to Mass Storage Media

Accessing the Enable FTP Access to Mass Storage Media task

This task allows your system processor to install software from mass storage media (CD, DVD, or USB flash memory drive) located on the Hardware Management Console. In addition to using this task you also need to work with the **Load from Removable Media or Server** task and monitor Operating System Messages. See "Installing software from a mass storage device" on page 827 for the entire procedure.

To allow FTP access to the mass storage media:

1. Open the **Enable FTP Access to Mass Storage Media** task. The Enable FTP Access to Mass Storage Media message window is displayed.
2. Click **Yes**, the Enable FTP Access to Removable Mass Storage Media window is displayed.
3. Specify the TCP/IP address or host name of the system processor that requires access to the Hardware Management Console for the mass storage media. The Enable FTP Access to Mass Storage Media message window is displayed.
4. Specify the user ID and password information from the **Load from Removable Media or Server** task.
5. Click **CLOSE** when you no longer need the FTP access and the installation is complete.

Enable FTP Access to Removable Mass Storage Media

Use this task to allow another computer to have FTP read-only access to the removable mass storage media (CD, DVD, or USB flash memory drive) on this Hardware Management Console. FTP access will be allowed only while this task is active, and only from the TCP/IP address specified.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed.

Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Installing software from a mass storage device

This procedure is used for installing an operating system (such as, Linux or z/VM) from a mass storage device to your system processor that does not have a CD or DVD drive attached to it. Using the **Enable FTP Access to Mass Storage Media** task, the **Load from Removable Media or Server** Recovery task, and monitoring the **Operating System Messages** will assist you in accessing this software.

Before you begin, you need to know the IP addresses of the following:

- The system processor you want to install the software on.
- The Hardware Management Console you will be getting the software from.

  To locate this IP Address:

  1. Open the **Customize Network Settings** task. The Customize Network Settings window is displayed.
  2. Select **LAN Adapters** tab. The **LAN Adapters** table is displayed. From the list of LAN adapters, note the IP address of the network adapter that connects the processor to the Hardware Management Console.

Perform the following Hardware Management Console steps:

1. If you have not already done so, log on to the Hardware Management Console using the SYSPROG default user ID or a user ID that has been assigned System Programmer roles.
2. Insert the media that contains the operating system you want installed on your processor.
3. Open the group of defined CPCs that contains the object with the Support Element that you want to connect to.
4. Select one CPC.
5. Open the group of defined CPC images that contains the image that you want to connect to.
6. Open the **Load from Removable Media or Server** task to start it. The Load from Removable Media or Server Task Confirmation window is displayed.
7. Click **Yes** to continue. The Load from Removable Media or Server window is displayed.
8. Select **Hardware Management Console CD / DVD-ROM** and specify a **File location** as required for your load media on the Load from Removable Media or Server window.
9. Click **OK** and perform the operation.
10. Open the **Enable FTP Access to Removable Mass Storage Media** task. The Enable FTP Access to Mass Storage Media message window is displayed. To allow FTP access to the mass storage media, click **Yes**.
11. The Enable FTP Access to Removable Mass Storage Media window is displayed.
12. Specify the TCP/IP address of the processor that you want the software to be sent to, then click **Enable**. The **Enable FTP Access to Mass Storage Media** message window is displayed. Minimize this window, you will need the information in step **10**.
13. Use **Operating System Messages** or the appropriate interface to continue the loading.
14. Click **OK** to close the window when installation is complete, or

    a. Click **Exchange Media** on the Enable FTP to Mass Storage Media window to insert the next media.

    b. Repeat step **a** until all media has been read, then click **CLOSE** on the Enable FTP to Mass Storage Media window when you are finished.

Additional functions are available from this window.

TCP/IP address
Specify the host name or an IPv4 or IPv6 TCP/IP address of the computer you want to allow access to the Hardware Management Console removable mass storage media. The IPv4 address is written as four decimal numbers, representing the four bytes of the IP address, separated by periods (for

example, `9.60.12.123`). The IPv6 address can be written as eight groups of four hexadecimal digits, separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

Note: For IPv6 simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or you can use a double colon in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

Enable
To begin allowing access to the mass storage media, click **Enable**.

Cancel
To end this task and not allow FTP access to the mass storage media, click **Cancel**.

Help
To display help for the current window, click **Help**.

Enable I/O Priority Queuing

Accessing the Enable I/O Priority Queuing task

This task allows you to enable or disable global input/output (I/O) priority queuing for the system. Enabling I/O priority queuing allows the system to specify a priority to be associated with an I/O request at start subchannel time. A range of priorities for a logical partition will be supported. These values will be passed on to the I/O subsystem for use when making query decisions with multiple requests.

To enable I/O priority queuing:

1. Select one or more CPCs (servers).
2. Open the **Enable I/O Priority Queuing** task. The Enable I/O Priority Queuing window is displayed.
3. Click the drop-down menu under **Setting** to make your selection for the specified CPCs:

   Enabled
   Activates I/O priority queuing for the CPC.

   Disabled
   Deactivates I/O priority queuing for the CPC.
4. Click **Save** to save the setting.

Enable Input/Output (I/O) Priority Queuing

Use this window to view or change global Input/Output (I/O) priority queuing current setting for the system. The possible settings are to enable I/O priority queuing or to disable I/O priority queuing.

I/O priority queuing, when enabled, allows the operating system to specify a priority to be associated with an I/O request at start subchannel time. A range of priorities for a logical partition will be supported. These values will be passed on to the I/O subsystem for use when making queuing decisions with multiple requests.

Enable Input/Output (I/O) Priority Queuing
Use this table to enable (or disable) I/O priority queuing dynamically after an Initial Microcode Load (IML).

I/O priority queuing allows the operating system to specify a priority to be associated with an I/O request at Start Subchannel time. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

Object Name
Displays the names of the CPCs in the group selected.

Setting
To enable I/O priority queuing for the CPC, select **Enabled**. To disable the I/O priority queuing for the CPC, select **Disabled**.

Save
To save the setting you selected, click **Save**.

Reset
To discard the unsaved changes made and display the initial settings, click **Reset**.

Cancel
To cancel your request to enable or disable I/O priority queuing, click **Cancel**.

Help
To display help for the current window, click **Help**.

Enable/Disable Dynamic Channel Subsystem

Accessing the Enable/Disable Dynamic Channel Subsystem task

Performing a power-on reset of the central processor complex (CPC), either directly or by activating the CPC, establishes many of its initial operational capabilities and characteristics, including whether dynamic input/output (I/O) configuration is enabled or disabled. After a power-on reset of the CPC is performed, changing its operational capabilities and characteristics requires performing another power-on reset.

If a power-on reset of the CPC initially enables dynamic I/O configuration, a task becomes available on the support element workplace for changing the CPC's dynamic I/O setting without performing another power-on reset.

To change the CPC's dynamic I/O setting without performing a power-on reset:

1. Open the **Enable/Disable Dynamic Channel Subsystem** task to start it.

   The Customize Dynamic Channel Subsystem window displays.
2. Use the window's controls, as follows, to enable or disable dynamic I/O for the CPC:
   a. Review the CPC's current setting for dynamic I/O. The selected **Enabled** or **Disabled**, indicates the current setting.
   b. While dynamic I/O is enabled, select **Disabled** to change the setting to disabled.
   c. Or while dynamic I/O is disabled, select **Enabled** to change the setting to enabled.
   d. Click **OK** to save the setting and close the window.

Enable or Disable Dynamic Channel Subsystem

Use this window to change the CPC's dynamic I/O setting *without* having to perform a power-on reset to make the new setting take effect.

Your input/output (I/O) configuration is the set of all I/O device, control units, and channel paths you define to your hardware and software.

Performing a power-on reset establishes the *hardware I/O definition*. That is, it defines the I/O configuration to the hardware. Loading the software establishes the *software I/O definition*. That is, it defines the I/O configuration to the software.

If the hardware and software support *dynamic I/O configuration*, you can change their I/O definitions dynamically. That is, changes made through dynamic I/O configuration take effect immediately; they do *not* require a power-on reset or load to make them take effect.

Performing a power-on reset of the CPC, either directly or by activating the CPC, establishes many of its initial operational capabilities and characteristics, including whether dynamic I/O is enabled or disabled. Ordinarily, after a power-on reset of the CPC is performed, changing its operational capabilities and characteristics requires performing another power-on reset. The **Enable/Disable Dynamic Channel Subsystem** task allows you to change the CPC's dynamic I/O setting *without* having to perform a power-on reset to make the new setting take effect.

Dynamic channel subsystem
This field indicates whether dynamic input/output configuration (dynamic I/O) currently is enabled or disabled for the central processor complex (CPC).

Select the new setting to change the setting, then click **OK** to make the new setting take effect. The settings are:

Enabled
To enable dynamic I/O, select this option.

Disabled
To disable dynamic I/O, select this option.

OK
To save the dynamic I/O setting currently selected, click **OK**.

Cancel
To end the task and undo any changes made to dynamic I/O, click **OK**.

Help
To display help for the current window, click **Help**.

Enabled/Disabled Setting

Enabled/Disabled Setting

Use the **Enabled** and **Disabled** settings for the **Automatic Activation** and **Enable I/O Priority Queuing** tasks.

Settings table
To enable the **Enable I/O Priority Queuing** or **Automatic Activation** tasks, select **Enabled**. To disable the tasks, select **Disabled**.

Save
To save the setting you selected, click **Save**.

Reset
To discard changes you made and display the current settings, click **Reset**.

Cancel
To cancel your request to enable or disable the **Enable I/O Priority Queuing** or **Automatic Activation** tasks, click **Cancel**.

Help
To display help for the current window, click **Help**.

Energy Optimization Advisor

Accessing the Energy Optimization task

Use this task to view recommendations that will reduce power consumption based on your present system operations. The task displays recommendations (advices) in graphical form. There are two types of power consumption you can manage; inlet air temperature and static power save mode.

Note: The messages are refreshed every 10 minutes. Relaunch this task to view the current messages.

1. Locate and open the **Energy Optimization Advisor** task. The Energy Optimization Advisor window displays.
2. Click the hyperlink in the Advice table to display thermal or utilization advice graphically for your system. You can optionally click the hyperlink to open the **Set Power Savings** task from the Processor Utilization Advice window.
3. Click **Close** to close the window.

Energy Optimization Advisor

This window displays recommendations that reduces power consumption based on the present system operation. Select the advice hyperlink to provide specific recommendations for your system.

Note: The messages are refreshed every 10 minutes. Relaunch this task to view the current messages.

The following list provides a description of each element in the Energy Optimization Advisor window:

Energy Optimization Advisor table toolbar

You can work with the table by using the table icons or **Actions** list from the Energy Optimization Advisor table tool bar.

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Provides a way to exclude or include specific columns from the table display. Available columns are in lists by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**

Columns in the Energy Optimization Advisor table

The following columns are displayed for the Energy Optimization Advisor table. You can modify the columns in the default table display by using the **Configure Options** icon.

“Thermal Advice” on page 831
Displays your system power consumption and inlet air temperatures graphically for each processor in the system.

“Processor Utilization Advice” on page 832
Displays your system processor utilization graphically and thermal advice.

Time and Date
Displays the time and date the advice was generated for your system.

Additional functions on this window include:

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

Thermal Advice

This window displays the power consumption and inlet air temperature graphically for your system and thermal advice. The graph displays the air inlet temperature on the left and the system power consumption on the right. The temperature threshold relevant to this recommendation is shown as a dashed horizontal line. Select the **Monitor Dashboard** link for real time trending data.

Select from the drop down list the time span for the x axis. Selecting a different time scale results in the chart re-rendering updating temperature and power consumption data on the span for the recommendation selected:

- Four hours
- One day
- Three days
- One week

Additional functions on this window include:

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

Processor Utilization Advice

This window displays the processor utilization graphically for each processor in the system. The graph displays the processor utilization as a percentage on the left side. The temperature threshold relevant to this recommendation is shown as a dashed horizontal line. Select the **Monitor Dashboard** link for real time trending data or **Set Power Savings** link to set the system into static power save mode.

Select from the drop down list the time span for the x axis. Selecting a different time scale results in the chart updating processor utilization for the recommendation selected:

- Four hours
- One day
- Three days
- One week

Additional functions on this window include:

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

Engineering Changes (ECs)

Accessing the Engineering Changes (ECs) task

Notes:

- The CPC(s) must be placed in Service Status before starting this task.
- You cannot perform this task remotely.
- Engineering Changes (ECs) is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task copies base code ECs from a CD/DVD-ROM to the Hardware Management Console to install on the primary Support Element of a CPC. You can upgrade the primary Support Element in either of the following ways:

Upgrade primary SE
Upgrade both the operating system code and the Support Element function code. This option deactivates the CPC and stops all operating systems running on the CPC.

Upgrade primary SE operating system
Upgrade only the operating system code. This option can be run concurrent to the operating systems running on the CPC.

To upgrade the primary Support Element:

1. Select a CPC (server).

2. Open the **Engineering Changes (EC)** task. The Upgrade Engineering Change (EC) window is displayed.
3. Click the engineering change option you want to perform, then click **OK**. The Insert the SE-CD window is displayed.
4. Ensure that the CD/DVD-ROM is in the drive, and click **OK**.

Upgrade Engineering Change (EC)

Use this window to upgrade the primary Support Element (SE) internal code and upgrade the primary SE operating system.

Upgrading the primary SE is a disruptive internal code change and requires deactivating the CPCs on which the changes are installed. Since deactivating a CPC ends its operating system activity, upgrading the primary SE internal code changes is considered a disruptive operation.

When the upgrade of ECs is complete, you must re-activate each CPC and restart all jobs.

Note: Confirm your request to upgrade the primary SE only if ending operating system activity on the selected CPCs is acceptable at this time.

Upgrading the primary SE operating system is not a disruptive internal code change and does not require CPC deactivation.

Upgrade primary SE
To upgrade the primary Support Element (SE) internal code, select **Upgrade primary SE**.

This option deactivates the CPC and stops all operating systems running on the CPU.

Upgrade primary SE operating system
To upgrade the primary Support Element (SE) operating system, select **Upgrade primary SE operating system**.

This option can be run concurrent to the operating systems running on the CPC.

OK
To confirm your request to upgrade the engineering changes, click **OK**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Upgrade Engineering Change (EC) Information

This window displays the Engineering Changes (ECs) for the primary or alternate Support Elements that are currently available on the media for the selected Central Processor Complex (CPC).

Use this window to copy base code engineering changes from the media to the Hardware Management Console.

List of engineering changes

Level
Displays the EC release level and number.

Description
Displays a brief description of the EC.

OK
To confirm your request to upgrade the engineering changes, click **OK**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Apply Changes Confirmation

Use this window to confirm or cancel your request to apply Engineering Changes (ECs) to the Central Processor Complexes (CPCs) listed.

If any systems will be deactivated, all jobs running on those systems will be stopped.

CPCs
The CPCs that you selected are listed in this window. Use this list of CPCs to confirm or cancel your request to apply Engineering Changes (ECs) to them.

OK
To confirm your request to apply the ECs, click **OK**.

Cancel
To cancel your request to apply the ECs, click **Cancel**.

Help
To display help for the current window, click **Help**.

Environmental Efficiency Statistics

Accessing the Environmental Efficiency Statistics task

Note: This task can only be used with IBM Z® (Z).

To display environmental efficiency statistics data:

1. Select a system.
2. Open the **Environmental Efficiency Statistics** task. The Environmental Efficiency Statistics window is displayed.
3. Specify a start date, start time, and make a selection from the duration list.
4. Click **Refresh** to update the window.
5. From the Chart Content list select the graphical display that you prefer.
6. If you are accessing the Hardware Management Console remotely, click **Export** to save the environmental efficiency data that is currently displayed to a Comma Separated Values (csv) file.
7. When you have completed this task, click **Close**.

Display Environmental Efficiency Statistics Data

This window displays the following environmental efficiency data graphically and in table format for the selected system:

- Power consumption (kW and Btu)
- Temperature (Celsius and Fahrenheit)
- CP utilization percentage

  Note: In addition to CPs; ICFs, IFLs, zIIPs, and zAAPs (Version 2.12.1 and earlier) are also included in this measurement.

To display new environmental efficiency data:

- Enter the start date, start time, and duration from the list
- Click **Refresh** to update the window
- Select from the Chart Content list what you want to display graphically
- Click **Export** if you want to export the displayed environmental efficiency data to a text file.

The following information describes the options available from this window.

Starting Date
Enter the starting date of the environmental efficiency data to display.

Starting Time
Enter the starting time of the environmental efficiency data to display.

Duration
Select the number of days of environment efficiency data to display beginning with the starting date and time.

Previous
To display environmental efficiency data for the prior time period based on the **Starting date**, **Starting time**, and **Duration**, click **Previous (<)**.

Next

To display environmental efficiency data for the next time period based on the **Starting date**, **Starting time**, and **Duration**, click **Next (>)**.

Chart Content
Select the type of environmental efficiency data from the chart content list to display graphically.

Refresh
To update the environmental efficiency statistics data with the new starting date, time, and duration, click **Refresh**.

Export
To export the Environmental Efficiency Statistics data into spread sheet format, click **Export**.

Note: This option is only available when you are accessing the Hardware Management Console remotely.

Close
To close this window, click **Close**.

Help
To display help for the current window, click **Help**.

FCP Configuration

Accessing the FCP Configuration task

The N Port Identifier Virtualization (NPIV) for Fibre Channel Protocol (FCP) channels allows sharing of a single physical FCP channel among operating system images. Use this task to display or alter worldwide port names assigned to FCP channels.

Use this task to:

- Display all N Port Identifier Virtualization (NPIV) port names currently assigned to FCP subchannels...
- Display WWPN for the physical ports of FCP channels...
- Import or export configuration...
- Release all port names that had previously been assigned to FCP subchannels that are now locked
- Release a subset of the port names that had previously been assigned to FCP subchannels that are now locked...
- Reset WWPN assignments for physical ports

To enable the NPIV mode for selected channel paths see the **FCP NPIV Mode On/Off** task.

To display or alter worldwide port names assigned to FCP channels:

1. Locate the **CPC** to work with.
2. Open the **FCP Configuration** task.

   The FCP Configuration window displays.
3. Select the operation you want to perform from the FCP Configuration window.

4. Click **OK** after making your selection.

FCP Configuration

This task allows you to display or alter worldwide part names assigned to FCP channels for the selected CPC.

When NPIV mode is enabled for selected logical partitions, the system provides a virtual FCP channel for each S/390® device definition for an FCP channel in the active input/output configuration.

Each virtual FCP channel is logged into the Storage Area Network (SAN) using a worldwide unique identifier. This worldwide port name (WWPN) is assigned by the system and used during the login procedure with the SAN when an operating system establishes a communication path to an FCP channel.

Use this FCP Configuration window to:

- Display all NPIV port names that are currently assigned to FCP subchannels...

  The "Display FCP NPIV Port Names" on page 837 window allows you to select what ports to display.
- Display WWPN for the physical ports of FCP channels...

  The "Display WWPN for the physical ports of FCP channels" on page 839 window displays the PCHID and corresponding WWPN.
- Import or export configuration...

  The "Import or Export Configuration" on page 836 window allows you to select an action and a location to export or import WWPN for physical ports.
- Release all port names that had previously been assigned to FCP subchannels and are now locked
- Release a subset of the port names that had previously been assigned to FCP subchannels and are now locked...
- Reset WWPN assignments for physical ports.

Additional functions on this window include:

Cancel
To exit this task, click **Cancel**.

OK
To continue with the operation, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Display all NPIV port names that are currently assigned to FCP subchannels...

To display the worldwide port names assigned to FCP subchannels, select **Display all NPIV port names that are currently assigned to FCP subchannels...**.

Display WWPN for the physical ports of FCP channels...

To display the worldwide port names for the physical ports assigned to FCP channels, select **Display WWPN for the physical ports of FCP channels...**.

Import or Export Configuration

Use this window to select an action and location to export or import NPIV system or mode configuration file.

Action:

- Export binary NPIV system configuration file
- Export binary NPIV mode configuration file
- Export WWPN for physical ports

- Import binary NPIV system configuration file
- Import binary NPIV mode configuration file
- Import WWPN for physical ports.

Location:

- Hardware Management Console USB flash memory drive
- FTP site.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Release all port names that had previously been assigned to FCP subchannels and are now locked...

To release and reassign all locked worldwide port names that had previously been assigned to FCP subchannels and are now locked, select **Release all port names that had previously been assigned to FCP subchannels and are now locked...**.

When NPIV mode is enabled for selected logical partitions, the system provides a virtual FCP channel for each S/390 device definition for a FCP channel in the active input/output configuration.

After a WWPN has been assigned to a virtual FCP channel and the S/390 device definition is deleted, the WWPN is not eligible for reassignment to a different virtual FCP channel. Rather, the WWPN and the virtual FCP channel are remembered in a least-recently used (LRU) list. If the same S/390 device definition is added back again, the same WWPN will be assigned to the pertaining virtual FCP channel.

Since the size of the LRU list is limited, the WWPN and the virtual FCP channel may be removed from the LRU list. The WWPN is then locked to prevent from reassignment to a different virtual FCP channel.

Use this window to release a subset of locked worldwide port names to make them available for assignment to different S/390 devices when WWPNs available for new virtual FCP channels become exhausted.

Release a subset of the port names that had previously been assigned to FCP subchannels and are now locked...

To release and reassign a subset of locked worldwide port names that had been previously assigned to FCP subchannels and are now locked, select **Release a subset of the port names that had previously been assigned to FCP subchannels and are now locked...**.

Display FCP NPIV Port Names

The selection list allows you to display all PCHID and/or LPAR assigned ports.

- Display all assigned ports
- Display all assigned ports for an LPAR
- Display all assigned ports for a PCHID.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit this task, click **Cancel**.

You can find more detailed help on the following elements of this window:

Display Assigned Port Names

Use this window to display the worldwide port names assigned to FCP subchannels.

Note: This window will not automatically refresh and therefore does not reflect any configuration changes while the window is open. You can transfer the information to a different server using the File Transfer Protocol (FTP) function on this window. This function may be useful when setting your Storage Area Network (SAN) configuration or devices attached to the SAN.

Select an option to:

- Show only entries defined with the current configuration
- Show only entries with NPIV On.

Additional functions on this window include:

Apply
To display information for the selected entry, click **Apply**.

Transfer via FTP
To export the worldwide port name assignment information into a file to transfer using FTP destination, click **Transfer via FTP**.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more help on the following elements of the Display Assigned Port Names window:

Display assigned port names table

Partition
Displays the name of the logical partitions.

CSS
Displays a number that identifies the channel subsystem a channel path is in.

ID
Displays the Image ID number that identifies the channel path.

CHPID
Displays a number that identifies the channel path identifier.

SSID
Displays the Subchannel Set ID for the channel path

Device Number
Displays a number that identifies a device.

WWPN
Displays the worldwide port numbers for the logical partitions.

NPIV Mode
Displays the NPIV mode for the logical partitions.

Current Configured
Displays whether the IOCDS for the logical partition is active.

PCHID selection

Select from the PCHID name list, the specific PCHID you want to display the assigned ports.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit this task, click **Cancel**.

LPAR selection

Select form the LPAR name list, the specific LPAR you want to display the assigned ports.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit the current window, click **Cancel**.

Display WWPN for the physical ports of FCP channels

This windows displays the physical channel identifier (PCHID) and corresponding worldwide port name for all FCP channels.

Additional functions on this window include:

Export to USB Flash Memory Drive

To export the WWPN view for the physical ports of FCP channels, click **Export to USB Flash Memory Drive**.

Notes:

- Available only from the Hardware Management Console.
- If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Release Subset

When NPIV mode is enabled for selected logical partitions, the system provides a virtual FCP channel for each S/390 device definition for a FCP channel in the active input/output configuration.

After a WWPN has been assigned to a virtual FCP channel and the S/390 device definition is deleted, the WWPN is not eligible for reassignment to a different virtual FCP channel. Rather, the WWPN and the virtual FCP channel are remembered in a least-recently used (LRU) list. If the same S/390 device definition is added back again, the same WWPN will be assigned to the pertaining virtual FCP channel.

Since the size of the LRU list is limited, the WWPN and the virtual FCP channel may be removed from the LRU list. The WWPN is then locked to prevent from reassignment to a different virtual FCP channel.

Use this window to release a subset of locked worldwide port names to make them available for assignment to different S/390 devices when WWPNs available for new virtual FCP channels become exhausted.

Additional functions on this window include:

Transfer via FTP
To export the worldwide port name assignment information into a file to transfer using FTP destination, click **Transfer via FTP**.

Release
To release the subset of worldwide port names that display on this window, click **Release**.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Import or Export Configuration

Use this window to select an action and location to export or import NPIV system or mode configuration file.

Action:

- Export binary NPIV system configuration file
- Export binary NPIV mode configuration file
- Export WWPN for physical ports
- Import binary NPIV system configuration file
- Import binary NPIV mode configuration file
- Import WWPN for physical ports.

Location:

- Hardware Management Console USB flash memory drive
- FTP site.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

FCP NPIV Mode On/Off

Accessing the FCP NPIV Mode On/Off task

Use this task to enable N Port Identifier Virtualization (NPIV) mode for selected channel paths. When NPIV mode is enabled for selected channel paths, the system provides a virtual FCP channel for each S/390 device definition for a FCP channel in the active Input/Output configuration.

Note: The channel paths must be configured offline to enable NPIV mode.

To set the NPIV configuration:

1. Open the **FCP NPIV Mode On/Off** task.

   The NPIV Mode On/Off window displays.
2. Click **Select All** to select all the listed channel paths to enable for NPIV mode.
3. Click **Deselect All** to deselect all the listed channel paths that are enabled for NPIV mode.
4. Click **Apply** to make the changes.

FCP NPIV Mode On/Off

Use this window to enable FCP NPIV mode for selected channel paths. The channel paths must be configured offline to enable FCP NPIV mode.

FCP NPIV Mode On/Off table

This table contains the following information:

Partition
Displays the name of the logical partition.

CSS
Displays a number that identifies the channel subsystem a channel path is in.

CHPID
Displays a number that identifies the channel path identifier.

FCP NPIV Mode Enabled
Displays the FCP NPIV mode for the logical partition.

Select All
To select all the listed channel paths to be enabled for FCP NPIV mode, click **Select All**.

Deselect All
To deselect all the listed channel paths that are enabled for FCP NPIV mode, click **Deselect**.

Apply
To make the current changes to this window, click **Apply**.

Cancel
To cancel your request to enable FCP NPIV mode for selected channel paths, click **Cancel**.

Help
To display help for the current window, click **Help**.

Fibre Channel Analyzer

Accessing the Fibre Channel Analyzer task

This task displays the errors on the fibre channels of attached Support Elements to assist in identifying link and control unit problems.

Note: To view the errors on the fibre channel, using this task, you must enable the **Fibre channel analysis** option from the **Customize Console Services** task.

To view the information:

1. Open the **Fibre Channel Analyzer** task. The Fibre Channel Error Summary window is displayed. The error logs displayed contain information about the following:
   - System
   - PCHID
   - Source Link Address
   - Destination Link Address
   - CHPID
   - Channel Type
   - Error Count.
2. Select one of the systems to view additional information. The Error Summary Details portion of the window displays this additional information.
3. Click **Close** when you are done reviewing the information.

Fibre Channel Analyzer Error Summary

Use this window to view the errors on the fibre channels of attached Support Elements to assist in identifying link and control unit problems. The information is analyzed to detect the trends and thresholds and reports the results to you.

When a fibre channel error has reached its threshold a Fibre Channel Network icon appears on the Hardware Management Console workplace. You can drag this icon to Hardware Messages where results of the analysis are displayed.

Fibre Channel Errors

You can work with the **Fibre Channel Errors** table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description is displayed. The icons and list actions perform the following functions:

Remove All Items
Removes all the data listed in the table.

If you select **Remove All Items**, the **Fibre Channel Analyzer** message window is displayed for verification. You can click **OK** to continue with the removal of all the data, or click **Cancel** to keep the data in the table.

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this downloaded CSV file into most spreadsheet applications.

If you select **Export Data**, the Save File window is displayed. You can select the **Fibre Channel Analyzer Data** link to proceed or click **Cancel** to return to the previous window.

Note: This function is available only when you are accessing the Hardware Management Console remotely.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click Edit Sort to define sorts for columns in a table. Alternatively, to perform single column sorting, click the ^ in the column header, to change from ascending to descending order.

Clear All Sorts
Returns to the default ordering.

Configure Columns
Arranges the columns in the table in the order you want or hides columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns.

This portion of the task window displays, in table format, the information gathered of the errors on the fibre channels of attached Support Elements. This table displays the following information:

- System
- PCHID
- Source Link Address
- Destination Address
- CHPID
- Channel Type
- Error Count.

Error Summary Details
This portion of the window displays additional infomation about the system you selected.

Close
To close this window when you are done using this task, click **Close**.

Help
To display help for the current window, click **Help**.

Format Media

Accessing the Format Media task

Note: You cannot perform this task remotely.

This task formats removable media.

Use this task to select the appropriate format type and file system for the removable media.

- Change management system update level
- Backup/restore
- Service data
- Upgrade data
- Security log
- Problem Analysis data
- User-specified label.

To format removable media:

1. Open the **Format Media** task. The Format Media window is displayed.
2. Select the format type for the removable media, make sure your media is properly inserted, then click **Format**. If you selected **User-specified label**, the Specify Label window is displayed. Specify a label, then click **Format**.
3. The Select Media Device window is displayed. Select the media you want to format, then click **OK**.
4. If you selected the USB flash memory drive, the Specify File System window is displayed. For all format types, except Backup/restore, select the file system (VFAT or EXT2) that you want to use to format the file on your USB flash memory drive, then click **Format**. Backup/restore defaults to the EXT2 file system.
5. When the media is formatted, the Format Media Completed window is displayed.

Format Media

Use this window to select the appropriate format type for the removable media.

Format	Label
“Change management system update level (ACTSUL)” on page 843	ACTSUL
“Backup/restore (ACTBKP)” on page 844	ACTBKP
“Service data (SRVDAT)” on page 844	SRVDAT
“Upgrade data (ACTUPG)” on page 844	ACTUPG
“Security log (ACTSECLG)” on page 844	ACTSECLG
“Problem Analysis data (VIRTRET)” on page 844	VIRTRET
“User specified label” on page 844	The label is automatically written to the removable media.

Change management system update level (ACTSUL)

This formatted removable media is used in the **Change Console Internal Code** task. To choose this format type, select **Change management system update level**.

Backup/restore (ACTBKP)

This formatted removable media is used in the **Backup Critical Console data** task. To choose this format type, select **Backup/restore**.

Service data (SRVDAT)

This formatted removable media is used in the **Transmit Console Service Data** task. To choose this format type, select **Service data**.

Upgrade data (ACTUPG)

This formatted removable media is used in the **Save Upgrade Data** task. To choose this format type, select **Upgrade data**.

Security log (ACTSECLG)

This formatted removable media is used in the **Archive Security Logs** task. To choose this format type, select **Security log**.

Problem Analysis data (VIRTRET)

This formatted removable media is used in the **Offload Problem Analysis Data to Removable Media** task. To choose this format type, select **Problem Analysis data**.

User specified label

To specify your own label or leave blank, select **User specified label**. You can specify any label, up to 11 characters.

Additional functions are available from this window.

Format
To use the format type that you selected for your removable media, click **Format**.

If you selected **User specified label** and then clicked **Format**, the **Specify Label** window is displayed. You can type your own label name (up to 11 characters) in the **Label** input field or leave it blank. Click **Format** from that window to continue or **Cancel** to return to the previous window.

Cancel
To close this task without selecting a format type for the removable media, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Media Device

Use this window to select the desired removable media that is to be formatted.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

USB Flash Memory Drive
To use a USB flash memory drive as the removable media to be formatted, select **USB Flash Memory Drive**.

OK
To confirm your request to format the selected removable media, click **OK**.

Refresh
To redisplay the list of available removable media, click **Refresh**. Use this option if you did not insert your media before this point in the task.

Cancel
To close this window without formatting the removable media and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Specify File System

Use this window to select the appropriate file system you want to use to format the file on your USB flash memory drive.

VFAT
VFAT is the default file system for USB flash memory drives, it is supported on multiple operating systems, and has a maximum file size of 4GB. To use the virtual file allocation table (VFAT) file system to format the file on your USB flash memory drive, select **VFAT**.

EXT2
EXT2 is a LINUX file system that supports file sizes greater than 4GB on a USB flash memory drive. To use the second extended filesystem (ext2) file system to format the file on your USB flash memory drive, select **EXT2**.

Note: If you need to put any file greater than 4GB in size on your USB flash memory drive, then you can only use the EXT2 file system. If you choose **Backup/restore** as your format type, then this window is not displayed and the USB flash memory drive is formatted with the EXT2 file system.

Format
To format the file using the selected file system, click **Format**. A message window is displayed. You can continue with the operation by clicking **Yes** or you can return to the previous window by clicking **No**.

Cancel
To close this window without specifying a file system, click **Cancel**.

Help
To display help for the current window, click **Help**.

Getting Started with DPM

Accessing the Getting Started with Dynamic Partition Manager task

The **Getting Started with Dynamic Partition Manager** task introduces you to some of the basic concepts and tasks related to Dynamic Partition Manager (DPM) systems, adapters, and partitions.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

You can access the **Getting Started with Dynamic Partition Manager** task from the main HMC Welcome page, or select the task from the Tasks Index. The task is organized into sequential pages through which you can access links to additional information, or open other DPM tasks. Although anyone can access the **Getting Started with Dynamic Partition Manager** task, other DPM tasks might require specific authorization.

1. To open the **Getting Started with Dynamic Partition Manager** task, use one of the following options:

   - From the main HMC Welcome page, click the **Get Started** icon ().
   - In the navigation pane, expand the Tasks Index and click the link for the **Getting Started with Dynamic Partition Manager** task.

Either option opens the task in a separate window. The **Welcome** page is displayed, and its name is highlighted. As you move through the pages using **Next** or **Back**, the title of the current page is highlighted.

2. The **Welcome** page briefly describes DPM, and tasks that you can accomplish with it. Click **Next** to advance to the next page.
3. The **Adapters** page briefly describes the adapter cards, autodiscovery, and settings. On this page:
   - Click the **Learn More** link, which opens a separate window of online help that describes adapters in more detail.
   - Click the **Customize Adapter Settings** link to work with adapters that are already configured on the system. This link opens the **Manage Adapters** task in a separate window. You must have the appropriate authorization to use the **Manage Adapters** task:
     - One of the following default user IDs: SYSPROG, ADVANCED, ACSADMIN, or SERVICE
     - Or a user ID that a system administrator authorized to this task through customization controls in the **User Management** task.
   - Click **Next** to advance to the next page.
4. The **Partitions** page briefly describes partitions on a DPM-enabled system, and their settings, and how to create them. On this page:
   - Click the **Learn More** link, which opens a separate window of online help that describes partitions in more detail. Topics in this online help also provide guidance and instructions for using the **New Partition** task.
   - Click the **Create Partition** link to open the **New Partition** task in a separate window. To open the **New Partition** task, you need to use either the default SYSPROG user ID or a user ID that a system administrator authorized to this task through customization controls in the **User Management** task.
5. When you are finished reviewing the pages, click **Close** to close the **Getting Started with Dynamic Partition Manager** task.

Adapters for DPM systems and partitions

Adapters on a system fall into four categories: Network, Storage, Accelerators, and Cryptos. Each adapter type plays a specific role in communication, or data transfer, for partitions and the applications that run in them.

Most adapters are installed in the I/O cage or drawer of a physical processor frame. Depending on your company's planned use of specific systems, each system might have a different combination of installed adapters.

When adapters are installed in the processor frame, the adapters are configured using default settings. DPM automatically discovers these adapters and assigns names to them, using a standard naming convention. You can change the name and other default adapter settings through the **Manage Adapters** task, to conform with conventions that your company uses, or to provide more easily recognizable names for monitoring purposes.

To make use of the adapters configured on a DPM-enabled system, you select them when you use the **New Partition** task to create a new partition. Factors that determine your selections include:

- The specific adapters that are actually configured on the system.
- The requirements of the operating system and its applications, which are sometimes called the *workload* that your new partition will support.
- Any requirements or restrictions that your company has for the use of specific adapters. For example, your company might recommend selecting several adapters of the same type to maximize efficiency and provide redundancy.

You can successfully create and start a partition that does not have access to any adapters, which you might do if you want to do limited testing, or if you only want to quickly experiment with the **New Partition** task. At a later time, you can use the **Partition Details** task to modify your partition so that it has access to adapters.

The following topics provide additional information about adapters on a DPM-enabled system.

- "Adapter types" on page 847
- "Sources of additional information" on page 849

Adapter types

Partitions can share all types of system adapters, up to specific limits. Both the **New Partition** and **Partition Details** tasks display current usage information so you can determine whether or not your partition can use a specific adapter.

The following list describes the four categories of adapters that can be configured on a DPM-enabled system. These category labels correspond to navigation labels in the **New Partition** and **Partition Details** tasks.

Network

Several types of network adapters enable communication through different networking transport protocols. These network adapters are:

- Open Systems Adapter-Express (OSA-Express) adapters, which provide direct, industry-standard Ethernet LAN connectivity through various operational modes and protocols. OSA adapters can provide connectivity between partitions on the same system, as well as connectivity to external LANs. The supported OSA adapters vary, depending on the system configuration.
- HiperSockets, which provide high-speed communications between partitions within a single system, without the need for any physical cabling or external networking connections.
- Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) Express adapters. These adapters provide high speed, low latency data transfer over Ethernet networks. RoCE features are installed in the Peripheral Component Interconnect Express (PCIe) I/O drawer. The supported RoCE adapters vary, depending on the system configuration.

A DPM-enabled system also requires two OSA-Express 1000BASE-T Ethernet features for primary and backup connectivity.

DPM automatically discovers OSA and RoCE adapters because they are physical cards that are installed on the system. In contrast, HiperSockets are not physical adapters; you must configure them if you want to use them on your system. To create HiperSockets on a DPM-enabled system, use the **Create HiperSockets Adapter** task, which is available through the **Actions** list on the **Adapters** tab of the **Manage Adapters** task.

Network interface cards (NICs) provide a partition with access to internal or external networks that are part of or connected to a system. Each NIC represents a unique connection between the partition and a specific network adapter that is defined or installed on the system.

Most systems have OSA adapters installed, and you will probably define a NIC to connect your partition to at least one of those OSA network connections. Your system planner or network administrator can advise you on which network connections to use for the workload that your partition supports.

Storage

Fibre Channel connections (FICON) provide high-speed data transfer between systems and storage devices. Fibre Channel networks consist of servers, storage controllers, and other storage devices as end nodes, which are interconnected by Fibre Channel switches, directors, and hubs. Switches and directors are used to build Fibre Channel networks or fabrics. Through cables, FICON adapter cards connect the DPM-enabled system to the devices in this storage area network (SAN).

FICON adapter cards operate in different modes, which determine the type of storage devices that you can access. Typically, storage administrators configure the mode in which each FICON adapter card operates.

- Fibre Channel Protocol (FCP) mode provides access to Small Computer System Interface (SCSI) disk and tape devices, through single- or multiple-channel switches. Support for FCP mode for access to

disk devices is available with all DPM releases. Support for access to FCP tape devices is available with DPM R4.3 and later DPM versions.

- FICON native (FC or FICON) mode provides access to extended count key data (ECKD) devices, and tape devices, through point-to-point (direct) connections, or single- or multiple-channel switches. ECKD devices are more commonly known as direct-access storage devices (DASD). Support for FICON mode for access to disk devices is available with DPM R3.1 and later DPM versions.

DPM automatically discovers any FICON adapter cards that are configured on the system. These storage adapter cards are FICON Express features, which enable multiple concurrent I/O operations at various data transmission rates in gigabytes-per-second (Gbps), using Fibre Channel connections. The supported FICON Express adapter cards vary, depending on the system configuration.

DPM also automatically discovers any Non-Volatile Memory Express (NVMe) storage adapters that are installed in the system. These storage adapters consist of solid state drives (SSDs) that are installed in carrier cards in the system I/O drawers, and they provide high-speed storage within a system. NVMe storage is available only when the system has one or more IBM Adapter for NVMe1.1 features. Support for NVMe storage is available with DPM R4.2 and later versions.

Accelerators

Accelerators are adapters that provide specialized functions to improve performance or use of computer resources. DPM automatically discovers accelerators that are installed on the system, such as the zEnterprise Data Compression (zEDC) feature, which provides hardware-based acceleration for data compression and decompression. Only specific systems support accelerators.

zEDC features are installed in the Peripheral Component Interconnect Express (PCIe) I/O drawer. For each feature installed in the PCIe I/O drawer, one adapter/coprocessor compresses data according to the Internet Engineering Task Force (IETF) DEFLATE Compressed Data Format Specification, RFC 1951.

An accelerator virtual function provides a partition with access to zEDC features that are installed on a system. Each virtual function represents a unique connection between the partition and a physical feature card that is configured on the system.

Accelerators are optional features and, therefore, might not be installed on the system. If one is installed, your decision to enable your partition to access it depends on the workload that your partition will support. Your system planner can advise you about the use of available accelerators.

Cryptos

The term *cryptos* is a commonly used abbreviation for adapters that provide cryptographic processing functions. Industry Public Key Cryptography Standards (PKCS) and the Common Cryptographic Architecture (CCA) define various cryptographic functions, external interfaces, and a set of key cryptographic algorithms. These specifications provide a consistent, end-to-end cryptographic architecture across supported operating systems.

The use of the IBM cryptographic architecture is enabled through Crypto Express features, which provide a secure hardware and programming environment for cryptographic processes. Crypto Express features are installed in the Peripheral Component Interconnect Express (PCIe) I/O drawer. The supported Crypto Express features vary, depending on the system configuration.

DPM automatically discovers cryptographic features that are installed on the system. Each Crypto Express adapter can be configured in one of the following modes.

- Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.
- Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.
- Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Crypto features are optional and, therefore, might not be installed on the system. If these features are installed, your decision to enable your partition to access them depends on your company's security

policies, and the workload that your partition will support. Your system planner or security administrator can advise you about the use of available crypto features.

Sources of additional information

- For a list of the adapter features that can be configured on a DPM-enabled system, and for planning considerations related to their configuration, see the *IBM Dynamic Partition Manager Guide*, SB10-7170, which is available through the Publications link on IBM Resource Link at http://www.ibm.com/servers/resourcelink
- If you are unfamiliar with basic mainframe and Linux system concepts and terminology, you can find a brief introduction in IBM Knowledge Center at https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zmainframe/zconc_mfhardware.htm
- For more details about OSA, FICON, RoCE, HiperSockets and other adapters, see the *IBM z Systems® Connectivity Handbook*, SG24-5444, which is available on the IBM Redbooks® web site at http://www.redbooks.ibm.com/
- For more information about a specific system, see the appropriate system overview on the IBM Redbooks website at http://www.redbooks.ibm.com/
- For planning, installation, and usage information about OSA features, see *OSA Express Customer's Guide and Reference*, SA22-7935, which is available through the Publications link on IBM Resource Link at http://www.ibm.com/servers/resourcelink
- For more information about configuring HiperSockets, see the *IBM HiperSockets Implementation Guide*, SG24-6816, which is available on the IBM Redbooks web site at http://www.redbooks.ibm.com/
- For a list of switches, storage controllers, and devices that are verified to work in a Fibre Channel network that is attached to FCP channel, and for specific software requirements to support FCP and SCSI controllers or devices, see the IBM I/O Connectivity web page at http://www.ibm.com/systems/z/hardware/connectivity/index.html
- For information about using cryptographic hardware features with Linux, see the Linux on Z security topics in IBM Knowledge Center at https://www.ibm.com/support/knowledgecenter/linuxonibm/liaaf/sec_hw_supp.html

Partitions on DPM systems

A partition is a virtual representation of the hardware resources of an IBM Z or LinuxONE system. A partition is the runtime environment for either a hypervisor and its guest operating-system images, each with their own applications; or a single operating system and its applications, which are sometimes called the *workload*.

To create a partition, you use the **New Partition** task, through which you define the hardware resources that the partition can use: processors, memory, adapters, and so on. The end result of the task is a partition definition, which you can modify through the **Partition Details** task, or use to start the partition through the **Start** task. When you start a partition, DPM uses the partition definition to determine which hardware resources to allocate to the partition, and starts the initialization process.

You can successfully create and start a partition that does not have access to any adapters, which you might do if you want to do limited testing, or if you only want to quickly experiment with the **New Partition** task. At a later time, you can use the **Partition Details** task to modify your partition so that it has access to adapters. You can also use the **Stop** task to stop a partition, or the **Delete Partition** task to delete it. You can accomplish these tasks programmatically as well, through the Hardware Management Console Web Services application programming interfaces (APIs) for DPM.

You can create as many partition definitions as you want, but only a specific number of partitions can be active at any given time. The system limit determines the maximum number of concurrently active partitions. Practical limitations of memory size, I/O availability, and available processing power usually reduce the number of concurrently active partitions to less than the system maximum. In fact, conditions on the system might prevent a partition from successfully starting, or change its status after it has successfully started. You can view the status of a partition through the **Partition Details** task or use the **Monitor System Events** task to set notifications for specific partition events, such as a change in status.

The following topics provide additional information about partitions on a DPM-enabled system.

Partition properties and configuration settings

When you are using the **New Partition** task to create (or **Partition Details** task to modify) a partition, the task displays indicate which hardware resources are available for your partition to use, and also show the current usage of those resources by active (started) or reserved partitions. When you specify that the system resources for a partition are to be reserved, DPM does not allocate them to any other partitions. This reservation means that your partition is guaranteed to be startable; in contrast, partitions without reserved resources might fail to start, if sufficient resources are not available.

The following list describes key properties and configuration settings of partitions on a DPM-enabled system. The list labels correspond to navigation labels or individual fields in the **New Partition** and **Partition Details** tasks. For a complete list of the partition properties and settings, see the online help for either task.

Name
A partition name must uniquely identify the partition from all other partitions defined on the same system. On a DPM-enabled system, you can define a name for your partition that is 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. This partition name is shown in HMC task displays that contain information about system partitions.

A partition also has a short name, which is a name by which the operating system can identify the partition. By default, DPM automatically generates a partition short name that you can modify.

Partition type
Administrators can choose one of the following partition types for a new partition. Through the partition type, DPM can optimize the partition configuration for a specific hypervisor or operating system.

Linux
In this type of partition, you can install and run a Linux on Z distribution as a single operating system, or as a hypervisor for multiple guests.

z/VM
In this type of partition, you can install and run z/VM as a hypervisor for multiple Linux guests.

Secure Service Container
This type of partition is a Secure Service Container, in which you can run only specific software appliances that the Secure Service Container supports.

Processors
Each system (also known as a *central processor complex* or *CPC*) can contain several different types of z/Architecture® processors; each processor type has a slightly different instruction set or different internal code that customize each type for different purposes. All of the processors in the CPC begin as equivalent processor units (PUs) or engines that have not been characterized for a specific use.

Most DPM-enabled systems support one type of processor: Integrated Facility for Linux (IFL). In some cases, a system might also support an additional type: Central Processor (CP).

When you create a new partition on a DPM-enabled system:

- You can select which processor type to use only if both types are installed on the system.
- You can specify the number of processors to assign to the partition, and view how your selection affects the processing resources of other partitions on the system. The number of processors that you can assign ranges from a minimum value of 1 to a maximum value of the total number of entitled processors on the system. Entitled processors are processors that are licensed for use on

the system; the number of entitled processors might be less than the total number of physical processors that are installed on the system.

Memory

Each partition on a DPM-enabled system has exclusive use of a user-defined portion of the total amount of entitled memory that is installed on the system. Entitled memory is the amount of memory that is licensed for use, which might be less than the total amount of memory that is installed on the system. The amount of memory that a specific partition requires depends on the storage limits of the operating system that will run in it, on the storage requirements of the applications that run on the operating system, and on the size of the I/O configuration.

When you define the amount of memory to be assigned, or allocated, to a specific partition, you specify an initial amount of memory, and a maximum amount that must be equal to or greater than the initial amount. The partition receives its initial amount when it is started. If the maximum amount of memory is greater than the initial amount, you can add memory up to this maximum to the active partition, without stopping and restarting it.

Network

Network interface cards (NICs) provide a partition with access to internal or external networks that are part of or connected to a system. Each NIC represents a unique connection between the partition and a specific network adapter that is defined or installed on the system.

You need to define a NIC for each network connection that is required for the operating system or hypervisor that runs on this partition, or for the applications that the operating system or hypervisor supports. For example:

- If the applications that will run in this new partition require access to applications that run in other partitions in the same system, define a NIC for a HiperSockets switch or OSA port on the DPM-enabled system.
- Similarly, if these same applications on this new partition also require access to your company's data network, define a NIC for the OSA or RoCE port that your company uses for its data network.
- If the operating system to be installed on this partition resides on a network server, define a NIC for the HiperSockets switch or OSA port that your company uses for its network boot environment.

Storage

Partitions can access a variety of internal and external storage, depending on the configuration of adapters and features on the system. The way in which partitions access storage depends on whether the system has the DPM R3.1 storage management feature or a later DPM version applied.

- Without the feature applied, you create host bus adapters (HBAs) through the **New Partition** or **Partition Details** task. HBAs provide a partition with access to external storage area networks (SANs) and devices that are connected to a system. Each HBA represents a unique connection between the partition and a physical FICON channel that is configured on the system.
- With the feature or a later DPM version applied, you create a storage group through the **Configure Storage** task to provide access to external or internal storage.
  - When administrators request and fulfill FICON or FCP storage groups for partitions to access disk storage in the SAN, DPM automatically generates the world wide port names (WWPNs) that are allocated to virtual storage resources when the storage group is attached to a partition. For partitions to access disk storage, you use the **New Partition** or **Partition Details** task to simply select and attach one or more storage groups. During the attachment process, DPM generates the virtual storage resources (host bus adapters or FICON subchannels) that are required for partitions, and the operating systems that they host, to access the physical storage volumes in the SAN.
  - Administrators create Non-Volatile Memory Express (NVMe) storage groups for partitions to access any NVMe solid state drives (SSDs) that are installed in the system. Because NVMe storage is internal to the system, the storage group is immediately available for use when it is attached to a partition through the **New Partition** or **Partition Details** task.
- Starting with DPM R4.3, you create an FCP tape link through the **Configure Storage** task to provide access to one tape library in the SAN. One tape link uses one or more FICON Express adapters that

are configured in FCP mode to provide connectivity to one tape library. DPM automatically generates the world wide port names (WWPNs) that are allocated to virtual storage resources when the tape link is attached to a partition. During the attachment process, DPM generates the HBAs that are required for partitions, and the operating systems that they host, to access the physical tape library in the SAN.

Accelerators

Accelerators are adapters that provide specialized functions to improve performance or use of computer resources. One supported accelerator is the zEnterprise Data Compression (zEDC) feature, which provides hardware-based acceleration for data compression and decompression.

Accelerators are optional features and, therefore, might not be installed on the system. If one is installed, your decision to enable your partition to access it depends on the workload that your partition will support. Your system planner can advise you about the use of available accelerators.

Cryptos

The term *cryptos* is a commonly used abbreviation for adapters that provide cryptographic processing functions. Crypto features are optional and, therefore, might not be installed on the system. If these features are installed, your decision to enable your partition to access them depends on your company's security policies, and the workload that your partition will support. Your system planner or security administrator can advise you about the use of available crypto features.

Boot options

The following types of hypervisors and operating systems can run on a partition on a DPM-enabled system:

- Various Linux distributions, which are listed on the IBM tested platforms page for Linux environments. These distributions include supported versions of Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Ubuntu Server (KVM or LPAR DPM).
- z/VM 6.4 or later. z/VM is supported as a virtualization hypervisor on which you can run multiple Linux images

When you define a partition with a type of **Linux** or **z/VM**, you can specify the boot option through which DPM locates and installs the executables for the hypervisor or operating system to be run in the partition. You can choose one of several different options, including booting from a storage device, network server, FTP server (with your choice of protocol), and Hardware Management Console removable media.

DPM automatically sets the boot option for the first-time start of Secure Service Container partitions.

Using the New Partition task to create a new partition

To create a new partition on a DPM system, use the **New Partition** task, in either basic or advanced mode. See the online help for this task for a comparison of the two modes and the implications of switching between them, as well as step-by-step instructions for each page or section of the task.

Sources of additional information

- For planning considerations related to creating and running partitions on a DPM-enabled system, see the *IBM Dynamic Partition Manager Guide*, SB10-7170, which is available through the Publications link on IBM Resource Link at http://www.ibm.com/servers/resourcelink
- If you are unfamiliar with basic mainframe and Linux system concepts and terminology, you can find a brief introduction in IBM Knowledge Center at https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zmainframe/zconc_mfhardware.htm
- For more information about a specific system, see the appropriate system overview on the IBM Redbooks website at http://www.redbooks.ibm.com/
- For information about the DPM APIs, see the appropriate version of *Hardware Management Console Web Services API*, which is available through the Library link on IBM Resource Link at http://www.ibm.com/servers/resourcelink

- For information about installing and running a Linux distribution on an IBM Z or LinuxONE server, see the Linux topics in IBM Knowledge Center, at https://www.ibm.com/support/knowledgecenter/linuxonibm/liaaf/lnz_r_lib.html
- For additional information about KVM for IBM z Systems®, see http://www.ibm.com/systems/z/solutions/virtualization/kvm/index.html
- To determine end-of-service dates of IBM software products that you can run in a Linux environment, use the following URL to search the IBM Software Support Lifecycle Policies: http://www.ibm.com/software/support/systemsz/lifecycle/

Grouping

Accessing the Grouping task from the Daily task list

Note: If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (by using the **Configure Data Replication** task), the data that is specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the Configure Data Replication task.

This task enables you to create, delete, add to, or delete from user-defined groups of objects. When you select one or more CPCs, CPC images, or groups and open the **Grouping** task, the Manage Groups window is displayed, allowing you to specify what type of action you want to take on the group. You can create a group when you want to perform the same task on several CPCs or CPC images simultaneously instead of repeating the task on each individual CPC or CPC image. You can also create groups when managing multiple sysplexes by creating a group for each sysplex controlled by the Hardware Management Console.

You can also create a *Pattern Match* group. A *Pattern Match* group is a group that contains all managed objects of a given type (custom groups, defined CPCs, or images) whose names match a certain pattern (for example, all CPCs starting with P0).

Note: Once a pattern match group is defined and includes those objects that match the defined pattern, you cannot add additional objects to that group without changing the Managed resource pattern for that group.

To create a group with all CPCs starting with *P0*:

1. Select the object or objects you want to work with, then open the **Grouping** task. The Manage Groups window is displayed. Select **Create a new pattern match group** on the Manage Groups window, then click **OK**. The Create Pattern Match Group window is displayed.

   Or, you can open the **Grouping** task without selecting an object or objects. The Create Pattern Match Group window is displayed.
2. As shown in Figure 44 on page 854, select the **Group type** that you are creating.
3. Specify *P0group* in the **New group name** field and add a description of the group in the **New group description** field.
4. Specify *P0.** in the **Managed Resource Pattern** field on the **Create Pattern Match Group** window, then click **OK**.
5. You receive a message that the group (*P0group*) is created and the selected objects are added to it.

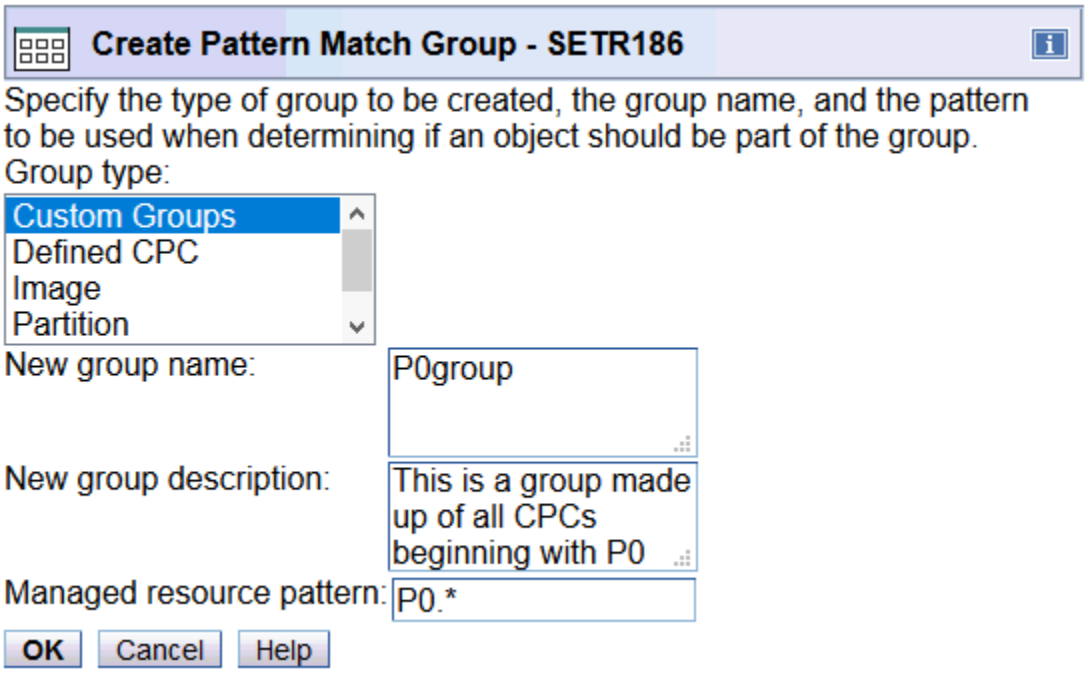


Figure 44. Create pattern match group window

Any new groups that you create are displayed in the **Systems Management** node. Also, an entry is displayed in the **User Management** task in the Manage Resource Roles table that indicates a group is added. The entry is **Groups created by *userid***, where ***userid*** is the name of the user that created the group.

To group CPCs or CPC images:

1. Open the group that contains the CPCs or images that you want to group.
2. Select one or more objects.
3. Open the **Grouping** task.
4. The Manage Groups window is displayed allowing you to add the selected object or objects to an existing group, remove the selected object or objects from a group, create a group, create a pattern match group, remove the group, create another pattern match group, or edit an existing pattern match group.

This task also allows you to group one or more user-defined groups into other groups. However, if you group user-defined groups into other groups, you cannot perform any task other than **Grouping** on these groups.

To group groups of user-defined CPCs and/or CPC images:

1. Select one of the groups you want to group together.
2. Open the **Grouping** tasks. The **Manage Groups** window is displayed.
3. Select **Create a new group**.
4. Enter a *group name* in the **New group name** input field and a description in the **New group description** input field.
5. Click **OK**. The Create a New Group window is displayed stating that you have successfully created a group.
6. Click **OK**. The new group is now displayed under **Custom Groups**.
7. Select another group that you want to add to the group you just created.
8. Open the **Grouping** task. The Manage Groups window is displayed.
9. Select **Add to an existing group**.

10. Select the *group name* that you created in **step 4** from the **Group Name** field.
11. Click **OK**. The Add to an Existing Group window is displayed stating that you have successfully added a group to another group.
12. Click **OK**. The group is no longer displayed in **Custom Groups** because it is now part of the group you created in **step 4.**
13. Repeat **steps 7** through **12** for as many groups that you want to add to the new group.

As previously stated, you cannot perform tasks on grouped groups. They can only be performed on the group that contains the individual CPCs or CPC images. You can get access to this group or the individual CPCs or CPC images in the group that uses one of the following methods:

- Click the group under the **Custom Groups** node in the navigation pane that you want to work with. This expands to show the groups that are nested within that group. Continue to click each nested group until the group that contains the individual servers is displayed in the work pane.
- Continue to click the group name from the work pane until the individual servers are displayed.

Manage Groups

Use this task to create, delete, add to, or remove from user-defined groups of objects.

Select one or more groups to manage. You can then specify whether you want to create a new group, add to an existing group, or remove from an existing group.

Selected Item(s)
Lists the server(s) or group(s) you currently have selected.

Group Action
Select a grouping action to perform by using the selected managed objects:

- Create a new group
- Add to an existing group
- Remove from an existing group
- Remove group
- Edit an existing group
- Create a new pattern match group

Create a new group
To add the selected objects into a new group, select **Create a new group**, and specify a name in the New group field.

Add to an existing group
To add selected objects to a group, select **Add to an existing group**, and select a name from the Group name list.

Remove from an existing group
To remove the selected objects from a group, select **Remove from an existing group**, and select a name form the Group name list.

Remove group
To delete the user-defined group, select **Remove group**.

Edit existing group
To change the properties of an existing group, select **Edit existing group**, then click **OK** to continue.

Note: You cannot change the group name.

Create a new pattern match group
To create a group that contains objects of one or more specified types with names that match a specified pattern, select **Create a new pattern match group**, then click **OK** to continue.

New group name
Specify a name for a new group. This name, consisting of 1 to 30 characters, is required to create a new group.

New group description
Specify a description that represents this group name.

Group name
Displays the names for existing groups. Selecting a name from this list is required to add to or delete objects in a group.

OK
To accept the group actions, click **OK**.

Cancel
To exit this task without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Create/Edit Pattern Match Group

Use this window to create or edit a pattern match group.

- Select one or more group types from the list to be added to the pattern match group.
- Specify the name of the new group and specify a pattern to determine when a managed object is included in the group.

  Notes:

  – You cannot change the name of an existing group.
  – Once a pattern match group is defined and includes those objects that match the defined pattern, you cannot add additional objects to that group without changing the Managed resource pattern for that group.

Group type
Displays the names of managed object types that can be included in pattern matching groups.

Select the type of managed objects to include in the group. You can select more than one type by pressing Ctrl while selecting each item.

New group name
Specify a unique name for the new group. This is a required field, consisting of 1 to 30 characters.

New group description
Specify a description that represents this group name.

Managed Resource Pattern
Specify a pattern (expression) to use to determine whether a managed object of the specified type is included in the group. For example, if you specified **P0.***, this includes all objects whose name begins with **P0** and includes any number of characters that follow.

The pattern is applied to the name of the managed object, and the object becomes part of the group if the name matches the pattern.

OK
To accept the group information you provided, click **OK**.

Cancel
To exit this task without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Hardware Messages

Accessing Hardware Messages

Displays consolidated hardware related messages for all selected hardware in the processor cluster, including your Hardware Management Console. These messages are available to all default user IDs.

Note: Depending on your user task role, you may only be able to view the hardware messages.

A message is a brief, one-line description of an event, such as a report of a Hardware Management Console failure. You can view further explanation and any recommended operator action for a single message by selecting one or more messages and then click **Details...**. The message details and any recommended operator action display, one at a time, for each selected message.

Hardware messages for all of the hardware objects are stored on the Hardware Management Console hard disk in the Message Log File. Because the Message Log File limits the number of messages to five hundred, try to view, act on, and delete messages promptly. Messages received over this limit will cause the oldest messages to be lost. Delete selected messages from the list by clicking **Delete**. A window displays for confirmation before any messages are deleted.

Note: Some messages are deleted automatically after you view the message details. These messages generally provide information only, and are deleted automatically because no further action is required.

The Hardware Messages window displays the hardware messages for the selected object. If more than one object or a group of objects was selected, a tab on the right side of the window is available for each object. Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

Hardware Messages

This window displays messages about hardware activity for selected systems on this console.

A system's hardware messages notify you of events that involve or affect its hardware or internal code. For example, a hardware message for a system may indicate a hard error or internal code error occurred, or it may indicate Problem Analysis was performed.

To display the message for an system, select the name of that system that appears on the right side of the window. Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

Tasks

All hardware messages awaiting operator action can be displayed for this system.

To promptly view, act on, and delete messages:

1. Select a message, then click **Details...** to display details.
2. If messages details are available and intervention is required, perform the operator action recommended in the details.
3. To delete the selected message, click **Delete**.

Note: This task may be view only for some user task roles.

Message Table
Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

Date
Displays the date the message was sent.

Time
Displays the time the message was sent.

Message Text
Displays the message.

Details...
To display a further explanation of the hardware activity described by the message and a recommended operator action when intervention is required, for each selected message, click **Details...**.

Delete
To delete one or more selected messages from the list, click **Delete**.

Select All Messages
To select all messages listed, click **Select All Messages**.

Deselect All Messages
To deselect all messages listed, click **Deselect All Messages**.

Cancel
To close this window and cancel the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Messages awaiting operator action

A message is displayed until an operator action causes it to be deleted.

Some messages are deleted automatically after an operator displays the message or its details, if available. These messages generally provide information only, and are deleted automatically because no further action is required.

Messages that require further action provide message details that include a recommended operator action. The message and its details remain available until an operator deletes it manually. This allows reviewing the message details to assist operator intervention. But an operator must delete the message when its information is no longer required.

Deleting messages provides greater assurance of displaying new messages as they are received.

HMC Mobile Settings

Accessing the HMC Mobile Settings task

The **HMC Mobile Settings** task provides enablement, security, and other controls for the IBM HMC Mobile for Z and LinuxONE (HMC Mobile) app for iOS and Android. Through the **HMC Mobile Settings** task, administrators can restrict usage to specific HMC users and IP addresses, restrict the app to read-only access, and more. This task also provides links to the iOS App Store or Google Play store, where you can download the HMC Mobile app to your mobile device.

To use this task, you need to log in to the HMC with either the default ACSADMIN ID, or a user ID that a system administrator has authorized to this task through customization controls in the **User Management** task. You can access this task by selecting it in the Tasks index, or through **SEARCH** on the HMC masthead.

To specify settings for the HMC Mobile app, complete the following steps.

1. Open the **HMC Mobile Settings** task.
2. Select **Enable HMC Mobile** to enable not only use of the app, but also the other app settings on the HMC Mobile Settings window.
3. Optional: If your HMC is connected to the internet, you can click one of the links to the iOS App Store or Google Play store, where you can download the HMC Mobile app to your mobile device.
4. In the User access section, select the users or templates to grant HMC Mobile and Web Services API access. Use the check box in the table header to automatically select or deselect all table entries; otherwise, use individual check boxes to enable only specific users or templates.
5. Depending on the HMC/SE version that you are using, you can limit HMC Mobile app users to read-only access through either the User actions section, or the Read-only access option. The User actions

section, which replaces the Read-only access option starting with HMC/SE Version 2.15.0, not only provides a read-only setting but also includes settings for more granular access control.

User actions
Use the **Actions are enabled** setting to enable or disable user actions. When user actions are disabled, the app is in read-only mode.

When user actions are enabled, the display includes a table of actions that users can perform through the app and, for each action, a list of users or templates with authorization to perform the action. You can edit actions in this list to grant permission to all users and templates, to no users or templates, or to only specific users and templates. Note that these users and templates also must have the equivalent task permissions assigned through the HMC **User Management** task.

Read-only access
When you select the Read-only access setting, all HMC Mobile app users can monitor system and partition events, but cannot make any changes to them, even if they have the appropriate permissions to do so on the HMC.

6. In the IP restrictions section, click the check box if you want to restrict use of the HMC Mobile app to specific IP addresses. To populate the table with IP address entries, complete the following steps.
   a. Click **ADD** to open the "Define IP address and mask" window.
   b. Select an IP address format and enter the required information for the format option that you selected.
   c. Click **ADD** to save your entry and close the "Define IP address and mask" window.
   d. Repeat, as necessary, to add more IP addresses to the table. When you have finished, go to the next section.
7. In the remaining sections of the HMC Mobile Settings window, select the password and push notification settings that you want to enable.
8. When you are finished, click **APPLY** to save your changes.

HMC Mobile Settings

The **HMC Mobile Settings** task provides enablement, security, and other controls for the IBM HMC Mobile for Z and LinuxONE (HMC Mobile) app for iOS and Android. The HMC Mobile app provides system and partition views, status monitoring, hardware messages, operating system messages, and the ability to receive push notifications from the HMC, using the existing support server connection. Through the app, users can monitor or manage systems that either run in standard mode (that is, with Processor Resource/System Manager or PR/SM), or run with Dynamic Partition Manager (DPM) enabled. They also can change activation profiles, as well as to start (or activate) and to stop (or deactivate) partitions.

Through the **HMC Mobile Settings** task, administrators can restrict usage to specific HMC users and IP addresses, restrict the app to read-only access, and more. To use this task, you need to log in to the HMC with either the default ACSADMIN ID, or a user ID that a system administrator has authorized to this task through customization controls in the **User Management** task.

When you open the **HMC Mobile Settings** task, the display includes the following sections through which you select the settings for the HMC Mobile app. You can select different mobile settings for each HMC. After you enable the app, which is disabled by default, app users can view the relevant settings that you selected for each HMC through **Security Policies** on the HMC Mobile app itself. (Specific users and IP addresses are not listed in **Security Policies**.)

IBM HMC Mobile for Z and LinuxONE
This section provides the control to enable or disable the use of the HMC Mobile app. Select **Enable HMC Mobile** to enable not only use of the app, but also the other app settings on the HMC Mobile Settings window.

This section also provides links to the iOS App Store or Google Play store, where you can download the HMC Mobile app to your mobile device. For these links to be displayed, you must be connected to the HMC through a remote browser and have access to the internet.

You must have one of the following versions installed on the mobile device that you plan to use.

- iOS 11 or later
- Android 4.4 (KitKat) or later

When you select one of these download links, a new browser tab or window opens to the HMC Mobile app page in the app store that you selected.

User access

After you select **Enable HMC Mobile**, this section displays a table that lists users or templates that you can select to grant HMC Mobile and Web Services API access. The table display includes the user or template name, type, and an indication of when a user last logged in to the HMC Mobile app.

Use the check box in the table header to automatically select or deselect all table entries; otherwise, use individual check boxes to enable only specific users or templates. Any selections that you apply through this task are also reflected in the **Customize API Settings** task.

You can scroll to view all entries, sort each table column, and filter the table entries. If you enter a text string in the Filter field, the table display is limited to only those entries with matching text, and the matching text in the Username and Type columns is highlighted in blue. To reset the table to display all entries, click **X** in the Filter field.

User actions

This section replaces the Read-only access option, starting with HMC/SE Version 2.15.0. This section not only provides a read-only setting but also includes settings for more granular access control. Use the **Actions are enabled** setting to enable or disable user actions. When user actions are disabled, the app is in read-only mode, and users can monitor system and partition events but cannot make any changes to systems or partitions, even if they have the appropriate permissions to do so on the HMC.

When user actions are enabled, the display includes a table of actions that users can perform through the app and, for each action, a list of users or templates with authorization to perform the action. You might need to hover your cursor over a table entry to view the complete list of authorized users and templates. Select **EDIT** for the action table entry to open a window through which you can further customize authority for the action. On the **Edit Action Permissions** window, you can use the radio buttons to grant permission to all users and templates, to no users or templates, or to only specific users and templates. If you select **Specific users and templates**, you might need to scroll through the table entries to see the complete list of users to which you can grant permissions. Note that these users and templates also must have the equivalent task permissions assigned through the HMC **User Management** task.

IP restrictions

After you select **Enable HMC Mobile**, this section displays the control through which you can restrict access to the HMC Mobile app to specific IP addresses. When you select the **Allow access** check box, this section displays a table through which you can add specific IP addresses and masks.

If you want to restrict access to specific IP addresses, you need to populate the table with entries by completing the following steps. Any IP addresses that you apply through this task are also reflected in the **Customize API Settings** task.

1. Click **ADD** to open the "Define IP address and mask" window.
2. On the "Define IP address and mask" window, select one of the following options for providing an IP address table entry:
   - IP address with optional mask
   - IP address and mask in Classless Inter-Domain Routing (CIDR) notation
   - Range of IP addresses

   An error message is displayed if you enter any characters other than numbers, slashes (/), colons (:), or periods (.).
3. Enter the required information for the option you selected.
4. Click **ADD** to save your entry and close the window. (If you want to close the window without saving your changes, you can click either **CANCEL**, the **X** in the upper right corner of the window, or any area off of the window but within the HMC Mobile Settings tab.)

If you need to remove any entries that you added to this table, select one or more entries and click **REMOVE**. You can use the check box in the table header to automatically select or deselect all table entries; otherwise, use individual check boxes to select only specific IP address table entries.

If you add entries to the IP addresses table and later deselect the **Allow access** check box, your entries are saved but hidden from view until you select the check box again.

HMC Mobile password
For another level of security, you can require users of the HMC Mobile app to set up a password to unlock the app every time it is opened. To set up this extra level of security, select the check box in this section. By default, the check box is not selected.

User ID password secure storage
For users' convenience, you can enable the HMC Mobile app to securely store the user's HMC password on the user's mobile device. With this setting enabled, a user can view systems managed by this HMC without having to reenter the HMC password. To permit this password storage, select the check box in this section. By default, the check box is selected.

Push notifications
To automatically notify HMC Mobile app users of system or partition events, you can enable push notifications by selecting the check box in this section. To enable this feature, your system must be under warranty or you must have a maintenance contract in place, because notifications are sent through the HMC support server connection.

Read-only access
This section is available only with HMC/SE versions prior to Version 2.15.0. When you select the Read-only access setting, all HMC Mobile app users can monitor system and partition events, but cannot make any changes to them, even if they have the appropriate permissions to do so on the HMC.

You can find more detailed help on the following elements of this window:

CANCEL
To exit the task without saving any changes you made in editable fields on the page, click **CANCEL**.

APPLY
To apply changes that you made in editable fields on the page, click **APPLY**.

HELP
To display help for the current window, click **HELP**.

Image Details

Image Details

This window displays the current instance information, task information, hypervisor information (if applicable), network information (if applicable), busy status (if applicable), and acceptable status settings for the selected image.

An *image* is a set of Central Processor Complex (CPC) resources capable of running a control program or operating system. One or more images are created during a power-on reset of the CPC. Depending on your machine type and model, you may have only logically partitioned (LPAR) mode or both LPAR mode and basic mode. When a power-on reset puts the CPC in LPAR mode, each logical partition is an image. When a power-on reset puts the CPC in a basic mode, the CPC has a single image.

- Instance Information includes the current status of the image and other information about the image's operating conditions, characteristics, and settings.

  Review the information under **Instance information**. Optionally, click **Change Options...** to change the setting of the activation profile used for activating the image from the group specified in the **Group** field.

  Task information is information about the task performed most recently on the image.
- "Status" on page 864 settings determine which image statuses are acceptable and which statuses are unacceptable. The Hardware Management Console reports when the image status becomes unacceptable.

Review the settings on the **Status** page. Optionally, make setting selections and click **Apply** to change the acceptable status settings.

- Busy Status specifies the reason why the image object is busy.

  Note: This tab is only available when an object is busy.

- Firmware includes firmware network configuration settings for the selected zAware image profile. Optionally, enter new firmware network configuration settings and click **Apply** to change the new firmware settings.

  Note: This tab is only available for z13, zEC12, and zBC12.

Apply
To save changes you made to the image's acceptable status settings, click **Apply**.

Change Options...
To change the setting of the activation profile used for activating this instance of the image from the selected group, click **Change Options**. You can have different activation profiles set for a single image by invoking the **Image Details** task from different system defined or user-defined custom groups containing the object and selecting **Change Options...**.

The **Change Options...** button is not available if the **Image Details** task is invoked from Tasks Index. It is also not available if the user does not have permission to the **Change Object Options** task. Your access administrator can grant permission to the **Change Object Options** task by using the **User Management** task.

Cancel
To close the window without saving changes you made to the image's acceptable status settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more information on the Image Details tabs:

Instance Information

This page displays the current instance information for the selected image.

Instance information includes the current status of the image and other information about the image's operating conditions, characteristics, and settings.

Group

Displays the name of the group that contains the instance of the image to which the instance information applies.

More than one group can contain a unique instance of the same image. This allows assigning different activation profiles to different instances of the image.

Note: The **Group** field is blank if the **Image Details** task is invoked from Tasks Index.

Activation profile

Identifies the activation profile used for activating this instance of the image.

Optionally, click **Change Options...** to change the setting of the activation profile used for activating this instance of the image.

Note: The **Activation profile** field is blank if the **Image Details** task is invoked from Tasks Index.

Last used profile
Identifies the activation profile used for the most recent image activation.

Sysplex name

Displays the name of the particular operating system's complex (Sysplex).

A Sysplex is a collection of images that cooperate, using certain hardware and software products, to process workloads. If the image is running a particular operating system other than z/VM operating system, this field displays the name of the particular operating system's complex (Sysplex), if any, of which the image is a member.

Secure Execution for Linux
Indicates whether the selected image is using (On) or not using (Off) the Secure Execution installed feature.

System recovery boost
Indicates whether additional CP capacity during particular system recovery operations is On or Off.

VMSSI name

Displays the name of the particular Single System Image (SSI).

An SSI is a collection of images that cooperate, using certain hardware and software products, to process workloads. If the image is running a z/VM operating system (version 6.2), this field displays the name of the particular SSI, if any, of which the image is a member.

Operating system
Displays the name of the operating system, if available, currently loaded for the image.

CPU LPAR cluster name
In the Image profile, the CPU LPAR cluster name is used by the operating system as a way to group images

Operating system type
Displays the type of the operating system, if available, currently loaded for the image.

Operating system level
Displays the version and level of the operating system, if available, currently loaded for the image.

Task name
Displays the name of the task most recently performed on the image.

Task status
Displays the status of the task most recently performed on the image.

Lockout disruptive tasks

To set the disruptive task lockout for the image:

- To lock it (to prevent using the Hardware Management Console to perform disruptive tasks on the image), click **Yes**.
- To unlock it (to allow using the Hardware Management Console to perform disruptive tasks on the image), click **No**.
- Click **Apply** to make the new settings take effect.

Some Hardware Management Console tasks can be *disruptive*. Performing a disruptive task on the Central Processor Complex (CPC) or an image may disrupt its operations. For example, activating the CPC and loading an image can be disruptive.

Setting **Lock out disruptive tasks** controls whether you can perform disruptive tasks on an object. You can lock an object to prevent accidentally performing disruptive tasks on it, then unlock the object only when you want to perform a disruptive task on it.

Note: When you use the Hardware Management Console to set an object's disruptive task lockout, the setting affects only disruptive tasks that are started manually by console operators using the Hardware Management Console (locally or remotely) or Web server sessions. The setting does *not* affect disruptive tasks started automatically or from other sources. For example, the setting does not affect tasks started by scheduled operations, by Operations Management commands, or by console operators using the Support Element console of the CPC.

Status

This page displays the current acceptable status settings for the image. **Acceptable status** settings determine which image statuses are acceptable and which statuses are unacceptable.

Use the "Acceptable status" on page 864 check boxes to change the settings:

- A check mark in a check box indicates an acceptable status.
- An empty check box indicates an unacceptable status.
- To change one setting to the other, click once on the check box.

The Hardware Management Console continuously monitors the status of each defined image and compares it to the image's acceptable status settings.

You can find the status for images in the Status column of the image's work pane table.

Setting the image's acceptable status settings allows you to control which statuses are reported as exceptions:

- Acceptable status, indicated by check marks in their check boxes, are *not* reported as exceptions.
- Unacceptable status, indicated by empty check boxes, are reported as exceptions.

You can find more detailed help on the following elements of this page:

Acceptable status

This field specifies which statuses are acceptable for the image. Select the statuses you want as acceptable. Then click **Apply** to save your changes and update the image status.

Operating
All CPs are operating.

Not operating
No CPs are operating, but the exact status of the CPs vary.

Exceptions
At least one CP is operating, but at least one CP is not operating.

Not activated
The image is not activated

Save as default

To allow you to change the acceptable status for all of the current objects defined with the same status type, select **Save as default**. After you click **Apply**, a message window appears confirming that you want to proceed with this operation.

Busy Status

This page specifies the user ID, the user's location, and the task that caused the object to become busy.

Note: This tab is only available when an object is busy.

Firmware

Note: This tab is only available for z13, zEC12, and zBC12.

Use this window to customize firmware network configuration settings for the selected logical partition in zAware operating mode. The firmware network configuration settings are:

Host name
Use this field to specify the host name for the selected firmware logical partition.

A host name can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a host name are alphanumeric characters, period (.), colons (:), and hyphens (-).

Master user ID
Use this field to specify the master user ID for the selected firmware logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a master user ID name are numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Use this field to specify the master password for the master user ID you specified.

A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Use this field to specify again the same master password you specified in the **Master password** field.

Default gateway
Use this field to specify the default gateway IPv4 or IPv6 address.

The icons perform the following functions in the Network Adapters and DNS Server table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

New...
Select this operation to add a new IP address type and CHPID/VLAN details for the selected firmware logical partition.

Edit...
Select this operation to edit the selected IP address type and CHPID/VLAN details for the selected firmware logical partition.

Delete...
Select this operation to delete the selected IP address type and CHPID/VLAN details for the selected firmware logical partition.

Use the Network Adapter table to view and change an IP address type and detail settings for the selected network adapters. You can add, edit, or remove the IP address type and detail settings using the **Select Action** list from the table tool bar. A maximum of 100 network adapters can be specified.

CHPID
Displays the CHPID for the selected firmware logical partition.

VLAN
Displays the VLAN for the selected firmware logical partition.

IP address
Displays the IPv4 or IPv6 address for the selected firmware logical partition. Also, indicates DHCP or Link Local if that is the specific IP address type.

Mask/Prefix
Displays the Mask/Prefix for the IPv4 or IPv6 address specified.

The DNS Servers table displays the IPv4 or IPv6 address for the selected firmware logical partition. You can add, edit, or remove the IP address using the **Select Action** list from the table tool bar. A maximum of 2 DNS addresses can be specified.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.jkltoys.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all host names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

CHPID
Displays the CHPID for the selected firmware logical partition.

VLAN
Displays the VLAN for the selected firmware logical partition.

IP address
Displays the IPv4 or IPv6 address for the selected firmware logical partition. Also, indicates DHCP or Link Local if that is the specific IP address type.

Mask/Prefix
Displays the Mask/Prefix for the IPv4 or IPv6 address specified.

You can find more detailed help on the following elements of this window:

New/Edit Network Adapters Entry

Use this window to add or edit the CHPID and VLAN for the selected firmware logical partition. If the IP address selected is a static IPv4 or IPv6, you can edit or add the corresponding IP address.

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Add/Edit DNS Entry

Use this window to add or edit the static IPv4 or IPv6 address configured for the selected firmware logical partition.

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Input/Output (I/O) Configuration

Accessing the Input/Output (I/O) Configuration task

The input/output (I/O) configuration of the central processor complex (CPC) is the set of all I/O devices, control units, and channel paths available to the CPC. During each power-on reset of the CPC, an input/output configuration data set (IOCDS) is used to define the I/O configuration to the channel subsystem.

You must build an IOCDS and store it on the CPC's Support Element before you can use it during power-on reset to define the CPC's I/O configuration. You can build an IOCDS by using an input/output configuration program (IOCP):

- An IOCP may be available as a batch program with your operating system.

  For information about using the IOCP, see: *Input/Output Configuration Program User's Guide for ICP IOCP*.
- A stand-alone IOCP also is available with the Support Element.

  For information about using the stand-alone IOCP, see: *Stand-Alone Input/Output Configuration Program User's Guide*.

This task allows you to start the support processor input/output configuration program (IOCP) for the selected CPC.

To start the stand-alone IOCP:

1. Open the **Input/output (I/O) Configuration** task.

   The Input/Output Configuration window displays.
2. Click **Options** from the menu bar to display the following menu options:
   - Enable Write Protection
   - Disable Write Protection
   - Copy Configuration
   - Export Source File
   - Import Source File
   - Open Source File
   - Delete Source File
   - Print Data Set Report
   - Write Report to Tape
   - Build Data Set
   - Disassemble Data Set.
3. Click **View** from the menu bar to display the following menu options:
   - Channel Path Configuration
   - Partition Images Configured
   - Dynamic Information
   - Configuration Program Level
   - Support I/O Mask.
4. Click **Tools** (Service role only) from the menu bar to display the following menu options:
   - Save Data Files on Hardware Management Console...
   - Save Data Files to USB Flash Memory Drive
   - Restore Data Files from Hardware Management Console...
   - Restore Data Files from the USB Flash Memory Drive...
   - Restore only IOCDS Data Files from USB Flash Memory Drive
   - Restore Only Channel Configuration Files from USB Flash Memory Drive
   - Erase Data Files from Hardware Management Console.
5. Click Exit from the **Options** menu bar to exit the window.

Input/Output Configuration

Use the **Input/Output Configuration** window to manage and modify input/output (I/O) configuration source files and data sets for the selected central processor complex (CPC). Use this window also to display information that defines the channel paths and logical partitions associated with the I/O configurations, and the status of configuration source files and data sets.

A configuration source file and an input/output configuration data set (IOCDS) are associated with each I/O configuration.

The source file is the input to the stand-alone I/O configuration program (IOCP). The IOCP uses a configuration source file to create or build an IOCDS.

The IOCDS is used during a power-on reset to define the I/O configuration program for the channel subsystem. The **Active input/output configuration data set (IOCDS)** field identifies the IOCDS used during the most recent power-on reset or selected by a dynamic activation from an operating system.

The **IOCDS matching hardware system area (HSA)** section displays the identifier of the IOCDS, if any, that matches the source most recently used to dynamically create the I/O definition currently in the channel subsystem HSA of the selected CPC, and then written to its support element. That is, the field identifies an IOCDS that supports dynamically changing the I/O definition defined by the IOCDS.

Note: If the I/O definition most recently created in the HSA was not written to the support element, then it may not match the I/O definition of the IOCDS identified by this field.

Click **Options** on the menu bar. The actions available for managing and modifying configuration files and data sets are listed below. Select an action from the following list:

“Enable Write Protection” on page 870
“Disable Write Protection” on page 870
“Copy Configuration” on page 870
“Export Source File” on page 871
“Import Source File” on page 872
“Export to HMC USB Flash Memory Drive” on page 872
Open Source File to edit the selected I/O configuration source file
Delete Source File to delete the selected I/O configuration file
“Print to printer” on page 873
“Write Report to Tape” on page 874
“Build Data Set” on page 875
“Disassemble Data Set” on page 876

Click **View** on the menu bar. The actions available for displaying information and status are listed below. Select an action from the following list:

“Channel Path Configuration” on page 876
“Partition Images Configured” on page 887
“Dynamic Information” on page 888
Configuration Program Level to display the version, release, and level of the stand-alone IOCP available on your Support Element .
“Supported I/O Mask” on page 889

Click **Tools** on the menu bar. The actions available for saving and restoring data files on the Hardware Management Console are listed below. Select an action from the following list:

“Save Data Files on Hardware Management Console” on page 889
Save Data Files to USB Flash Memory Drive to copy the IOCDS data files and channel configuration files from the Support Element console to the USB Flash Memory Drive
“Restore Data Files on Hardware Management Console” on page 889
Restore Data Files from the USB Flash Memory Drive to restore the IOCDS data files and channel configuration files from the Support Element console to the USB Flash Memory Drive

Restore only IOCDS Data File from USB Flash Memory Driveto restore only IOCDS data files from the Support Element console to the USB Flash Memory Drive

Restore only Channel Configuration Data File from USB Flash Memory Drive to restore only the channel configuration files from the Support Element console to the USB Flash Memory Drive

Erase Data File from Hardware Management Console to erase the IOCDS data file from the Hardware Management Console's hard drive. The fully qualified path name for the data files must be specified at the Target path name entry field.

You can find more detailed help on the following element of this window:

I/O configuration table

Select an input/output (I/O) configuration data set (IOCDS) to work on from the list. The list provides the following information about each data set:

Data Set
Displays the two-character identifier of an IOCDS. There are 5 data sets (A0, A1, A2, A3, and D0).

Name
Displays the eight-character name of an IOCDS. This name primarily identifies the data set to users, while the data set identifier is used by the system.

A data set name is specified by the first eight characters from the **MSG1=** keyword of the **ID** statement in the configuration source file.

Write Protected
Indicates whether write protection is enabled for the IOCDS. Enabled write protection prevents the IOCDS from being overlaid with a new IOCDS written by batch or the stand-alone IOCP.

No
Indicates write protection is disabled.

Yes
Indicates write protection is enabled.

Date
Displays the month, day, and year that the IOCDS was built.

Time
Displays the hour, minute, and second (continental time) that the IOCDS was built on the indicated date.

Data Set Status
Indicates the status of the I/O configuration data set.

Active
Indicates the data set was used during the most recent power-on reset or was selected by a dynamic activation from an operating system.

Valid
Indicates the data set contains no errors and can be used at power-on reset.

Invalid
Indicates the data set is not usable at power-on reset. This occurs when IOCP is currently writing to the IOCDS or the IOCDS was written in preparation for a CPC upgrade and will be unusable until the CPC is upgraded to the type of CPC supported by the IOCDS.

Source Status
Indicates the status of the I/O configuration data set source that is used in the build process by the stand-alone IOCP.

Empty
Indicates no source. This occurs when you delete the source file and when batch IOCP writes an IOCDS.

Imported
Indicates the source file was imported from the USB flash memory drive or FTP.

Modified
Indicates the source file has been changed by the editor.

Verified
Indicates the source file has no errors from the build process.

Warnings
Indicates the source file has warning or caution messages from the build process.

Errors
Indicates the source file has error messages from the build process. No IOCDS is written and the IOCDS remains as it was before the build.

Unknown
Indicates an error condition.

Version
Indicates the version of the IOCP that built the data set.

Enable Write Protection

Select **Enable Write Protection** to prevent modification of the selected input/output configuration data set (IOCDS) and the configuration source file.

With write protection enabled, the IOCDS cannot be modified using the build function of the input/output configuration program (IOCP), and the IOCDS cannot belong to the target configuration of the copy function. With write protection enabled, the configuration source file cannot be the target of the following functions:

- copy configuration
- import source
- open source
- delete source
- build
- disassemble

Disable Write Protection

Select **Disable Write Protection** to allow modification of the selected input/output configuration data set (IOCDS) and the configuration source file.

With write protection disabled, the IOCDS may be modified using the build function of the input/output configuration program (IOCP), and the IOCDS can belong to the target configuration of the copy function.

With write protection disabled, the source file may be modified using the open function, and the source file can be the target of the import or disassemble function or belong to the target configuration of the copy function.

Copy Configuration

Select **Copy Configuration** to copy an input/output (I/O) configuration.

The copy function duplicates the source file and the input/output configuration data set (IOCDS) of the source configuration and replaces the corresponding files of the target configuration. The target I/O configuration cannot be write-protected.

Source Configuration
Displays the identifier of the source configuration data set

Target Configuration
Select the identifier of the target configuration data set.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Source File

Select **Export Source File** to export a configuration source file from the Support Element hard disk to an FTP destination.

The export function copies a source file from the Support Element to an FTP destination.

Verify that the name in the **Source configuration** identifies the configuration that owns the source file you want to export.

Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Source configuration data set
Displays the identifier of the source configuration data set.

Source configuration data set name
Displays the name of the source configuration data set.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Export** drop-down, select **From Remote Server**. The Export Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Export window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Export
To export configuration data files to an FTP destination, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Import Source File

Select **Import Source File** to copy a configuration source file from one medium to the Support Element.

The import function copies a source file from the FTP destination to the Support Element hard disk.

Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Target configuration data set
Displays the identifier of the target configuration data set

Target configuration data set name
Displays the name of the target configuration data set

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import data configuration files to an FTP destination, click **Import**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export to HMC USB Flash Memory Drive

Select **Export Source File** to export a configuration source file from the Support Element hard disk to a USB Flash Memory Drive destination.

The export function copies a source file from the Support Element to a USB Flash Memory Drive destination.

Verify that the name in the **Source configuration** identifies the configuration that owns the source file you want to export. Use the **Target File name** field to type the fully qualified name and extension of the file to receive the configuration source file on the USB Flash Memory Drive.

Source configuration data set
Displays the identifier of the source configuration data set.

Source configuration data set name
Displays the name of the source configuration data set.

Target file name

Specify the fully qualified file name for the target file. For example:

```
DriveDirectoryfilename.ext
```

Additional functions on this window include:

OK
To export configuration data files to a HMC USB Flash Memory Drive destination, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Import to HMC USB Flash Memory Drive

Select **Import Source File** to import a configuration source file to the Support Element hard disk from a USB Flash Memory Drive destination.

The import function copies a source file to the Support Element to a USB Flash Memory drive destination.

Verify that the name in the **Source configuration** identifies the configuration that owns the source file you want to export. Use the **Target File name** field to type the fully qualified name and extension of the file to receive the configuration source file on the USB flash memory drive.

Source configuration data set
Displays the identifier of the source configuration data set.

Source configuration data set name
Displays the name of the source configuration data set.

Target file name

Specify the fully qualified file name for the target file. For example:

```
DriveDirectoryfilename.ext
```

Additional functions on this window include:

OK
To import configuration data files from a HMC USB Flash Memory Drive destination, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Print to printer

Select **Print to Printer** to specify the options necessary to print a configuration report.

This function works only with printers that accept standard line printer commands.

You must specify the device number of the printer, the number of lines to print per page, and whether to end the process upon a data check error. The printer must be a channel-attached device and must be in the active IOCDS and must be available to the logical partition you are using to run IOCP.

Use **Continue if data check errors occur** to indicate whether you want to stop printing if the printer receives a character that cannot be printed. A printer cannot print characters that are not recognized, or are not in the printer character set. Select this option if you want data check errors ignored. Otherwise, leave this selection blank.

Printer address
Specify the device number of the printer you want to use in the field. The printer's device number must be configured in the active IOCDS. The active IOCDS is the one that matches the current I/O configuration of the central processor complex (CC).

Lines per page
Specify the maximum number of lines printed on each page. The default value for this field is 55 lines per page. The IOCP uses the default value if the field is blank. The IOCP uses a value of 20 if you specify a value less than 20.

Continue if data check erros occur
To continue printing even with data check errors, click **Continue if data check errors occur**. When a character that cannot be printed is received, it is replaced with a blank and printing continues.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected functions, click **Cancel.**

Help
To display help for the current window, click **Help**.

Write Report to Tape

Select **Write Report to Tape** to specify the options necessary to write a formatted I/O configuration report to tape.

You must specify the device number of the tape drive, the file number location for the file on the tape, and the number of lines to include per page of the configuration report. The tape drive must be a channel-attached device and must be in the active IOCDS and must be available to the logical partition you are using to run IOCP.

Tape drive address
Specify the device number of the tape drive you want to use in the field. The device number must be configured in the active IOCDS. The active IOCDS is the one that matches the current I/O configuration of the central processor complex (CPC).

File number
Specify the number of the physical file on the tape (such as 1,2, or 3) where you want to store the file. IOCP issues a Rewind command followed by forward space file commands to position the tape to the requested file.

Lines per page
Specify the maximum number of lines to include per page of the I/O configuration report. The default value for this field is 55 lines per page. The IOCP uses the default value if the field is blank. The IOCP uses a value of 20 if you specify a value less than 20.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Build Data Set

Select **Build Data Set** to run the stand-alone input/output configuration program (IOCP) and create an input/output configuration data set (IOCDS).

Note: This action cannot be used with an input/output (I/O) configuration that is write-protected.

The IOCP will build the IOCDS from the statements in the source file associated with the selected I/O configuration. The IOCP checks the syntax of the source file statements and validates the source file information. The IOCP imbeds error messages in the source file upon detecting errors.

If no terminal errors are encountered, the IOCP writes the IOCDS to the Support Element hard disk. Otherwise, edit the source file to correct the errors if it is not a dynamic I/O configuration. Conditions that result in warning or caution messages from the IOCP will not cancel the build.

If you select the option to print a report of the built IOCDS on a system printer, the system printer must be configured in the active IOCDS and available to the logical partition you are using to run IOCP.

Send output to printer
To send the report of the built IOCDS to the system printer select **Send output to printer**. The system printer must be configured in the active IOCDS and available to the logical partition you are using to run the IOCP.

Printer address
Specify the device number of the printer you want to use in this field. The printer's device number must be configured in the active IOCDS. The active IOCDS is the one that matches the current I/O configuration of the central processor complex (CPC).

Lines per page
Specify the maximum number of lines printed on each page. The default value for this field is 55 lines per page. The IOCP uses the default value if the field is blank. The IOCP uses a value of 20 if you specify a value less than 20.

Continue if data check error occur
To continue the build even with data check errors, select **Continue if data check errors occur**. When a character that cannot be printed is received, it is replaced with a blank and printing continues.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Input/Output Configuration Progress

The **Input/Output Configuration** window indicates the progress of the requested stand-alone IOCP task.

Start time
Displays the time at which the task begun

Elapsed time
Displays the amount of time that has elapsed since the task began

Current step
Displays the current step number being performed

Total number of steps
Displays the number of steps to be performed for the requested task

Status messages
Displays messages indicating the step being performed and the final result of the requested task

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Disassemble Data Set

Select **Disassemble Data Set** to run the stand-alone IOCP to generate a new I/O configuration source file based on the selected IOCDS. The new source file contains the full configuration described in the original customer IOCP input file and is the logical equivalent of the input file. However, it will not appear as it did in the original. Since IOCP does not save comments, comments do not appear in the source file.

Channel Path Configuration

Use the **Channel Path Configuration** window to select a channel path and the type of channel path information you want to view. The Channel path configuration table lists the channel paths that exist in the selected IOCDS.

Select a channel path, then select an action to display the type of channel path information you want to view. You can display information for control units or input/output (I/O) devices assigned to the channel path, or for names of logical partitions that have access to the path.

Click **View** on the menu bar. The actions available for displaying information are listed below. Select an action from the following list:

"Channel Subsystem Information" on page 878
"CHPID Information" on page 881
"Control Unit Information" on page 882
"Device Information" on page 884
"Image Candidate List" on page 885
"Image Access List" on page 885

Click **Search** on the menu bar. The actions available for searching information are listed below. Select an action from the following list:

"PCHID" on page 878
"CSS.CHPID" on page 878

The channel path information displayed is associated with keywords on the IOCP CHPID statement. The CHPID statement defines the characteristics of a channel path.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

You can find more detailed help on the following elements of this window:

Channel path configuration table

Select a channel path from the list to view more information about the channel path including the control units and devices assigned to the channel path.

PCHID=
The PCHID keyword identifies the physical channel identification number, if any, associated with the channel path.

TYPE=
The TYPE keyword identifies the mode of input/output (I/O) operation for the channel path.

CSS
The CSS parameter indicates the channel subsystems a channel path is in. This parameter is set in the PATH keyword of a CHPID statement. If a channel path is in multiple channel subsystems and

therefore defined as spanned, **SPAN** is displayed. To display the specific channel subsystems a spanned channel path is in, use the Channel Subsystem Information view.

CHPID
This number identifies the channel path identifier. A channel path identifier is assigned by the PATH keyword of a CHPID statement.

SWITCH=
The SWITCH keyword identifies a number, if any, associated with an ESCON Director or FICON Director to support dynamic connections of the corresponding channel path identifier through the Director. It is valid for ESCON and FICON channel types only.

CHPARM=
The CHPARM keyword indicates how the channel path is to operate. Only certain channel path types support CHPARM. Also, for some channel path types that support CHPARM, only non-zero values are displayed.

PNETID
Displays the physical network identifier for the channel path.

TYPE keyword

The TYPE keyword identifies the mode of input/output (I/O) operation for the channel path.

A channel path may operate in one of the following modes:

CBY
Indicates a channel attached to an ESCON converter and operating in byte multiplexer mode. CBY channel paths operate the same as parallel channels operating in byte multiplexer mode.

CFP
Indicates coupling facility peer channel.

CIB
Indicates Coupling over Infiniband channel.

CNC
Indicates an ESCON channel path, and that all attached control units and I/O devices support the ESCON Architecture protocol.

CTC
Indicates an ESCON channel path that permits channel-to-channel communications.

CVC
Indicates a channel attached to an ESCON converter and operating in block multiplexer mode. CVC channel paths operate the same as parallel channels operating in block multiplexer mode.

FC
Indicates a native FICON channel path, and that all attached control units and I/O devices support the FICON Architecture protocol.

FCP
Indicates Fibre Channel Protocol channel for SCSI Devices.

ICP
Indicates Internal Coupling facility peer channel.

IQD
Indicates internal queued direct communication (HiperSockets).

OSC
Indicates an OSA channel that operates as an OSA-Express integrated console controller (OSA-ICC) for 3270 support.

OSD
Indicates an OSA channel for QDIO architectures.

OSE
Indicates an OSA channel for non-QDIO architectures.

OSM
Indicates an OSA channel for intra node management network (INMN).

OSN
Indicates an OSA for network control program (NCP) channel.

Channel Path Configuration Search

Select **Channel Path Configuration Search** to search for a channel path using a PCHID number.

PCHID
Select **PCHID** to search for a channel path using a PCHID number. Specify the PCHID number associated with the channel path you want to find. If a channel path does not have a PCHID (for example, channel path types ICP and IQD), you must use the CSS.CHPID option when searching for the channel path. Also, note that channel paths without a PCHID are always displayed at the bottom of the Channel Path Configuration window.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Channel Path Configuration Search

Select **Channel Path Configuration Search** to search for a channel path using a combination of CSS and CHPID numbers.

CSS.CHPID
Specify the CSS number (in the range 0-F) associated with the channel path you want to find. If a channel path is available to multiple channel subsystems and therefore spanned, the CSS value on the Channel Path Configuration window is SPAN. Specify 's' for the CSS number when searching for a spanned channel path. Specify the CHPID number associated with the channel path you want to find.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Channel Subsystem Information

Select **Channel Subsystem Information** to display the logical channel subsystem information for the selected channel path.

The channel subsystem information displayed is associated with keywords on the IOCP CHPID statement. The CHPID statement defines the characteristics of a channel path.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Channel subsystems
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Channel Subsystem Selection

The **Channel Subsystem Selection** window is displayed when a spanned channel path is selected along with an action to display information that must be associated with a single channel subsystem.

The channel path you selected is spanned (that is, it is in multiple channel subsystems). The action you chose requires that a single channel subsystem (CSS) be selected for the channel path before any information is displayed. Select a CSS from the list and click **OK**.

If the selected channel path belongs to a single CSS and is not spanned, this window is not displayed.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword

Channel subsystems
Displays the channel subsystems a channel path is in. Select a CSS.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Select a Link Address

The **Select a Link Address** window is displayed when a channel path is selected that has multiple link addresses and an action is chosen to display information for the control units or input/output (I/O) devices attached to the path.

The channel path you selected has multiple control units with different link addresses The channel path is connected to an ESCON or FICON director. The action you chose requires that a single link address be selected for the channel path before any information is displayed. Select a link address from the list and click **OK**.

If the selected channel path does not have multiple link addresses, this window is not displayed.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword

Link address
Displays each link address associated with the selected channel path.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Select Control Unit

The **Select Control Unit** window is displayed so you can select the control unit for which you want to display device information.

The control units listed are all associated with the same composite path (CSS.CHPID.LINK) you selected. Select a control unit from the list and click **OK**.

Control units are defined by IOCP CNTLUNIT statements. The following columns identify information provided by the parameters and keywords of the CNTLUNIT statements. The column headings are the same as the parameters and keywords, unless stated otherwise.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Link address
Displays either the only link address associated with the channel path or the link address you selected. A link address is specified by the LINK keyword on the IOCP CNTLUNIT statement.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Control unit table

The control unit table contains a list of control units associated with the selected path (CSS.CHPID.LINK). The column headings are the same as the keywords on the IOCP CNTLUNIT statement. Select a control unit.

CUNUMBR=
The CUNUMBR keyword identifies the control unit number. The control unit number is a unique, arbitrary identifier for the control unit. Control unit numbers are within the hexadecimal range of 0000 to FFFE, and are assigned by the person who edited the statements.

UNIT=
The UNIT keyword identifies the type of control unit. The control unit type is an alphameric identifier, of up to eight characters.

SHARED=
The SHARED keyword indicates the level of concurrency of input/output requests that a parallel channel allows for a control unit. IOCP sets the control unit type (1 or 2) based on the SHARED parameter on the IOCP CNTLUNIT statement. **Y** indicates a type 1 control unit. **N** indicates a type 2 control unit. The SHARED keyword is meaningful only for TYPE=CVC channel paths but IOCP assigns a level of concurrency for all control units. Therefore, a **Y** or **N** is displayed for all channel path types to indicate whether the control unit is type 1 or 2.

PROTOCL=
The PROTOCL keyword indicates the interface protocol used by a control unit when operating with parallel channel paths to which it is attached. The PROTOCL keyword is meaningful only for TYPE=CVC channel paths. A value of **D** specifies the direct-coupled interlock (DC interlock) protocol. A value of **S** specifies the data streaming protocol as a maximum data rate of 3.0 megabytes per second. A value of **S4** specifies the data streaming protocol at a maximum data rate of 4.5 megabytes per second.

UNITADD=
The UNITADD keyword identifies the ranges of addresses of I/O devices recognized by the control unit.

Multiple ranges of addresses are displayed on separate lines under the first line. The other control unit information is the same for each address range, and is not repeated on the additional lines.

CUADD=
The CUADD keyword identifies the logical address of the control unit.

PATH=
The PATH keyword identifies the channel paths to which the control unit is attached. A control unit may be attached to 1 to 8 channel paths.

CHPID Information

Select **CHPID Information** to display information about a channel path for a specific channel subsystem.

If the selected channel path belongs to more than one channel subsystem (CSS), you will need to select a single CSS before the CHPID information is displayed.

The CHPID information displayed is associated with keywords on the IOCP CHPID statement. The CHPID statement defines the characteristics of a channel path.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystem a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

LSYSTEM
Displays the name of the local system if the selected channel path type is CIB. The local system name is assigned by the LSYSTEM keyword on the IOCP ID statement.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

CHPID information table

Displays information about the selected channel path.

Shared
Indicates whether the channel path can be configured on by multiple logical partitions at the same time. **Yes** indicates the channel path is shared. **No** indicates it is not shared. The Shared characteristic is set by the SHARED, PARTITION, NOTPART, IOCLUSTER, and PATH keywords.

REC
The REC parameter indicates whether a channel path is reconfigurable between logical partitions. **Yes** indicates the channel path is reconfigurable. **No** indicates it is not reconfigurable. This parameter is set in the PARTITION keyword.

PARTITION= IOCLUSTER=
If the channel path is not shared, the name of the single logical partition it is assigned to is displayed. If the channel path is shared and the IOCLUSTER= keyword was specified, the I/O cluster name is displayed. If the channel path is shared and the IOCLUSTER= keyword was not specified, nothing is displayed.

The following additional information is displayed only for CIB channel path types.

AID=
Displays the adapter identifier (AID) associated with the host channel adapter on which this channel path is defined. An AID is assigned by the AID keyword.

PORT=
Displays the port number on the host channel adapter to which this channel path is defined. A port number is assigned by the PORT keyword.

CSYSTEM=
Displays the name of the system that connects to the selected channel path. A system name is assigned by the LSYSTEM keyword on the IOCP ID statement. The name of the connecting system for this channel path is assigned by the CSYSTEM keyword.

CPATH
Displays the channel subsystem and CHPID identifier (CSS.CHPID) to which the selected channel path is connected. The connecting channel path information is assigned by the CPATH keyword.

Control Unit Information

Select **Control Unit information** to display the control units attached to the selected channel path.

If the selected channel path belongs to more than one channel subsystem (CSS), you will need to select a single CSS before a list of control units is displayed. Also, if the channel path uses multiple link addresses on a Director, you will need to select a single link address. Then all the control units assigned to the composite path CSS.CHPID.LINK are displayed.

Control units are defined by IOCP CNTLUNIT statements. The following columns identify information provided by the parameters and keywords of the CNTLUNIT statements. The column headings are the same as the parameters and keywords, unless stated otherwise.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Link address
Displays either the only link address associated with the channel path or the link address you selected. A link address is specified by the LINK keyword on the IOCP CNTLUNIT statement.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Control unit table

The control unit table contains a list of control units associated with the selected path (CSS.CHPID.LINK). The column headings are the same as the keywords on the IOCP CNTLUNIT statement.

CUNUMBR=
The CUNUMBR keyword identifies the control unit number. The control unit number is a unique, arbitrary identifier for the control unit. Control unit numbers are within the hexadecimal range of 0000 to FFFE, and are assigned by the person who edited the statements.

UNIT=
The UNIT keyword identifies the type of control unit. The control unit type is an alphameric identifier, of up to eight characters.

SHARED=
The SHARED keyword indicates the level of concurrency of input/output requests that a parallel channel allows for a control unit. IOCP sets the control unit type (1 or 2) based on the SHARED parameter on the IOCP CNTLUNIT statement. **Y** indicates a type 1 control unit. **N** indicates a type 2 control unit. The SHARED keyword is meaningful only for TYPE=CVC channel paths but IOCP assigns a level of concurrency for all control units. Therefore, a **Y** or **N** is displayed for all channel path types to indicate whether the control unit is type 1 or 2.

PROTOCL=
The PROTOCL keyword indicates the interface protocol used by a control unit when operating with parallel channel paths to which it is attached. The PROTOCL keyword is meaningful only for TYPE=CVC channel paths. A value of **D** specifies the direct-coupled interlock (DC interlock) protocol. A value of **S** specifies the data streaming protocol as a maximum data rate of 3.0 megabytes per second. A value of **S4** specifies the data streaming protocol at a maximum data rate of 4.5 megabytes per second.

UNITADD=
The UNITADD keyword identifies the ranges of addresses of I/O devices recognized by the control unit.

Multiple ranges of addresses are displayed on separate lines under the first line. The other control unit information is the same for each address range, and is not repeated on the additional lines.

CUADD=
The CUADD keyword identifies the logical address of the control unit.

PATH=
The PATH keyword identifies the channel paths to which the control unit is attached. A control unit may be attached to 1 to 8 channel paths.

Device Information

Select **Device Information** to display the information specified for the parameters and keywords of IODEVICE statements.

If the selected channel path belongs to more than one channel subsystem (CSS), you will need to select a single CSS before a list of control units is displayed. Also, if the channel path uses multiple link addresses on a Director, you will need to select a single link address. Then all the control units assigned to the composite path CSS.CHPID.LINK are displayed. If the composite path has multiple control units, you will need to select a single control unit. Then all the devices associated with the selected control unit and path are displayed.

Input/output devices are defined by IOCP IODEVICE statements. The following columns identify information provided by the parameters and keywords of the IODEVICE statements. The column headings are the same as the parameters and keywords, unless stated otherwise.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Device table

The device table contains a list of devices assigned to the selected control unit. The column headings are the same as the keywords on the IOCP IODEVICE statement.

UNITADD=
The UNITADD keyword identifies the physical unit address assigned to the I/O device. A physical unit address identifies an I/O device to the control units to which it is attached.

ADDRESS=
The ADDRESS keyword identifies the device number.

SCHSET=
The SCHSET keyword identifies the subchannel set in the selected CSS to which this device belongs.

UNIT=
The UNIT keyword identifies the type of I/O device. The device type is an alphameric identifier, of up to eight characters.

MODEL=
The MODEL keyword identifies the model number of the I/O device. The model number is an alphameric identifier, of up to four characters.

STADET=
The STADET keyword indicates whether the Status Verification Facility is enabled. A value of **Y** indicates the Status Verification Facility is enabled. A value of **N** indicates the Status Verification Facility is not enabled.

TIMEOUT=
The TIMEOUT keyword indicates whether the I/O interface time-out function is active. A value of **Y** indicates the I/O interface time-out function is active. A value of **N** indicates the I/O interface time-out function is not active. The TIMEOUT keyword is meaningful only for TYPE-CVC channel paths. Devices assigned to TYPE=CBY channel paths always have the time-out function active. For all other channel path types, the timeout function is not active.

Image Candidate List

Select **Image Candidate List** to display the logical partitions for a specific channel subsystem that can access the channel path.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Image candidate list table

MIF image ID
The MIF image ID within the CSS that is associated with the logical partition.

Partition name
The name of a logical partition in the image candidate list for the selected channel path and CSS.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Image Access List

Select **Image Access List** to display the logical partitions for a specific channel subsystem that have the channel path configured online at partition activation following initial power-on reset (POR) of the IOCDS.

After the initial POR of the IOCDS, PR/SM LPAR retains which logical partitions will have the channel path configured online at partition activation following subsequent PORs with the same IOCDS.

The image access list displayed is associated with keywords PARTITION, NOTPART, SHARED, and PATH on the IOCP CHPID statement.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Image access list table

MIF image ID
The MIF image ID within the CSS that is associated with the logical partition. For a null image access list, this field is left blank.

Partition name
The name of a logical partition in the image access list for the selected channel path and CSS. If the channel path has a null image access list, a zero is displayed. A null image access list indicates that no logical partitions in the CSS will access the channel path following partition activation for the initial POR of the IOCDS.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Function ID Configuration

Use the **Function ID Configuration** window to select a channel configuration data set of information you want to view. The table lists the FIDs and assigned PCHID that exist in the selected IOCDS.

The function configuration table display:

FID
Displays the Function ID for the selected configuration data set

TYPE
Displays the function type the card is defined as

PCHID
Displays a four-digit physical channel identifier (PCHID) for the selected configuration data set.

PORT
Displays the port assignment for a specific Function ID

VF
Displays the virtual function for the selected configuration data set

UUID
Displays the unique user-defined ID for the configuration data set

Access Partition Name
Displays the partition name the configuration data set

PNETID
Displays the physical network identifier configuration data set.

The icons perform the following actions for the selected configuration data set:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Additional functions on this window include:

Close
To close the current window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Image Candidate List

Select **Image Candidate List** to display the logical partitions for a specific channel subsystem that have the FID configured online at partition activation following initial power-on reset (POR) of the IOCDS.

After the initial POR of the IOCDS, PR/SM LPAR retains which logical partitions will have the FID configured online at partition activation following subsequent PORs with the same IOCDS.

The image candidate list displayed is associated with keywords PARTITION, NOTPART, SHARED, and PATH on the IOCP CHPID statement.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID
Displays the PCHID identifier, if any, for the selected FID. A PCHID identifier is assigned by the PCHID keyword.

FID
Displays the FID identifier for the selected channel. A FID identifier is assigned by the PATH keyword.

Partition Name
Displays the Partition Name for the FID.

Additional functions on this window include:

Close
To close the current window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Partition Images Configured

Select **Partition Images Configured** to display the MIF image ID numbers and names of the logical partitions defined in the selected input/output configuration data set (IOCDS).

You can sort the list of logical partitions by partition name or by CSS and MIF image ID numbers.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

Partition images configuration table

The partition images configuration table displays all of the logical partitions defined in the selected IOCDS. All the following logical partition information is specified with the PARTITION keyword on the RESOURCE statement.

CSS
The CSS parameter indicates the channel subsystem a logical partition is in.

MIF Image ID
The MIF image ID within the CSS that is associated with the logical partition.

Partition Name
The name of the logical partition.

Dynamic Information

Select **Dynamic Information** to check and compare an input/output configuration data set (IOCDS) token and the current channel subsystem hardware system area (HSA) token. If the selected IOCDS does not have a token, it does not contain any dynamic information and the Dynamic Information view cannot be selected.

Configuration data set shows the identifier of the IOCDS you selected on the previous window. Its token displays in the **Data set token** field. An IOCDS has a token if it was created using an operating system feature that supports dynamically changing the input/output (I/O) definition defined by the IOCDS.

Hardware system area token shows current HSA token, if any. The HSA token is only displayed if the system has been power-on reset using an IOCDS that had a token in it and the power-on reset enabled dynamic I/O configuration.

Configuration data set
Displays the identifier of the configuration data set.

Data set token
Displays the IOCDS token.

Hardware system area token

Displays the token most recently saved in the hardware system area (HSA). A token is saved in the HSA when:

- A power-on reset is performed using an IOCDS that contained a token and the power-on reset enabled dynamic I/O configuration.
- An operating system feature that supports dynamically changing the I/O definition is used to alter the HSA.

If the most recent power-on reset did not enable dynamic I/O configuration changes, this field is blank.

When the HSA token and the data set token match, and the data set is active, the operating system feature can be used to dynamically change the I/O definition.

Data set maximum number of devices
Displays the maximum number of devices allowed for each channel subsystem (CSS) and each subchannel set. This is defined by IOCP with the MAXDEV keyword on the RESOURCE statement.

Hardware system area maximum number of devices
Displays the maximum number of devices allowed for each channel subsystem (CSS) and each subchannel set within the HSA. These maximums are established during power-on reset and cannot be changed dynamically.

If the most recent power-on reset did not enable dynamic I/O configuration changes, this field is blank.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Supported I/O Mask

Select **Supported I/O Mask** to display and compare the supported I/O masks in the selected IOCDS and supported by your CPC.

The supported I/O mask contains hexadecimal values that identify the processor functions or channel path types defined in the IOCDS or supported by your CPC. If the IOCDS contains a value not in the Machine Supported I/O mask, then the Unsupported mask items display shows which items are not supported by the system. The system cannot power-on reset with the selected IOCDS.

See "CPC activation and Power-on Reset Error" in the *Input/Output Configuration Program User's Guide* for a description of the supported functions and channel path types.

IOCDS supported I/O mask
The supported I/O mask in the IOCDS indicating the functions and channel path types contained in the IOCDS.

Machine supported I/O mask
The supported I/O mask for the machine indicating all the functions and channel path types supported by the machine.

Unsupported mark items
The specific items in the IOCDS that are not supported by the machine. This line is displayed only when unsupported items are present. The IOCDS cannot be used to power-on reset the machine.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Save Data Files on Hardware Management Console

Use this window to copy the IOCDS data files from the Support Element console to the Hardware Management Console's hard drive. The fully qualified path name for the data files must be specified at the Target path name entry field.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Restore Data Files on Hardware Management Console

Use this window to copy the IOCDS data files from the Hardware Management Console's hard drive to the Support Element's hard drive. The fully qualified path name for the data files must be specified at the Target path name entry field.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Input/Output (I/O) Configuration Save and Restore

Accessing the Input/Output (I/O) Configuration Save and Restore task

This task allows you to save, restore, or erase Input/Output (I/O) configuration data files for a specified object on the Hardware Management Console.

Note: If you choose to save data files on the Hardware Management Console, any previously saved files will be erased.

To save or restore data files:

1. Select a CPC (server).
2. Open the **Input/Output Configuration Save and Restore** task. The Input/Output Configuration Save and Restore window is displayed.
3. Select one of the options:
   - Save data files
   - Restore data files
   - Restore only the IOCDS data files
   - Restore only the channel configuration files
   - Erase the data files
4. Click **OK** to proceed with your choice, or click **Cancel** to exit the task.

Input/Output Configuration Save and Restore

Use this window to save, restore, or erase I/O configuration data files for this object on the Hardware Management Console. Select the option you prefer, then click **OK** to proceed.

Note: If you choose to save data files on the Hardware Management Console, any previously saved files will be erased.

Save data files on Hardware Management Console
To save I/O configuration data files on the Hardware Management Console, select **Save data files on Hardware Management Console**.

Restore data files from Hardware Management Console
To restore I/O configuration data files from the Hardware Management Console, select **Restore data files from Hardware Management Console**.

Restore only IOCDS data files from Hardware Management Console
To restore only the IOCDS data files from the Hardware Management Console, select **Restore only IOCDS data files from Hardware Management Console**.

Restore only channel configuration files from the Hardware Management Console
To restore only channel configuration files from the Hardware Management Console, select **Restore only channel configuration files from the Hardware Management Console**.

Erase data files from Hardware Management Console
To erase the I/O configuration data files from the Hardware Management Console, select **Erase data files from Hardware Management Console**.

OK
To perform the selection you have made, click **OK**.

Cancel
To exit this task without performing one of the functions, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installation Complete Report

Accessing the Installation Complete Report task

Note: You cannot perform this task remotely.

This task is used by support system personnel to report installation information. This information is used to assess the success of the installation and make improvements in the installation processes. The information can be transmitted directly to the support system from the Hardware Management Console or copied to removable media.

The following types of installations should be reported:

- New install
- MES (Miscellaneous Equipment Specification)
- Reinstall
- Patch, Ucode, LIC
- Refresh, PTF
- Discontinue.

To provide an installation complete report:

1. Open the **Installation Complete Report** task. The Installation Complete Report window is displayed.
2. Provide the appropriate information to complete the report.
3. Click **Continue** to proceed to the next window to provide more information or proceed with the process of transmitting the report to the support system.

Installation Complete Report (installation activities)

Use this window to fill in and send product support a report about installation activities for a customer's machine(s), presumably located at or near the location of this Hardware Management Console. You should report any of the following installation activities:

- Installing new machines.
- Upgrading previously installed machines (MES).
- Reinstalling previously installed machines.
- Changing licensed internal code of machines.
- Upgrading corrective service levels of machine control programs (refresh or PTF).
- Removing previously installed machines (Discontinue).

An installation complete report should take only a few minutes to complete. The information in the report helps product support to maintain field inventory databases and to identify, resolve, and prevent defects.

Team Leader Name
Specify your name, or the name of the person to contact about the installation and the information in this report.

Telephone number
Specify your telephone number, or the telephone number of the person to contact about the installation and the information in this report.

Specify the three-digit area code in the leftmost field, then use the middle and rightmost fields to specify the seven-digit local number.

Activity Group
This section identifies the types of activities performed during the installation. You must select at least one of the following types of activity, but you can select more than one or all of the types of activities.

New install
Indicates the installation activities included installing one or more new machines.

MES
Indicates the installation activities included upgrading one or more previously installed machines.

Re-install
Indicates the installation activities included installing again one or more previously installed machines.

Patch, Ucode, LIC
Indicates the installation activities included changing the licensed internal code for one or more machines.

Refresh, PTF
Indicates the installation activities included upgrading the corrective service level of the control program for one or more machines.

Discontinue
Indicates the installation activities included removing one or more previously installed machines.

Continue
When you are finished providing the information requested on the window, click **Continue**. This displays the next window in the current report.

Cancel
To discard the current report and close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installation Complete Report (date and time checkpoints)

Use this window to report the date and time when installation checkpoints were completed, and to indicate whether the installation was defect-free.

Machine arrival date/time
Use these fields to specify the date and time the hardware was delivered to the installation site. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Install start date/time
Use these fields to specify the date and time the first installation activity was started. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Mechanical complete date/time
Use these fields to specify the date and time the final hardware installation activity was completed. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Solution software complete date/time
Use these fields to specify the date and time the final software installation activity was completed. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Install complete date/time
Use these fields to specify the date and time the final installation activity was completed. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Total idle time
Specify the total amount of time spent not performing any installation activities between starting the first installation activity and completing the final installation activity.

Then use the **Explain idle time or missed commitment** field to specify an explanation of the reasons for the idle time.

Was commitment to customer met?
To indicate **the customer's** expectations for the installation were met, select **Yes**.

Otherwise, if **the customer's** expectations for the installation were not met, select **No**. Then use the **Explain idle time or missed commitment** field to specify an explanation of the reasons the commitment was not met.

Explain idle time or missed commitment
Specify an explanation of the reasons for any idle time, or why the commitment to the customer was not met. That is, specify an explanation when:

- You specified any non-zero amount of time in the **Total idle time** field, or
- You selected **No** to answer **Was commitment to customer met?**

Were problems encountered?
To indicate one or more problems occurred during the installation, select **Yes**. Otherwise, select **No**.

A problem is any event that:

- Prevents the completion of the installation.
- Delays the completion of the installation.
- Requires performing activities during the installation that would not be performed if the event had not occurred.

  Example: Removing and replacing a defective part.

Continue
When you are finished providing the information requested on the window, click **Continue**.

If you selected **No** to answer **Were problems encountered?**, then the report is complete. Clicking **Continue** starts the process for transmitting the report to the support system.

Otherwise, if you answered **Yes** to indicate one or more problems occurred, then you must provide more information about each problem. Clicking **Continue** displays additional windows for reporting problem information.

Cancel
To discard the information on this window, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installation Complete Report (additional information for a problem)

On a previous window, you indicated problems were encountered during the installation. Use this window to provide more information about one of the problems.

A problem is any event that:

- Prevents the completion of the installation.
- Delays the completion of the installation.
- Requires performing activities during the installation that would not be performed if the event had not occurred.

  Example: Removing and replacing a defective part.

System lost time
Specify the amount of time the system was not available because of the problem.

Problem resolution time
Specify the amount of time required to diagnose and correct the problem.

Part procurement time
Specify the amount of time between requesting and receiving parts required to correct the problem.

Defect Summary
This section describes the cause of the problem, and describes how the problem was solved.

For each field, you can select the term that best describes the information it requests by clicking the scroll arrow for a list of choices or you can specify a new entry.

Component
Select or specify the term that best describes the specific unit of hardware, software, or documentation that caused the problem.

Action
Select or specify the term that best describes how the problem with the component was solved.

Source
Select or specify the term that best describes the general unit of hardware, software, or documentation that contained the component that caused the problem.

Defect
Select or specify the term that best describes the problem with the component.

Parts not Recorded by Repair and Verify
If you removed and replaced a part while diagnosing or correcting the problem, but were not instructed to do so by an online service procedure, then use this section to describe the part you removed and the part that replaced it.

Reference code
Specify the reference code, if any, for the problem.

Part number
Specify the Custom Card Identification Number (CCIN) of the removed part.

Serial number
Specify the serial number of the removed part.

Location
Specify the part location from which the part was removed.

Note: If the removed part is identified by two part locations, specify the first location in this field, then specify the second location in the **To location** field. For example, cables are identified by two part locations. Each part location identifies where one end of the cable is connected.

To location
If the removed part is identified by two part locations, specify the second part location from which the part was removed. Specify the first location in the **Location** field.

Note: For example, cables are identified by two part locations. Each part location identifies where one end of the cable is connected.

New part number
If a different part was installed to replace the removed part, specify the Custom Card Identification Number (CCIN) of the replacement part.

New serial number
If a different part was installed to replace the removed part, specify the serial number of the replacement part.

BOM number
If the replacement part was ordered new, specify the number of its Bill of Materials (BOM).

Patch or MCL fixes
If you installed and activated an internal code fix while correcting the problem, use this section to specify the Engineering Change (EC) number of the internal code fix in the **Patch number** field.

Comments about the defect
Specify any additional information that describes the problem or its solution.

Continue
When you are finished providing the information requested on the window, click **Continue**. A message displays for you to use to indicate whether there are additional problems to report.

Cancel
To discard all problem information on the window and in the current report, and to return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Part Location

Part Location identifies the location of a part in a frame.

Parts can be located in the power module section or card section within a Central Processor Complex (CPC) or an optional expansion cage.

Part locations are identified by up to twelve characters. Some parts, like cables, are identified by up to twelve characters for the location of each end, with the two locations separated by a dash.

The first character of a twelve character location identifies the frame location.

A
Identifies the rightmost frame in the machine.

Z, Y, X, W, or V
Identifies frames attached to the left of frame A.

Note: The identifiers used for additional frames are determined by the machine model.

The next three characters identify the location of the CPC or expansion cage within the frame.

01A
Indicates the location is the bottom of the frame.

18A
Indicates the location is the top of the frame.

The remaining four to eight characters identify the type of part, and indicate where the part is located within the CPC or expansion cage.

- For the following parts in the card section, 'nn' identifies the card socket where the part is located:

  D1nn
  Coupling facility channel link card

  D2nn
  Coupling facility channel link card

  LGnn
  Logic card

  Example: A logic card in card socket 26 of the CPC or expansion cage at the bottom of frame Y is identified by part location:

  Y01ALG26

- For the following parts in the power module section, 'nn' is a number that distinguishes a module from other modules of the same type:

  AFnn
  AC front end card (power module)

  BUnn
  Battery backup module

ELnn
Energy limiting module

PSnn
Power supply, AC/DC modules

UPnn
Unit panel (central processor complex)

Example: The second of two energy limiting modules in the top CPC in frame A is identified by part location:

A18AEL02

Integrated 3270 Console

Accessing the Integrated 3270 Console task

Notes:

- Not all host operating systems support the integrated 3270 console. Refer to your host operating system documentation to determine whether the host operating system supports the integrated 3270 console and to learn how to use the integrated 3270 console with the host operating system.
- One 3270 console is available for each image.
- It is valid to start the **Integrated 3270 Console** task before you start the host operating system. In this case, the 3270 console window remains unchanged until the host operating system is started.
- You can perform a session takeover from any HMC, even if you are logged on to the same HMC as the user of the current session.

To start the **Integrated 3270 Console** task:

1. From the navigation pane, click **Systems Management**, then choose a server.
2. The work pane table displays a list of images applicable for the chosen server.
3. Select a server that you want to work with by clicking in the **Select** column.
4. From the tasks pad, click **Recovery**.
5. Click the **Integrated 3270 Console** task under Recovery to start the task of the selected image. The Integrated 3270 Console window is displayed.
6. Click the **X** in the upper right corner of the window when you are done working with the console.

Integrated 3270 Console

Use the **Integrated 3270 Console** task to provide a 3270 console that can be used with a host operating system without the need for any special connectivity, such as control units, TCP/IP, or network connection. The **Integrated 3270 Console** task uses the existing network connection between the Hardware Management Console and Support Element and the connection between the Support Element and the CPC or partition to communicate with the host operating system.

Attention: Not all host operating systems support the integrated 3270 console. Refer to your host operating system documentation to determine whether the host operating system supports the integrated 3270 console and to learn how to use the integrated 3270 console with the host operating system.

The **Integrated 3270 Console** task displays a 3270 console window with the "X SYSTEM" indicator that is displayed in the status area. At the same time, the **Integrated 3270 Console** task tries to establish communications with the host operating system. After the host operating system responds, the 3270 console window is updated with the data that is provided by the host operating system. If the host operating system is not running or does not support the integrated 3270 console, then the 3270 console window remains unchanged.

If you selected a CPC in PR/SM mode, see “PR/SM mode” on page 897 or if you selected a partition that has DPM enabled, see “DPM mode” on page 897.

PR/SM mode

If the host system is not running, close the blank window, then you can start the system by using the **Load** task.

1. Selecting the same object, open the **Load** task.
2. The Load window is displayed.
3. Enter the *load address* of your operating system in the **Load address** input field.
4. Enter the *load parameter* (for example, **sysg** for z/VM 4.4) in the **Load parameter** input field.
5. Click **OK**. The Load Task Confirmation window is displayed.
6. Click **Yes**. The Load Progress window is displayed indicating the progress of the load and the outcome.
7. Click **OK** to close the window when the load completes successfully.
8. After the load completes, select the object again, open the **Integrated 3270 Console** task. The Integrated 3270 Console window is displayed and updated with data that is provided by the host operating system.

DPM mode

With DPM, an administrator uses the **Boot** section of the **Partition Details** task to specify how to start the operating system.

Use the following steps for an existing partition that is not active:

1. Select **Systems Management** from the navigation pane.
2. Select **Partitions** tab from the work pane.
3. Select a partition and open the **Partition Details** task.
4. Select **Boot** from the navigation pane. The Boot section of the Partition Details window is displayed.
5. Select **Storage Device (SAN)** from the **Boot from** list to display the **OS load parameters** input area.
6. Type **sysg** or leave blank (default) in the **OS load parameters** input area to open the Integrated 3270 Console task window.
7. Click **OK** or **Apply** to save the updates to the Boot section.
8. Click **Save** to confirm your changes to the partition definition.
9. Open the **Integrated 3270 Console** task.
10. Use the **Start** task to start the partition and its operating system.

If you use the **New Partition** task, follow the previous steps for the Boot section, then proceed with the following:

1. Review the Summary page and click **Finish** to save the partition definition.
2. Open the **Integrated 3270 Console** task.
3. Use the **Start** task to start the partition and its operating system.

Integrated ASCII Console

Accessing the Integrated ASCII Console task

Notes:

- This task is supported by the Linux operating system that is running in an LPAR partition or as a guest of z/VM (Version V5.3 or later).
- One ASCII console is available for each CPC image.

This task provides an ASCII console that can be used with a host operating system without the need for any special connectivity or additional hardware, such as control units or network connections. The Integrated ASCII Console uses the existing network connection between the Hardware Management Console and the Support Element, and the connection between the Support Element and the CPC to connect with the host operating system.

To start the console:

1. Select a CPC image.
2. Open the **Integrated ASCII Console** task. The Integrated ASCII Console window is displayed.

   If the Linux operating system is already started, the Integrated ASCII Console task tries to establish communications with it. After the operating system responds, press Enter, the Integrated ASCII Console window will be updated with the Linux Welcome screen.

   If the Linux operating system is not running, you can start the system by performing the **Load** task.

   a. With the CPC still selected, open the **Load** task (under the Recovery task group).
   b. The Load window is displayed.
   c. Enter the *load address* of your operating system in the **Load address** input field.
   d. Click **OK**. The Load Task Confirmation window is displayed.
   e. Click **Yes**. The Load Progress window is displayed indicating the progress of the load and the outcome.
   f. Click **OK** to close the window when the load completes successfully.
   g. After the load completes, select the CPC again, open the **Integrated ASCII Console** task. The Integrated ASCII Console window is displayed and updated with the Linux Welcome screen.
3. Click the **X** in the upper right corner of the window when you are done working with the console.

Integrated ASCII Console

Use the **Integrated ASCII Console** task to open a terminal with the Linux operating system.

You can scroll the information that is displayed for the terminal session. To scroll up, hold Shift and press Page Up. To scroll down, hold Shift and press Page Down.

To start the **Integrated ASCII Console** task:

1. Make sure that the Linux operating system is running on the image where you want to open it. You might have to perform a **Load** task.
2. In the navigation pane, click **Systems Management**, then choose a server.
3. The work pane table displays a list of images applicable for the chosen server.
4. Select an image that you want to work with by clicking in the **Select** column.
5. From the tasks pad in the task list, click **Recovery**.
6. Click the **Integrated ASCII Console** task under Recovery to start the task of the selected image.

Note: Only one console can run on an image.

Load

Accessing the Load task

Notes:

- Depending on your machine type, model, and features installed, you can have up to three Load types:
  - Standard load
  - SCSI load

  - SCSI dump.
- For daily or routine loading of images, it is recommended that you customize activation profiles to specify how you want to load images, and then use a profile with the **Activate** task to perform all the operations necessary to make an image operational, including loading it with a control program.
- The **Load** task is considered a disruptive task. If the object is locked, you must unlock it before continuing.

Load (except coupling facility and SSC images) causes a program to be read from a designated device and initiates execution of that program. If the CPC is operating in logically partitioned (LPAR) mode, the logical partition is the target of the load. Otherwise, if the CPC is operating in basic mode, the CPC is the target of the load.

To perform a load:

1. Select one or more CPC images.
2. Open the **Load** task. The Load window is displayed with the information that was last used when the CPC image was loaded.
3. Review the information in the window to verify that the object you will load is the correct one.

   If the information is correct, click **OK**. The Load Task Confirmation window is displayed. If you click **Yes** to proceed, then the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
4. To continue with the load, click **Yes**. The Load Progress window is displayed indicating the progress of the load and the outcome.
5. Click **OK** to close the window when the load completes successfully. Otherwise, if the load does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Load

Use this window to provide or change information used to load the selected images with a control program.

Note: Other products and documentation may refer to this operation as an *initial program load (IPL)*.

Use the tabs to select the image whose information you want to view.

1. Review or change the information displayed on the window. It will be used to load the selected image with a control program.
2. Click **OK** to request a load using the displayed information.

Task

Use this window while “Loading an image during a recovery procedure” on page 899.

Note: For daily or routine loading of images, It is recommended that you customize activation profiles to specify how you want to load images and then use a profile with the **Activate** task to perform all the operations necessary to make an image operational, including loading it with a control program.

Loading an image during a recovery procedure

You can use a Hardware Management Console to load an image. You can try to load any image at any time, but this task is intended for use during recovery procedures.

Note: For daily or routine loading of images, the following alternative is recommended:

1. Use the **Activation Profiles** task to customize and store load information in activation profiles for Central Processor Complexes (CPCs) and their images.
2. Use the **Activate** task and a profile to perform all the operations necessary to make a CPC or image operational, including loading it with a control program.

If the load type is Standard Load the following elements are unavailable.

- Worldwide port name
- Logical unit number
- Boot program selector
- Boot record logical block address
- Operating system specific load parameters

Descriptions for the information on this window follows:

CPC
Displays the name of the central processor complex (CPC) that supports the selected image.

Image
Depending on your model and machine type, you may have only logically partitioned (LPAR) mode or both LPAR mode and General mode. If the CPC is operating in LPAR mode, this field displays the name of the logical partition that supports the selected image. The logical partition is the target of the load.

An **image** is a set of CPC resources capable of running a control program or operating system. One or more images are created during a power-on reset of a CPC. When a power-on reset puts the CPC in LPAR mode, each logical partition is an image. When a power-on reset puts the CPC in a basic mode, the CPC has a single image.

Load type
Select the type of load to perform for the logical partition without clearing the main storage. Optionally, select the clear main storage on the logical partition before loading. You would use the SCSI dump option to do a standalone dump to a SCSI device.

Standard load
To perform the load on the logical partition, click **Standard load**.

Note: You must select this choice if you want to perform the **Store status** function.

SCSI load
To load from a device that requires a SCSI load, click **SCSI load**.

SCSI dump
To load a standalone dump program from a device that requires a SCSI load, click **SCSI dump**.

NVMe load
To load from a device that requires a NVMe load, click **NVMe load**.

NVMe dump
To load a standalone dump program from a device that requires a NVMe load, click **NVMe dump**.

Enable Secure Boot for Linux
To verify the signature of the load program and distributor's signature match , select **Enable Secure Boot for Linux**.

Clear the main memory on this partition before loading it
Select this to clear main memory storage on the logical partition before a load.

Note: Available when **Standard load**, **SCSI load**, or **NVMe load** are selected. Clearing partitions with larger amounts of main memory storage may take longer.

Store status
The store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations. (This function is effective only when the status of the processor performing the load is **Stopped**.)

If the selected load type is **Standard load**, this check box indicates whether to perform the store status function before the load.

Note: This is applicable only when the selected load type is **Standard load**. Otherwise, this selection is unavailable.

If the selected load type is **Standard load**, click the check box to change the setting.

- A check mark indicates performing the store status function before the load.
- An empty check box indicates not performing the store status function before the load.

Load address
This field displays the address of the device most recently used to load the selected image. To use a different device for this load, type a new address.

The address of the input/output (I/O) device provides access to the control program to load. For a SCSI load, NVMe load, SCSI dump, or NVMe dump, this field has the device number of the device (for example, fibre channel adapter) that will be used to perform the load.

This should contain four hexadecimal digit device address for NVMe load or five hexadecimal digit device address for SCSI load. It must also be defined in the input/output (I/O) configuration that is currently active.

Load parameter
This field displays the optional information, if any, most recently used to further control how the control program was loaded for the selected image. To use different information for this load, type a new parameter.

Some control programs support using a load parameter to provide additional control over the performance or outcome of a load.

For control programs that do not support a load parameter, leave the field blank. Otherwise, if a control program supports a load parameter, you must use the correct syntax and it must satisfy the following requirements:

- A load parameter can be from one to eight characters long. Valid characters for a load parameter are:
  - At (@)
  - Pound (#)
  - Dollar ($)
  - Blank character
  - Period (.)
  - Decimal digits 0 through 9
  - Capital letters A through Z (Lowercase letters, if any, are changed to uppercase when you click **OK**.)

Note: For information about the syntax of a load parameter, refer to system commands or operations documentation for the control program. Some documentation may refer to the load parameter differently, for example, as LOADPARM, or IPL parameter, or IPLPARM.

Time-out value
This displays the time-out value allowed for completing the load. The default is 60 seconds. To allow more time for the load to complete, type a new value. The time-out value can be from 60 to 600 seconds. If the load cannot be completed within the specified time, it is canceled and an error is returned.

Note: This field is disabled if a load type of **SCSI load** or **SCSI dump** is selected.

Worldwide port name
The Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (64 bits, according to the FCP/SCSI-3 specifications). This field contains the 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

Note: This field is disabled for a load type of **Standard load** and **NVMe load**.

Logical unit number
The number of the logical unit as defined by FCP (64 bits, according to the FCP/SCSI-3 specifications). This field contains the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

Note: This field is disabled for a load type of **Standard load** and **NVMe load**.

Boot program selector
This field identifies the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30. This parameter provides the possibility of having up to 31 different boot configurations on a single disk device. This field should be set to 0 for optical media SCSI devices.

Note: This field is disabled for a load type of **Standard load**.

Boot record logical block address
Specify an address if your file system supports dual-boot or booting from one of the multiple partitions. This record is organized as an array, which lets you select an array element other than the first one.

The load block address field contains a 64-bit binary number, represented by 16 hexadecimal characters, designating the logical-block address of a boot record on the FCP-load device. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident. This field should be set to all zeroes for optical media SCSI devices.

Note: This field is disabled for a load type of **Standard load**.

Operating system specific load parameters
This field contains a variable number of characters to be used by the program that is loaded. This information is given to the IPLed operating system and ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this. Any line breaks you enter are transformed into spaces before being saved.

Note: This field is disabled for a load type of **Standard load**.

OK
To load the selected image, click **OK**.

Reset
To erase the information you typed and re-display the information most recently used to load the selected image, click **Reset**.

Cancel
To exit this window and return to the Hardware Management Console workplace without performing the load, click **Cancel**.

Help
To display help for the current window, click **Help**.

Load from Removable Media or Server

Accessing the Load from Removable Media or Server task

Note: Loading from removable media or an FTP server is considered a disruptive task. If the object is locked, you must unlock it before you continue. For more information about disruptive tasks, expand the Introduction section of the help Table of Contents, then select **Disruptive tasks**.

This task loads system software or utility programs from removable media or from an FTP server.

To load the software:

1. Select a CPC image.
2. Open the **Load from Removable Media or Server** task. The Load from Removable Media or Server window is displayed.
3. Select the source of the software:

- Hardware Management Console removable media
- Hardware Management Console removable media and assign for operating system use
- FTP Server

  If you are loading from an FTP server, you need to:

  – Enter the FTP host name.
  – Enter your user name.
  – Enter your password.
  – Select the FTP protocol.

4. Choose the location of the software program by specifying the relative or absolute file path on the **File path** field, if necessary.
5. Click **OK**.
6. Proceed with the "Select Software to Install" on page 904 window by selecting the **.ins** file and performing the load.
   - If the source is in the root directory of the CD/DVD-ROM, select **Hardware Management Console removable media device**, and leave the File location blank.
   - **Relative Path:** If the source is in the LINUX subdirectory, you can select **Hardware Management Console removable media device** and enter `LINUX` (or `LINUX/`) in the File location. (Note that the path name is case-sensitive.)

   The File location field works the same way whether the source you choose is the local removable media device or the FTP server.
7. After you complete the current window and select the file or program you want to load, click **OK** to continue with this task. A load in-progress window is displayed showing the duration and elapsed times.
8. Click **OK** to close the window when the task completes successfully.

Load from Removable Media or Server

This task loads system software or utility programs from removable media or from an FTP protocol. You can specify only one software source.

Note: For any of the sources of the software that you select, you must prepare the **.ins** file and the actual software or programs to load on the source using the "Select Software to Install" on page 904 instructions.

Hardware Management Console removable media
To retrieve operating system software or utility programs from the Hardware Management Console removable media, select **Hardware Management Console removable media**.

If you use **CD/DVD-ROM** as the source, the ISO image must be burned using the ISO9960 file system format.

If you use **USB flash memory drive** as the source, the USB flash memory drive must be formatted first using the Hardware Management Console. For more information on the USB flash memory drive, expand the Introduction section from the help Table of Contents, then select **USB flash memory drive**.

Note: If there is no valid USB flash memory drive on the Hardware Management Console, this option is not available.

Hardware Management Console removable media and assign for operating system use
To retrieve operating system software or utility programs from the Hardware Management Console removable media and assign for operating system use, select **Hardware Management Console removable media and assign for operating system use**.

FTP Server
To retrieve operating system software or utility programs from an FTP source, select **FTP Server**.

When want to use an **FTP server** as the source, make sure the Hardware Management Console has access to the target FTP server using one of these protocols: FTP (File Transfer Protocol), FTPS (FTP Secure), or SFTP (SSH File Transfer Protocol).

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To continue to load from removable media or server, click **OK**.

Cancel
To close the window and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Software to Install

This Load from Removable Media to Server - Select Software to Install window allows you to load software or utility programs from the Hardware Management Console's removable media or from an FTP server.

Select the software or utility program to load. Use your cursor movement keys or your mouse to highlight the selection, then click **OK** to proceed. Only one selection is allowed at a time.

After you specify the system software or utility program to load, all files within that package are loaded into the target and started. The **.ins** files represent packages of software or programs that can be loaded. They have a file extension of **ins.** and are in the form:

*Description line
/relative path/filename1.extension < space > < address of where to load >
/relative path/filename2.extension < space > < address of where to load >
/relative path/filename3.extension < space > < address of where to load >
.
.
.
/relative path/filenameN.extension < space > < address of where to load >

Where **path** is relative to the location of the **ins** file.

For example, **Sample1.ins** could contain:

** SuperUtilities Package Version 12.34*
/directory1/file1.txt 0x00000000
/directory2/file2.txt 0x00100000

All addresses start with "0x", followed by an 8 character hexadecimal address of where to start to load the file in memory.

An asterisk (*) in the first line of the file starts a comment line and is used to supply a one-line description of the file used on this window and on the confirmation window. The remainder of the file is a list of which files on the source (relative to where the load control file is located) and the addresses of where to load the data.

Generally, data files are a multiple of 4 bytes. If a file is only 2 bytes long and contains 0x1234, then 4 bytes are loaded into memory as 0x12340000. The highest address allowed is 0x7FFFFFFF. **Load from removable media device or FTP server** is intended for loading a software or utility installation program, not for normal IPLs.

Software table
Displays a list of the operating system software or utility programs that you want to retrieve.

OK
To proceed with loading the selected software or utility program to removable media or to an FTP server, click **OK**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Logical Processor Add

Accessing the Logical Processor Add task

This task allows you to select logical processor definitions to be changed dynamically on the system, in the image profile, or both. Dynamic changes will take effect without performing a reactivation of the logical partition.

The initial control settings of each logical partition are established by the activation profiles used to activate them, see the **Customize/Delete Activation Profiles** task for more information.

To dynamically add one or more logical processors:

1. Select a CPC image.
2. Open the **Logical Processor Add** task for an active partition. The Logical Processor Add window is displayed.
3. Based on the current logical partition configuration, change the logical processor definitions for the partition:
   a. Increase the initial values, reserved values, or both for installed logical processor types.
   b. Add a reserved value and set weight capping indicators for logical processor types that have not yet been installed and have no reserved CPs defined.
   c. Increase the reserved value for logical processor types that have not been installed and already have reserved CPs defined.
4. To have the new changes take effect immediately, click **Change Running System**.

Logical Processor Add

This window allows you to select logical processor definitions to be changed dynamically on the system, in the image profile, or both. Dynamic changes will take effect without performing a reactivation of the logical partition. This tasks allows you to:

- Increase the initial and/or reserved values for installed logical processor type(s).
- Add a reserved value and set weight and capping indicators for logical processor type(s) that have not yet been installed and have no reserved CPs defined.
- Increase the reserved value for logical processor type(s) that have not been installed and already have reserved CP(s) defined.

The partition status (active/inactive) is indicated in the window title, along with the logical partition name. If the logical partition is active, the current settings are displayed. If the logical partition is inactive, the settings contained in the image profile will be displayed.

Logical processor add table

This table displays the logical processor assignments for the logical partition. There is one row in the table for each CP type allowed for the logical partition's mode. Input fields are enabled/disabled depending on the logical partition configuration and current settings.

CP Type
Displays the logical processor type.

Number of Initial CPs
The number of initial central processing units for the logical processor type. If the logical processor type is installed, this value can be increased.

Number of Reserved CPs
The number of reserved central processing units for the logical processor type. In order to increase this value in the profile, the logical processor type must be currently installed. If the logical processor type is not currently installed, the number can be increased in the active logical partition only.

Capping
Indicates whether or not the initial processing weight of the logical processor type is capped. When the initial processing weight is capped, it is a limit. When the initial processing weight is *not* capped, it is a target, not a limit. Initial capping can be modified only when new processor type(s) are being defined and they are non-dedicated.

Dedicated
Indicates whether or not the logical processor type is dedicated or shared within the logical partition. This field cannot be modified.

Initial Weight
The initial processing weight for the processor type. The initial processing weight can be modified only when new processor type(s) are being defined and the logical processor type is non-dedicated.

Minimum Weight
The minimum processing weight for the processor type. The minimum processing weight can be modified only when new processor type(s) are being defined and Workload Manager (WLM) is enabled for the logical partition.

Maximum Weight
The maximum processing weight for the processor type. The maximum processing weight can be modified only when new processor type(s) are being defined and Workload Manager (WLM) is enabled for the logical partition.

Additional functions are available from this window.

Save to Profiles
If you want the new settings to take effect whenever the logical partition is activated with the modified profile, click **Save to Profiles**

Saving new settings modifies the following activation profiles:

- Saves a logical partition's processor control settings in its image profile. The settings take effect whenever the logical partition is activated with its image profile.
- **Save to Profiles** can be selected for both active and inactive logical partitions. The partition status (active/inactive) is indicated in the panel title, along with the logical partition name.

Note: Saving processor controls to the image profile saves *all* the processor controls currently displayed, regardless of when the settings were made. For example, if the **Logical Processor Add** window was previously used to change some of the active partition's processor controls, those changes are saved in the profile along with any changes subsequently made.

Change Running System
If you want the new settings to take effect in the active logical partition immediately, click **Change Running System**.

Changes the processor settings in the logical partition without reactivating the partition. The new settings remain in effect for the logical partition until you either dynamically change the settings again or reactivate the partition.

Note: Change Running System can be selected for an active logical partition only. For an inactive partition, the **Change Running System** button will be disabled.

Save and Change
If you want the new settings to take effect immediately *and* whenever the logical partition is activated with the modified profile, click **Save and Change**.

Save and Change performs the combined operations of **Save to Profiles** and **Change Running System**.

Reset
To return the values back to their original values, click **Reset**.

Cancel
To close this window without saving changes you made and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Capping

Use this field to set capping of the initial processing weight when defining a non-dedicated logical processor. A check indicates the logical processor's initial processing weight is capped.

For each logical processor type that is already defined, the field in this column displays the initial capping setting for the processor. If the processor is already defined, capping cannot be changed.

A logical processor's *initial weight* is its relative amount of shared processor resources. The *initial capping* setting indicates whether the logical processor is prevented from using processor resources in excess of its processing weight.

- When the initial processing weight is *not* capped, it is a target, not a limit. It represents the share of resources guaranteed to a logical processor when all processor resources are in use.
- When the initial processing weight is capped, it is a limit. It represents the logical processor's maximum share of resources, regardless of the availability of excess processor resources.

Note:

- Initial capping can be modified only when new processor type(s) are being defined and they are non-dedicated.
- Initial capping cannot be selected if the logical partition is WLM managed because they are mutually exclusive.

Initial Weight

Use this field to set the initial processing weight when defining a logical processor type that is non-dedicated.

For each logical processor type that is already defined, the field in this column displays the initial processing weight assigned to the processor. If the processor is already defined, the initial processing weight cannot be modified.

A logical processor's *initial processing weight* is its relative amount of shared processor resources.

An initial processing weight represents the share of resources guaranteed to the logical partition when all processor resources are in use. Otherwise, when excess processor resources are available, the logical partition can use them if necessary. When a logical partition is not using its share of processor resources, other active logical partitions can use them.

While excess processor resources are available, initial processing weights have no effect on how those resources are used. Instead, initial processing weights take effect only when the number of logical processors requiring a timeslice is greater than the number of available physical processors.

Note:

- The initial processing weight can be a value from 1 to 999.
- Initial processing weight can be modified only when new processor type(s) are being defined and they are non-dedicated.

Minimum Weight

Use this field to set the minimum processing weight when defining a non-dedicated logical processor and Workload Manager (WLM) is enabled for the logical partition.

For each logical processor type which is already defined, the field in this column displays the minimum processing weight assigned to the processor. If the processor is already defined, the minimum processing weight cannot be modified.

When Workload Manager is enabled, a logical partition's *minimum weight* places a lower limit on the amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

- The minimum processing weight can be a value from 0 to 999. A value of 0 indicates that there is no minimum processing weight.
- The minimum weight must be less than or equal to the initial processing weight.
- Minimum processing weight can be modified only when new processor type(s) are being defined, they are non-dedicated and WLM is enabled for the logical partition.

Maximum Weight

Use this field to set the maximum processing weight when defining a non-dedicated logical processor and Workload Manager (WLM) is enabled for the logical partition.

When Workload Manager is enabled, a logical partition's *maximum weight* places an upper limit on the amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

- The maximum processing weight can be a value from 0 to 999. A value of 0 indicates that there is no maximum processing weight.
- The maximum weight must be greater than or equal to the initial processing weight.
- Maximum processing weight can be modified only when new processor type(s) are being defined, they are non-dedicated and WLM is enabled for the logical partition.

Logoff or Disconnect

Accessing the Logoff or Disconnect task

This task allows you to end the current user session and logs off the Hardware Management Console or to disconnect while your tasks continue running. If you disconnect, you can reconnect at a later time to continue working. However, a disconnected session is eventually ended. (This is because disconnected sessions exist only while the Hardware Management Console application is running. If the Hardware Management Console is restarted or the console is shut down or rebooted, all session information is lost.)

Select the log off operation when you no longer need access to the Hardware Management Console. Logging off the console does not affect the status of the CPC or images. After you log off or disconnect, the Welcome to the HMC window is displayed. If you chose to disconnect rather than logoff, when you logon again, the Choose a Disconnected Session window is displayed. You can select the disconnected session to continue working or you can begin a new session. (The number of windows displayed depends on the state of the session when it was disconnected. One of the windows is the main user interface; additional windows are for each task that was running when the session was disconnected.)

To log off the Hardware Management Console:

1. Open the **Logoff or Disconnect** task or select **Logout** from the user ID drop down located in the upper right corner of the workplace. The Choose to Logoff or Disconnect window is displayed.
2. Select **Log off**.
3. Click **OK** to end your session on the Hardware Management Console.

To disconnect from the Hardware Management Console:

1. Open the **Logoff or Disconnect** task or select **Logout** from the user ID drop down located in the upper right corner of the workplace. The Choose to Logoff or Disconnect window is displayed.
2. Select **Disconnect**.
3. Click **OK** to disconnect from your session on the Hardware Management Console with the intent of returning at a later time.

Hardware Management Console Logoff or Disconnect

This task is used to close the console workplace and log off or disconnect from the console.

Log off
To exit the console, select **Log off**.

Logging off only ends the current console session. It does *not* affect the status or operation of the defined Central Processor Complexes (CPCs) or CPC images.

Note: If you log off while tasks are active or windows are open the console will notify you that there are active tasks or open windows. You have the option to proceed, terminating all tasks that are running before they complete.

Disconnect
To disconnect from the console, while preserving your session as your tasks continue to run, select **Disconnect**.

When you log back on you will be notified of the disconnected sessions and whether or not you want to reconnect to them or begin a new session.

OK
To continue with the selection you made, click **OK**.

Cancel
To close the window without logging off or disconnecting from the console, click **Cancel**.

Help
To display help for the current window, click **Help**.

Logon

Hardware Management Console Logon

This window is used to specify a user identification (user name) and password for logging on to the console.

Your user name and password are assigned to you initially by your access administrator. Afterward, you can change your password while logging on to the console. If you do not know your user name and password, contact your access administrator or whoever is responsible for controlling access to the console.

Note: If your password has expired, you are prompted to change it.

Complete both input fields, then click **LOGIN** or **CONTINUE** to log on to the console.

Username
Specify the string of characters that identifies you to the console.

Password
Specify the string of characters that verifies your user identification and your authority to log on the console.

Note: Your password is not displayed. Black dots are displayed as you type your password.

LOGIN
If there are no users on this console that require Multi-factor Authentication (MFA), then to access the console:

1. Specify your user name in the **Username** input field.
2. Specify your password in the **Password** input field.
3. Click **LOGIN**. The **Hardware Management Console Workplace** is displayed.
4. To exit your session and close the window, select the **Logoff or Disconnect** task, click the **X** in the upper-right corner of the window, or click your user ID from the masthead and select **Logout**.

CONTINUE
If there are users on this console that require multi-factor authentication, then all users log on to this console using the following procedure.

1. Specify your user name in the **Username** input field.
2. Specify your password in the **Password** input field.
3. Click **CONTINUE**.
4. If you need to setup HMC MFA, the *Secure your account with multi-factor authentication* window is displayed. Proceed with the "Setting up Time-based One-Time Password Multi-factor Authentication" on page 910 section.
5. If you have previously setup HMC MFA, enter your authentication code and click **LOGIN**.
6. If you do not have an authentication code or do not need to provide an authentication code, leave the field blank and click **LOGIN**.
7. To exit your session and close the window, select the **Logoff or Disconnect** task, click the **X** in the upper-right corner of the window, or click your user ID from the masthead and select **Logout**.

Cancel
To close the window without logging on to the console, click **Cancel**.

HELP
To display help for the current window, click **HELP**.

Setting up Time-based One-Time Password Multi-factor Authentication

If your access administrator requires you or other users to use the Time-based One-Time Password (TOTP) multi-factor authentication to log on to the console, continue with the following steps the first time

you log on to the console. The access administrator set the HMC MFA setting from the **User Management** task.

1. Provide your user name and password on the logon window, then click **CONTINUE**.
2. You will begin the multi-factor authentication set up, the *Secure your account with multi-factor authentication* window is displayed, click **NEXT**.

   At any point during this multi-factor authentication process, you can use the following options that appear on the windows:

   Cancel Setup
   To leave this window without logging on to the console, click **Cancel Setup**. A window is displayed verifying that you want to cancel the setup of the multi-factor authentication. Click **YES** to return to the logon window or click **NO** to continue with the set up.

   NEXT
   To continue with multi-factor authentication, click **NEXT**.

   BACK
   To go back to the previous window, click **BACK**.
3. The *Install an authentication app on your mobile device* window is displayed.
4. Install the Google Authenticator app (or any compatible app) on your mobile device. This is a supported multi-factor authentication app for logging on to the console. Once you have installed the app on your mobile device, click **NEXT**.
5. The *Scan the bar code with your authentication app* window is displayed.
   - If you choose to scan the bar code, use your mobile device to scan the code displayed in the window and receive your one-time-use password from the app on your mobile device.
   - You can select **View text code instead** and use the key that appears on the *Enter the following key in your authentication app* window. Provide this key to the app on your mobile device to receive the one-time-use password.
6. After receiving your one-time-use password from the authentication app, click **NEXT**, the *Enter your authentication code* window is displayed.
7. Enter your one-time-use password in the authentication code field, then click **NEXT**. The *Success! Multi-factor authentication is now enabled* window is displayed.

   Notes:

   - Your one-time-use password changes every 30 seconds.
   - The console accepts the one-time-use password for the current, previous, and next 30-second interval, according to its clock.
     - That allows some time for you to enter the authentication code, and it allows for some discrepancy between the mobile device clock and the console clock.

The next time you logon to the console, you will only need to enter your user name, password, and the current authentication code from the app on your mobile device.

Manage Adapters

Accessing the Manage Adapters task

Use this task to view and customize the adapters and devices that are associated with a Dynamic Partition Manager (DPM)-enabled system.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

Perform the following steps to display and optionally modify details about a system's adapters and devices.

1. Select a DPM-enabled system.
2. From the **Configuration** task group, open the **Manage Adapters** task. The Manage Adapters window is displayed.

Manage Adapters

Use the **Manage Adapters** task to view and customize the adapters and devices of a Dynamic Partition Manager (DPM)-enabled system.

The main window of the **Manage Adapters** task includes the following:

- The name of the target system, which is displayed at the top of the window.
- A tabbed table, which can be used to view or customize the details pertaining to the adapters, devices, and cryptos that are defined for the system. The table is organized into the following tabs:
  - **Adapters** (see "View or Customize Adapters" on page 912)
  - **Devices** (see "View or Customize Devices" on page 916)
  - **Cryptos** (see "View or Customize Cryptos" on page 925). If no cryptos are installed on the target system, this tab is not displayed.

  To make a change, use the appropriate tab to select the new adapters, ports, or switches, then select an action from one of the tab's action menus. For more information about the **Adapters**, **Devices**, or **Cryptos** tab, click the appropriate link in the preceding list.
- The **Related Tasks** menu contains the following options:

  System Details
  Opens the **System Details** task against the target system.

  Monitor System
  Brings the main user interface to the foreground, selects the system's node in the navigation tree, and selects its Work area's **Monitor** tab.

  Monitor System Events
  Opens the **Monitor System Events** task against the target system.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

Additional functions on this window include:

Close
To exit the task, click **Close**. You can also exit the task if you click the red X in the upper right corner of the window.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

View or Customize Adapters

Use the **Adapters** tab to view or customize the adapters of a DPM-enabled system.

The **Adapters** tab consists of the following elements:

- A table that lists the adapters that are defined for the target system. See "Select Adapters" on page 913.
- A group of filters that help you control the information that is displayed on the table. See "Filter Adapters" on page 915.
- Several action menus that allow you to make changes. See "Select an Action" on page 915.

To make a change, use the table and filters to select the new adapters, ports, or switches, then select an action from one of the tab's action menus.

Select Adapters

The **Adapters** tab includes a table that lists the adapters that are defined for the target system. The adapters table is updated dynamically, so that it always reflects the current adapters, ports, and switches, and their values. Use this table to select the target adapters and view details, perform desired actions, and monitor status. Note that when the system has IBM Adapter for NVMe1.1 features, this table includes information about Non-Volatile Memory Express (NVMe) storage adapters only when NVMe solid state drives (SSDs) are installed in carrier cards in the system I/O drawers.

Each adapter appears in its own row in the table. By default, the ports and switches rows are collapsed. To view them, click the expand icon to expand the adapter row.

The information is arranged into the following columns:

Name
Name of the adapter, port, or switch. This value is a link that launches the **Adapter Details** task.

The name must be unique and must be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. The name shown in the adapter row is editable, but only for adapters (not for ports or switches). To edit the name, double-click on the name field.

ID
Physical channel ID (PCHID) of the adapter. This value is a four-character hexadecimal number. A value appears in this column for adapters only (not for ports or switches).

Type
Type of adapter.

Status
Status of the adapter. A value appears in this column for adapters only (not for ports or switches). The adapter status values include the following:

Active
Indicates that the adapter is operating normally.

Exceptions
Indicates that at least one adapter on the system is not operating.

Not active
Indicates that the adapter is not operating.

Service
Indicates that the adapter requires service.

State
State of the adapter. A value appears in this column for adapters only (not for ports or switches).

Card Type
Card type of the adapter. A value appears in this column for adapters only (not for ports or switches).

Location
Location of the adapter. A value appears in this column for adapters only (not for ports or switches).

Device Allocation
Progress bar that displays the percentage of devices that can be defined on an adapter. This value includes only devices of active or reserved partitions.

If you place your cursor over a cell in the column, two values are displayed, as follows:

- The progress bar value (percentage of devices that can be defined on the adapter, for active and reserved partitions only).
- The allocation for all defined partitions, including partitions that are inactive. This value can exceed 100 percent.

For an NVMe adapter, the allocation value is either 0 (when the adapter is available for use) or 100 (when a partition is using the adapter).

Number of Partitions
Number of partitions whose devices are defined to use the adapter or port/switch. When you click on a value in this column for a particular adapter, port, or switch, one of the following tables is displayed.

Storage Groups table
This table is displayed only when the system has the DPM R3.1 storage management feature or a later DPM version applied. The Storage Groups table lists storage groups and partitions that are using the target adapter. The table is empty under the following conditions:

- The adapter is not configured as either FCP or FICON.
- The adapter is not being used by any storage groups.

Storage Group
Name of an FCP or FICON or NVMe storage group that is using this adapter. The name is a hyperlink that opens the Storage Group Details page of the **Configure Storage** task.

Partition
Name of the partition that is using this adapter through the attached storage group. The name is a link that opens the **Partition Details** task. This field is empty when none of the listed storage groups are attached to a partition.

Partition Active/Reserved
Indicates whether the partition is active or reserved. A check mark indicates that the partition is either active, reserved, or both; a dash indicates that the partition is not active or reserved.

HBA Name
Name of the host bus adapter through which the partition can access the adapter. This column is shown in the table for FCP adapters only.

WWPN
Worldwide port name of the HBA. This column is shown in the table for FCP adapters only.

Device Number
Four-digit hexadecimal device number for the HBA. This column is shown in the table for FCP adapters only.

Network Interface Cards, Host Bus Adapters, or Virtual Functions table
This table provides information about the network interface cards (NICs), Host Bus Adapters (HBAs), or Virtual Functions (VFs) that are configured to use the specified adapter, port, or switch. The adapter, port or switch name is shown at the top of the window. The values that are displayed in the **Name** and **Partition** columns are links that launch the **Partition Details** task. The **Partition Active/Reserved** column shows whether the partition has been started, or if it is reserved. The devices table is updated dynamically as an adapter's partition count changes and as devices are modified.

The **Network Interface Cards**, **Host Bus Adapters**, or **Virtual Functions** tables also include the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Partitions table
This table provides information about the partitions that are configured to use the crypto adapter. The adapter name is shown at the top of the window. The values that are displayed in the **Partition** column are links that launch the **Partition Details** task. The **Active/Reserved** column shows whether the partition has been started, or if it is reserved. The partitions table is updated dynamically as an adapter's partition count changes and as a crypto's configuration changes.

The **Partitions table** also includes the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Description
Displays the user-provided description, if any, of the adapter, port, or switch. To edit the existing text or provide a description, double-click in the field and type the new description. To save your changes, select **Enter** or click outside the field.

Filter Adapters

The **Adapters** tab includes a row of filter icons that is used to control the information that is displayed in the table. You can click the filter icon to filter the table. Any row in the table that meets the criteria of the selected filters is displayed.

Note: If the target system does not include adapters that apply to a particular filter icon, the corresponding filter icon is not displayed on the **Adapters** tab. For example, if there are no crypto adapters installed on the system, the Crypto filter icon is not displayed.

The following filter icons are included on the **Adapters** tab:

Network
Displays the network adapters and their ports and switches. This includes only adapters and child ports of type OSD, OSM, RoCE, or HiperSockets. To filter network adapters, click the Network filter icon ().

Storage
Displays the storage adapters and their ports. To filter storage adapters, click the Storage filter icon ().

The type of adapters shown in this display varies, depending on whether the system has the DPM R3.1 storage management feature or a later DPM version applied. Possible types are FCP, FICON, and Unconfigured.

Accelerator
Displays accelerator adapters of type zEDC. To filter accelerator adapters, click the Accelerator filter icon ().

Crypto
Displays crypto adapters. This includes only adapters of type Crypto. To filter crypto adapters, click the Crypto filter icon ().

Select an Action

The **Adapters** tab includes the following menus and toolbar icons for performing operations against the specified adapters.

Actions menu
To select an action using the **Actions** menu, click on one or more adapters in the table, then select one of the following actions from the **Actions** menu.

Adapter Details
Opens the **Adapter Details** task for each adapter that is selected. This option is enabled only when one or more adapters are selected. For more information about this task, see "Adapter Details" on page 929.

Delete HiperSockets Adapter
Opens the **Delete HiperSockets Adapter** task. This option is enabled only when one (and only one) HiperSockets adapter is selected.

If one or more network interface cards (NICs) are defined for the specified HiperSockets adapter, an error dialog is displayed. This error dialog contains a table that shows the NICs that are defined for the specified adapter. The values that are displayed in the **Name** and **Partition** columns are links that launch the **Adapter Details** and **Partition Details** tasks, respectively. The **Partition Active/Reserved** column shows whether the partition has been started, or if it is reserved. To exit the dialog, click **Close**.

If no NICs are defined for the specified HiperSockets adapter, a confirmation dialog is displayed. This dialog contains the following options:

Delete
To delete the adapter, click **Delete**.

After the adapter has been successfully deleted, the **Validation** dialog appears. Click **Close** to end the task.

Cancel
To cancel the delete action and exit the dialog, click **Cancel**.

Create HiperSockets Adapter
Opens the **Create HiperSockets Adapter** task for the target system. For more information about this task, see "Create HiperSockets Adapter" on page 941.

Reassign Channel Path IDs
Opens the **Reassign Channel Path IDs** task.

Row menu
The **Row** menu contains the same options as the **Actions** menu. To use the **Row** menu, right-click on the row for the adapter that you wish to select, then select an action from the menu.

Toolbar action icons
The table's toolbar provides icons for the **Adapter Details** and **Create HiperSockets** adapter options, which are also included in the **Actions** menu and **Row** menu. The **Adapter Details** option is not available unless one or more rows are selected.

View or Customize Devices

Use the **Devices** tab to view or customize the devices of a DPM-enabled system.

The **Devices** tab consists of the following elements:

- A table that lists the devices that are defined for the target system. See "Select Devices" on page 916.
- A group of filters that help you control the information that is displayed on the table. See "Filter Devices" on page 917.
- Several action menus that allow you to make changes. See "Select an Action" on page 918.

To make a change, use the table and filters to select the new devices, then select an action from one of the action menus.

Select Devices

The **Devices** tab includes a table that lists the devices that have been defined for the partitions on this system. Each table row represents a network interface card (NIC), a host bus adapter (HBA), or a virtual function (VF). Note that HBAs are listed only when the system does not have the DPM R3.1 storage

management feature or a later DPM version applied. If the feature or a later version is applied, no storage devices are included in this table.

Name
Displays the name of a NIC, HBA, or VF. The name is editable.

An icon that represents the type of device also appears next to the name. This icon corresponds to a filter option, through which you can either show or hide all entries for this type of device. If the device is causing, or has the potential to cause a **Degraded** status, this icon is replaced by a warning icon. For information about filters, see “Filter Devices” on page 917.

Partition
Displays the name of the partition that is associated with the device. This value is a link that opens the **Partition Details** task.

Adapter Name
Displays the name of the adapter that is associated with the device. This value is a link that opens the **Adapter Details** task.

Adapter Port
Displays the adapter port value in decimal.

Adapter Type
Indicates the type of adapter, which varies by the device type. Valid values include the following:

- For NICs: HiperSockets, or RoCE, or an abbreviation that starts with the letters "OS" for an OSA adapter
- For HBAs: FCP.
- For VFs: Crypto or zEDS.

Adapter Card Type
Indicates the type of adapter card, which varies depending on the device type and on the adapter cards that the system supports. Valid values include the following:

- For NICs: HiperSockets, or specific OSA Express or RoCE Express adapter names
- For HBAs: specific FICON Express adapter names.
- For VFs: specific zEDS Express adapter names.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the device.

MAC Address
For a NIC only, this entry displays the user-supplied or system-generated MAC address. The address consists of six groups of two lower-case hexadecimal digits, separated by colons; for example: `02:ff:12:34:56:78`

Description
Displays the user-provided description, if any, of the adapter, port, or switch. To edit the existing text or provide a description, double-click in the field and type the new description. To save your changes, press the **Enter** key or click outside the field.

Filter Devices

The **Devices** tab includes a row of filter icons that is used to control the information that is displayed in the table. You can click the filter icon to filter the table. Any row in the table that meets the criteria of the selected filters is displayed.

Note: If the system does not include adapters that apply to a particular filter icon, the corresponding filter icon is not displayed on the **Devices** tab. For example, if no accelerator adapters exist in a system, the Virtual Functions filter icon is not displayed.

The following filter icons are included on the **Devices** tab:

Network Interface Cards
Displays the network interface cards. To filter network interface cards, click the Network filter icon ( ).

Host Bus Adapters
Displays host bus adapters. To filter host bus adapters, click the Storage filter icon ( ). This filter is not available when the system has the DPM R3.1 storage management feature or a later DPM version applied.

Virtual Functions
Displays virtual functions. To filter virtual functions, click the Accelerator filter icon ( ).

Select an Action

The **Devices** tab also includes the following menus and toolbar buttons for performing operations against the specified devices.

Actions menu
To select an action using the **Actions** menu, click on one or more devices in the table, then select one of the following actions from the **Actions** menu.

Partition Details
Opens the **Partition Details** task for the partition of each selected device. This option is enabled only when one or more devices are selected.

Adapter Details
Opens the **Adapter Details** task for the adapter of each selected device. This option is enabled only when one or more devices are selected.

Reassign Devices
Opens the **Reassign Devices** dialog for the selected devices. This option is enabled only when one or more devices are selected. The devices that are selected must all be of the same adapter type. When specifying network interface cards (NICs), the target NICs must all be of the same type; OSA, HiperSockets, or RoCE. Note that this option is available for storage devices only on a system that does not have the DPM R3.1 storage management feature or a later DPM version applied. If the feature or a later version is applied, no host bus adapters (HBAs) are included in the table.

Export WWPNs
Opens the **Export WWPNs** task for each of the selected host bus adapters.

Row menu
To select an action using the **Row** menu, right-click on the row for the device that you wish to select, then select an action from the menu. The **Row** menu contains the same options as the **Actions** menu. Refer to the description of the **Actions** menu for information about these options.

Toolbar action buttons
The table's toolbar provides buttons for the **Partition Details**, **Reassign Devices**, and **Export WWPNs** device options, which are also included in the **Actions** menu and **Row** menu. Refer to the description of the **Actions** menu for information about these options.

Reassign Devices Dialog

Use the **Reassign Devices dialog** to change the adapter, port, or switch for one or more devices (NICs, HBAs, or VFs). This dialog is displayed after the **Reassign Devices** option is specified on the **Devices** tab of the **Manage Adapters** main window. This dialog is available for HBAs only on a system that does not have the DPM R3.1 storage management feature or a later DPM version applied.

The **Reassign Devices dialog** is made up of two tables. The first is a devices table, and the second is an adapter/port/switch table.

Devices table
Lists the target devices and their associated adapters. All of the devices that appear in this table are of the same type; network interface cards (NICs), host bus adapters (HBAs), or virtual functions (VFs). The title and content of this table varies, depending on the type of device that was specified.

Adapter/port/switch table
Lists the selectable adapters, ports, and switches to which the target devices can be reassigned. The title and content of this table varies, depending on the type of device that was specified.

The devices table and adapter/port/switch table also include the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

To perform a reassignment, select an adapter, port, or switch, then click **Reassign**.

The content of the **Reassign Devices dialog** is slightly different, depending on the adapter type of the devices you chose on the **Devices** tab. For information on using the dialog for the device type you chose, refer to one of the following.

- For network interface cards (NICs), see “Reassign Devices dialog - NICs” on page 919.
- For host bus adapters (HBAs), see “Reassign Devices Dialog - HBAs” on page 921.
- For virtual functions (VFs), which are supported only by specific systems, see “Reassign Devices Dialog - VFs” on page 923.

Additional functions on this window include:

Reassign
To change the adapter, port, or switch, for the target devices, click **Reassign**. The **Validation** dialog appears to confirm that the devices have been successfully updated. On the **Validation** dialog, click **Close** to return to the main window.

Cancel

- To close the window without saving any changes, click **Cancel**.
- If you have made changes but did not save them, a confirmation window opens. Click **Yes** to close the window or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Reassign Devices dialog - NICs

Use the **Reassign Devices dialog** to change the ports or switches for one or more network interface cards (NICs). This dialog appears after the **Reassign Devices** option is specified on the **Devices** tab of the **Manage Adapters** main window, and all of the selected devices are NICs.

The **Reassign Devices dialog** for NICs includes a devices table (titled **Target Network Interface Cards**) and an adapter/port/switch table (titled **OSA Switch**, **HiperSockets Switch**, or **RoCE Port**, depending on the type of NIC that was selected).

Use the tables described here to select the ports or switches that should be assigned to the target NICs, then click **Reassign**. For information about the **Reassign** option on this dialog, see “Reassign Devices Dialog” on page 918.

The **Target Network Interface Cards** table provides details about the target devices. The information is arranged into the following columns:

Name
Displays the name of a virtual network interface card (NIC). The name is a hyperlink through which you can open the **NIC Details** window. To edit the name, double-click in the table cell and type the new name.

If this NIC represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Partition
Displays the name of the partition that is associated with this device. This value is a link that opens the **Partition Details** task.

Partition Active/Reserved
Indicates whether the partition has been started, or if it is reserved.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port
Displays the adapter port value in decimal.

Adapter Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the NIC. The operating system to be installed on the partition will use this device number to access the NIC. When creating a new NIC for an OSA card or HiperSockets switch, DPM generates three consecutive device numbers for the operating system to use for unit addresses, and displays only the first number in this field.

Change the device number if your company uses a specific numbering convention for its networks. To edit the device number, double-click in the table cell and type a new hexadecimal value. When you edit the device number for an OSA card or HiperSockets switch, DPM uses this new value as the first device number, and generates two consecutive device numbers based on the new value.

Notes:

- You cannot use a device number of 0000 for a PCI adapter, such as a RoCE adapter.
- The z/VM hypervisor does not support a device number of 0000 for an OSA card or HiperSockets switch.

Description
Displays the user-provided description, if any, of the network interface card. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

The **OSA Switch**, **HiperSockets Switch**, or **RoCE Port** table provides details about the configured ports or switches to which the target NICs can be reassigned. The port or switch that you select on this table is assigned to the target NICs. The information is arranged into the following columns:

Adapter Name
Name of the port or switch's adapter. The names shown in this column are updated dynamically. This value is a link that opens the **Adapter Details** task.

Adapter Port
Index of the adapter port.

Card Type
Card type of the adapter.

Utilization
Progress bar that displays the average uplink utilization for the port or switch during the last five minutes. For OSA and RoCE, the physical port utilization is displayed. For HiperSockets, the switch utilization is displayed.

Adapter NIC Allocation
Progress bar that displays the percentage of NICs that can be defined on an adapter. This value includes only NICs of active and reserved partitions.

If you place your cursor over a cell in the column, two values are displayed, as follows.

- The progress bar value (percentage of NICs that can be defined on the adapter for active and reserved partitions).
- The allocation for all defined partitions, including partitions that are inactive. This value can exceed 100 percent.

If the selected adapter port or switch does not have sufficient allocation space for the NICs, a warning or error message is displayed directly above the table.

Location
Location of the port or switch.

Description
User-defined description of the port or switch. If a value is not displayed, the adapter description serves as the port or switch description. The descriptions shown in this column are updated dynamically.

The **OSA Switch**, **HiperSockets Switch**, and **RoCE Port** tables also include the following menus for performing operations that are related to the specified port or switch.

Actions menu
To use the **Actions menu**, select a port or switch in the table, then select an option from the **Actions menu**.

The **Actions menu** contains the following options:

Adapter Details
Opens the **Adapter Details** task for the specified port or switch's adapter. This option is enabled only when a port or switch is selected.

Row menu
To use the **Row menu**, double-click on the row for the port or switch that you wish to select, then select an action from the menu. The **Row menu** contains the same option as the **Actions menu**; **Adapter Details**. Refer to the description of the **Actions menu** for information about this option.

Reassign Devices Dialog - HBAs

Use the **Reassign Devices dialog** to change the port for one or more host bus adapters (HBAs). This dialog appears after the **Reassign Devices** option is specified on the **Devices** tab of the **Manage Adapters** main window, and all of the selected devices are HBAs. This dialog is available only on a system that does not have the DPM R3.1 storage management feature or a later DPM version applied.

Use the tables described here to select the port that should be assigned to the target HBAs, then click **Reassign**. For information about the **Reassign** option on this dialog, see “Reassign Devices Dialog” on page 918.

The **Reassign Devices dialog** for host bus adapters includes a devices table (titled **Target Host Bus Adapters**) and a port table (titled **FCP Port**).

The **Target Host Bus Adapters** table provides details about the target devices. The information is arranged into the following columns:

Name
Displays the name of a host bus adapter (HBA). The name is a hyperlink through which you can open the **HBA Details** window. To edit the name, double-click in the table cell and type the new name.

If this HBA represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Partition
Displays the name of the partition that is associated with this device. This value is a link that opens the **Partition Details** task.

Partition Active/Reserved
Indicates whether the partition has been started, or if it is reserved.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the HBA. The operating system to be installed on the partition will use this device number to access the HBA. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by selecting the **Details** action and editing the HBA device number. To edit the device number, double-click in the table cell and type a new hexadecimal value.

Description
Displays the user-provided description, if any, of the host bus adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

The **FCP Port** table provides details about the configured FCP ports to which the target HBAs can be reassigned. The port that you select on this table is assigned to the target HBAs. The information is arranged into the following columns:

Adapter Name
Name of the port's adapter. The names shown in this column are updated dynamically. This value is a link that opens the **Adapter Details** task.

A warning icon is displayed beside the adapter name if selecting that port would cause the HBA and, therefore its partition, to become degraded.

Card Type
Card type of the adapter.

Adapter HBA Allocation
Progress bar that displays the percentage of HBAs that can be defined on an adapter. This value includes only HBAs of active and reserved partitions.

If you place your cursor over a cell in the column, two values are displayed, as follows.

- The progress bar value (percentage of HBAs that can be defined on the adapter for active and reserved partitions).
- The allocation for all defined partitions, including partitions that are inactive. This value can exceed 100 percent.

If the selected adapter port does not have sufficient allocation space for the HBAs, a warning or error message is displayed directly above the table.

Fabric ID
World Wide Name (WNN) of the uplink Fibre Channel switch.

Location
Location of the port.

Description
User-defined description of the port. If a value is not displayed, the adapter description serves as the port description. The descriptions shown in this column are updated dynamically.

Actions menu
To use the **Actions menu**, select a port in the table, then select an option from the **Actions menu**.

The **Actions menu** contains the following options:

Adapter Details
Opens the **Adapter Details** task for the specified port. This option is enabled only when a port is selected.

Row menu
To use the **Row menu**, double-click on the row for the port that you wish to select, then select an action from the menu. The **Row menu** contains the same option as the **Actions menu**; **Adapter Details**. Refer to the description of the **Actions menu** for information about this option.

Reassign Devices Dialog - VFs

Use the **Reassign Devices** dialog to change the adapter for one or more virtual functions (VFs), which are supported only by specific systems. This dialog appears after the **Reassign Devices** option is specified on the **Devices** tab of the **Manage Adapters** main window, and all of the selected devices are VFs.

The **Reassign Devices** dialog for VFs includes a devices table (titled **Target Virtual Functions**) and an adapter/port/switch table (titled **Adapter**).

Use the tables described here to select the adapters that should be assigned to the target VFs, then click **Reassign**. For information about the **Reassign** option, see “Reassign Devices Dialog” on page 918.

The **Target Virtual Functions** table provides details about the target devices. The information is arranged into the following columns:

Name
Displays the name of the virtual function. The name is a hyperlink through which you can open the **Virtual Function Details** window. To edit the name, double-click in the table cell and type the new name.

If this virtual function represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Partition
Displays the name of the partition that is associated with this device. This value is a link that opens the **Partition Details** task.

Partition Active/Reserved
Indicates whether the partition has been started, or if it is reserved.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the virtual function. The operating system to be installed on the partition will use this device number to access the virtual function.

Change the device number if your company uses a specific numbering convention for its accelerators. To edit the device number, double-click in the table cell and type a new hexadecimal value. Note that you cannot use a device number of 0000 for accelerator adapters.

Description
Displays the user-provided description, if any, of the virtual function. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

The **Adapter** table provides details about the configured adapters to which the target VFs can be reassigned. The adapter that you select on this table is assigned to the target VFs. The information is arranged into the following columns:

Name
Name of the adapter. The names shown in this column are updated dynamically. This value is a link that opens the **Adapter Details** task.

A warning icon is displayed beside the adapter name if selecting that port would cause the virtual function and, therefore its partition, to become degraded.

Card Type
Card type of the adapter.

Utilization
Progress bar that displays the average uplink utilization for the adapter during the last five minutes.

Virtual Function Allocation
Progress bar that displays the percentage of VFs that can be defined on an adapter. This value includes only VFs of active and reserved partitions.

If you place your cursor over a cell in the column, two values are displayed, as follows.

- The progress bar value (percentage of VFs that can be defined on the adapter for active and reserved partitions).
- The allocation for all defined partitions, including partitions that are inactive. This value can exceed 100 percent.

If the selected adapter does not have sufficient allocation space for the VFs, a warning or error message is displayed directly above the table.

Location
Location of the adapter.

Description
User-defined description of the adapter. The descriptions shown in this column are updated dynamically.

The Adapter table also includes the following menus for performing operations that are related to the specified adapter.

Actions menu
To use the **Actions menu**, select an adapter in the table, then select an option from the **Actions menu**.

The **Actions menu** contains the following options:

Adapter Details
Opens the **Adapter Details** task for the specified port adapter. This option is enabled only when an adapter is selected.

Row menu
To use the **Row menu**, double-click on the row for the adapter that you wish to select, then select an action from the menu. The **Row menu** contains the same option as the **Actions menu**; **Adapter Details**. Refer to the description of the **Actions menu** for information about this option.

View or Customize Cryptos

Use the **Cryptos** tab to view or customize the adapters or partitions of a DPM-enabled system.

The **Cryptos** tab consists of the following elements:

- A table that lists the crypto adapters that are defined for the target system. See "Select Adapters or Partitions" on page 925.
- A table that lists the partitions that are defined to use the crypto adapters of the target system. See "Select Adapters or Partitions" on page 925
- Several action menus that allow you to make changes. See "Select an Action" on page 927.

Use the tables to select an adapter or partition, then select an action from one of the tab's action menus.

Select Adapters or Partitions

The **Cryptos** tab includes an adapters table (titled **Crypto Adapters**) that lists the adapters that are defined for the target system. It also includes a partitions table (titled **Partitions**) that lists the partitions that are defined for the adapters. These tables are updated dynamically, so that they always reflect the current adapters and partitions, and their values.

The **Crypto Adapters** table and **Partitions** table also include the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Use the tables described here to select the adapters or partitions that you want to view or customize, then select an action from one of the action menus (see "Select an Action" on page 927).

Crypto Adapters Table

The **Crypto Adapters** table provides details about the defined crypto adapters. The information is arranged into the following columns:

Name
Name of the adapter. This value is a link that opens the **Adapter Details** task. The adapter name is editable. If the device is causing, or has the potential to cause a **Degraded** status, a warning icon is displayed beside the name.

Conflicts
Whether or not there are any conflicts. A conflict exists when the same usage domain and crypto adapter are defined to multiple partitions. Exactly one of the conflicting partitions can be active or reserved simultaneously. When a conflict exists, a warning icon is displayed. To view the conflict, click on the warning icon or use the **View Conflicts** action in the **Actions** menu of the **Crypto Adapters** table to open the "Crypto Conflicts - adapter" on page 928.

Type
Type of adapter.

Status
Status of the adapter. The adapter status values include the following:

Active
Indicates that the adapter is operating normally.

Exceptions
Indicates that at least one adapter on the system is not operating.

Not active
Indicates that the adapter is not operating.

Service

State
State of the adapter. A value appears in this column for adapters only (not for ports or switches).

Crypto Number
Card type of the adapter. A value appears in this column for adapters only (not for ports or switches).

UDX-Loaded
Whether a User Defined Extension (UDX) file was installed for the crypto adapter.

Card Type
Card type of the crypto adapter.

Location
Location of the crypto adapter.

Number of Partitions
Number of partitions whose devices are defined to use the adapter.

When you click on a value in this column for a particular adapter, a table is displayed, which provides information about the partitions that are configured to use the crypto adapter. The adapter name is shown at the top of the window. The values that are displayed in the **Partition** column are links that open the **Partition Details** task. The **Active/Reserved** column shows whether the partition has been started, or if it is reserved. The partitions table is updated dynamically as an adapter's partition count changes and as a crypto's configuration changes.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the field and type the new description. To save your changes, press the **Enter** key or click outside the field.

Partitions Table

The **Partitions** table provides details about the partitions that are defined to use crypto adapters. The information is arranged into the following columns:

Name
Name of the partition. This value is a link that opens the **Partition Details** task.

Conflicts
Whether or not there are any conflicts. A conflict exists when a partition's adapters and usage domains conflict with another defined partition. In this case, both could not be active or reserved at the same time. When a conflict exists, a warning icon is displayed. To view the conflict, click on the warning icon or use the **View Conflicts** action in the **Actions** menu of the **Partitions** table to open the “Crypto Conflicts - partition” on page 928.

Active/Reserved
Whether the partition has been started, or if it is reserved.

Adapters (Crypto Numbers)
List of crypto adapters that are assigned to the partition, and the Adjunct Processor (AP) numbers of those cryptos. AP numbers range from 1 to 10. Each adapter in the list is a link that opens the **Adapter Details** task.

Usage Domains
Usage domains used by the partition. A logical partition's control and usage domains are domains in the cryptos that can be used for cryptographic functions. The usage domain assignment, in combination with the Cryptographic Number must be unique across all partitions defined to the CPC.

Control Domains
Control domains used by the partition. A logical partition's control domains are those cryptographic domains for which remote secure administration functions can be established and administered from this logical partition. This value includes the usage domains.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the field and type the new description. To save your changes, press the **Enter** key or click outside the field.

Select an Action

The **Cryptos** tab includes the following menus and toolbar buttons for performing operations against the specified adapters or partitions.

Crypto Adapters Table Menus

Actions menu
To select an action using the **Actions** menu, click on an adapter in the table, then select one of the following options from the **Actions** menu.

Details
>Opens the **Adapter Details** task for the specified adapter. This option is enabled only when one or more adapters is selected.

View Conflicts
Opens the **Adapter Crypto Conflicts** dialog for the selected adapters. This option is enabled when one, and only one, adapter is selected, and that adapter has conflicts.

Row menu
To select an action using the **Row** menu, right-click on the row for the device that you wish to select, then select an action from the menu. The **Row** menu contains the same options as the **Actions** menu. Refer to the description of the **Actions** menu for information about these options.

Toolbar action buttons
The table's toolbar provides buttons for the **Details** and **View Conflicts** options, which are also included in the **Actions** menu and **Row** menu. Refer to the description of the **Actions** menu for information about these options.

Partitions Table Menus

Actions menu
To select an action using the **Actions** menu, click on one or more partitions in the table, then select one of the following options from the **Actions** menu.

Details
Opens the **Partition Details** task for the specified partition. This option is enabled only when one or more partitions are selected.

View Conflicts
Opens the **Partition Crypto Conflicts** dialog for the selected partition. This option is enabled when one, and only one, partition is selected, and that partition has conflicts.

Row menu
To select an action using the **Row** menu, right-click on the row for the device that you wish to select, then select an action from the menu. The **Row** menu contains the same options as the **Actions** menu. Refer to the description of the **Actions** menu for information about these options.

Toolbar action buttons
The table's toolbar provides buttons for the **Details** and **View Conflicts** options, which are also included in the **Actions** menu and **Row** menu. Refer to the description of the **Actions** menu for information about these options.

Crypto Conflicts - adapter

Use the **Crypto Conflicts** window to view the details about partitions that are defined to use the same usage domain as the target crypto adapter. Use the **Partition Details** task to remove the usage domain from one of the partitions to resolve the conflict.

The **Crypto Conflicts** window contains the **Conflicting Partitions** table, which provides the following information. If all conflicts are resolved, this table does not contain any partitions.

Partition
Name of the conflicting partition. This value is a link that opens the **Partition Details** task to resolve the conflict.

Active/Reserved
Whether the partition has been started, or if it is reserved.

Usage Domains
Set of usage domains that are assigned to the partitions that are in conflict with the target partition.

The **Conflicting Partitions** table also includes the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Additional functions on this window include:

Close
To exit the **Crypto Conflicts** window, click **Close**.

Help
To display help for the current window, click **Help**.

Crypto Conflicts - partition

Use the **Crypto Conflicts** window for partitions to view details about partitions that are defined to use the same usage domain and crypto adapter as the target crypto partition. Use the **Partition Details** task to remove the conflicting usage domain from one of the partitions.

The **Crypto Conflicts** window contains the **Conflicting Partitions** table, which provides the following information. If all conflicts are resolved, this table does not contain any partitions.

Partition
Name of the conflicting partition. This value is a link that opens the **Partition Details** task to resolve the conflict.

Active/Reserved
Whether the partition has been started, or if it is reserved.

Adapters (Crypto Numbers)
List of crypto adapters that are assigned to the partition, and the Adjunct Processor (AP) numbers of those cryptos. AP numbers range from 1 to 10. Each adapter in the list is a link that opens the **Adapter Details** task.

Usage Domains
Set of usage domains that are assigned to the partitions that are in conflict with the target partition.

The **Conflicting Partitions** table also includes the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose

the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Additional functions on this window include:

Close
To exit the **Crypto Conflicts** window, click **Close**.

Help
To display help for the current window, click **Help**.

Adapter Details

Use the **Adapter Details** task to view or modify the adapter settings of the selected adapter.

Note that when this task is launched in view-only mode, the information in the **Adapter Details** window is not editable. If the status of the adapter is **Not configured**, the **Adapter Details** task window is displayed as view-only.

The content of the Adapter Details main window varies, depending on the adapter type. Use one of the following links:

- Adapters of type OSD, RoCE, HiperSockets, and OSM. See "View or Modify OSD, RoCE, HiperSockets and OSM adapters" on page 930.
- Adapters of type NVMe, FCP, FICON, and Unconfigured. See "View or Modify NVMe, FCP, FICON, and Unconfigured Adapters" on page 932.
- Adapters of type zEDC, which are supported only by specific systems. See "View or Modify zEDC Adapters" on page 935.
- Adapters of type Crypto. See "View or Modify Crypto Adapters" on page 938.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

Additional functions on this window include:

Related Tasks
Depending on the target adapter type, provides a hyperlink to the following task:

- **Monitor System**. Opens the **Monitor System** task for the target adapter. The link for this task is displayed only if the target adapter is configured.

OK
To close the window, click **OK**. If you made changes in editable fields in the window, those changes are applied. This option is not displayed in view-only mode.

Apply
To apply changes you made in editable fields on the page, click **Apply**.If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to apply the changes or **Cancel** to return to the previous window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window. This option is not displayed in view-only mode.

Close
To close the window, click **Close**. This option is displayed only in view-only mode.

Help
To display help for the current window, click **Help**.

View or Modify OSD, RoCE, HiperSockets and OSM adapters

Use the **Adapter Details** page to view or modify the adapter settings for adapters of type OSD, RoCE, HiperSockets, and OSM.

The name of the target adapter is displayed at the top of the window.

The **Adapter Details** page provides a **General** area, in which you can make modifications to general details about the adapters. It also includes a devices table, called **Network Interface Cards**, that allows you to view the devices to which those changes should apply.

View or Modify General Details

The following information is displayed in the **General** area for the target adapter. Modify the details here, as needed.

Notes:

- An asterisk (*) preceding the label indicates that a value is required; other values are optional.
- The fields that are included on this page vary, depending on adapter type. The differences are noted in this list.

Name
Specifies the name of the target adapter, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. An adapter name must uniquely identify the adapter from all other adapters defined on the same system.

This field is updated dynamically, so that it always reflects the current name of the target adapter.

Description
Specifies the user-supplied description, if any, of the target adapter. The description can be up to 1024 characters in length. There are no character restrictions.

This field is updated dynamically, so that it always reflects the current description of the target adapter.

Object ID
Object ID of the target adapter. This is a read-only field.

System
Name of the system.

Status
Status of the target adapter. This field is updated dynamically, so that it always reflects the current status of the target adapter.

Detailed Status
Physical Channel ID (PCHID) status of the target adapter.

State
State of the adapter. This field is updated dynamically, so that it always reflects the current state of the target adapter.

NIC allocation
Network interface card (NIC) allocation for adapters of type OSD, HiperSockets, or RoCE. Displays a progress bar that shows the percentage of NICs that can be defined on the adapter. This value includes only NICs of active or reserved partitions. The NIC allocation value can exceed 100 percent.

If you place your cursor over the **NIC allocation** field, two values are displayed, as follows.

- The progress bar value (percentage of NICs that can be defined on the target adapter, for active and reserved partitions only).
- The allocation for all defined partitions, including partitions that are inactive. The allocation value for all defined partitions can exceed 100 percent.

The **NIC allocation** field is updated dynamically, so that it always reflect the current allocation value of the target adapter.

Adapter ID
ID (four-character PCHID value) of the target adapter.

Adapter type
Adapter type of the target adapter.

Channel path ID (OSD, OSM, and HiperSockets adapters only)
Channel path ID of the adapter. The value that is shown is a link that opens the **Reassign Channel Path IDs** task. This field is updated dynamically, so that it always reflects the current channel path ID of the target adapter. See “Reassign Channel Path IDs” on page 942 for more information.

Card type
Card type of the target adapter.

Location
Location of the target adapter.

LED
Current state of the target adapter's LED. Click anywhere on the switch to toggle the LED on or off. The switch corresponds to the physical LED light that is above the card in the cage.

Switches (OSD adapters only)
Description of the target adapter's switches. The **Switches** table displays the adapter's switches and their related descriptions. The descriptions are editable.

Ports (RoCE adapters only)
Description of the target adapter's ports. The **Ports** table displays the adapter's ports and their related descriptions. The descriptions are editable.

MTU frame size (HiperSockets adapters only)
Current MTU frame size. Use the drop down menu to define a maximum frame size, based on the traffic characteristics of each HiperSocket adapter. Choose from the following values: 8/16, 16/24, 32/40, or 56/64.

Switch description (HiperSockets adapters only)
Description of the target adapter's switch.

Network Interface Cards Table

The **Network Interface Cards** table allows you to view the NICs to which changes to OSD, RoCE, and HiperSockets adapters should apply. A devices table is not included for OSM adapters. Each NIC appears in its own row in the table, and the information is arranged into the following columns.

Name
Name of the adapter.

Partition
Name of the adapter's partition. This value is a link that opens the **Partition Details** task.

Partition Active/Reserved
Whether the partition has been started, or if it is reserved.

Port
Port that is used by the adapter.

Device Number
Four-digit hexadecimal value for the device.

Description
User-defined description of the device.

The **Network Interface Cards** table includes the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose

the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

After making changes and selecting adapters, click one of the following buttons:

OK
To close the window, click **OK**. If you made changes in editable fields in the window, those changes are applied. The **OK** option is not displayed in view-only mode.

Apply
To apply changes you made in editable fields on the page, click **Apply**. If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to apply the changes or **Cancel** to return to the previous window.

This option is not displayed in view-only mode.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window. This option is not displayed in view-only mode.

View or Modify NVMe, FCP, FICON, and Unconfigured Adapters

Use the **Adapter Details** page to view or modify the adapter settings for NVMe, FCP, FICON, and Unconfigured adapters. The name of the target adapter is displayed at the top of the window.

The **Adapter Details** page consists of two sections: a General section and either a Host Bus Adapters section or a Connections section. The Connections section is displayed only when the system has the DPM R3.1 storage management feature or a later DPM version applied. For Unconfigured adapters, the Connections section contains an empty table.

General section

The following information is displayed in the General section for the target adapter. The fields in this display vary, depending on the version of DPM that is applied on the system. Modify the details here, as needed.

An asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Specifies the name of the target adapter, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. An adapter name must uniquely identify the adapter from all other adapters defined on the same system.

This field is updated dynamically, so that it always reflects the current name of the target adapter.

Description
Specifies the user-supplied description, if any, of the target adapter. The description can be up to 1024 characters in length. There are no character restrictions.

This field is updated dynamically, so that it always reflects the current description of the target adapter.

Object ID
Object ID of the target adapter. This is a read-only field.

System
Name of the system.

Status
Status of the target adapter. This field is updated dynamically, so that it always reflects the current status of the target adapter.

Detailed Status
Physical Channel ID (PCHID) status of the target adapter.

State
State of the adapter. This field is updated dynamically, so that it always reflects the current state of the target adapter.

Adapter allocation
For FICON adapters, the percentage of adapter resources that are allocated to started and reserved partitions. For NVMe adapters, the allocation value is either 0 (when the adapter is available for use) or 100 (when a partition is using the adapter).

HBA allocation
For FCP adapters, the host bus adapter (HBA) allocation displays a progress bar that shows the percentage of HBAs that can be defined on the adapter. The percentage value includes only HBAs of active or reserved partitions.

If you place your cursor over the **HBA allocation** field, two values are displayed, as follows.

- The progress bar value (percentage of HBAs that can be defined on the target adapter, for active and reserved partitions only).
- The allocation for all defined partitions, including partitions that are inactive. The allocation value for all defined partitions can exceed 100 percent.

The **HBA allocation** field is updated dynamically, so that it always reflect the current allocation value of the target adapter.

Maximum HBAs
For FCP adapters, the maximum number of HBAs that can be active or reserved for the target adapter. Click the up and down arrows to modify this value or type a value in the field. Valid values are in the range 0 - 254. If the specified value is out of range, or is not a valid number, an error message is displayed. Note that the maximum number of HBAs cannot be less than the number of allocated HBAs.

When this value is modified, the value shown in the **HBA allocation** field is recalculated.

Fabric ID
For adapters of type FCP and Unconfigured, the World Wide Name (WNN) of the uplink Fibre Channel switch.

Physically connected to
For FICON adapters, the name of a switch or storage subsystem to which this adapter is physically connected. The name is a hyperlink that opens to the Configure FICON Connections page in the **Configure Storage** task.

Adapter ID
ID (four-character PCHID value) of the target adapter.

Adapter type
Adapter type of the target adapter. Only when the system has the DPM R3.1 storage management feature or a later DPM version applied, the field value is a link to the **Configure Storage Cards** page of the **Configure Storage** task. Hover help identifies the adapter card in the display on the **Configure Storage Cards** page.

Channel path ID (CHPID)
Channel path ID of the adapter. The value shown is a link that opens the **Reassign Channel Path IDs** task. This field is updated dynamically, so that it always reflects the current channel path ID of the target adapter. See “Reassign Channel Path IDs” on page 942 for more information.

Card type
Card type of the target adapter.

Optic type
For FICON adapters, the type of fiber optic cables.

Location
The location of the target adapter.

LED
Current state of the target adapter's LED. Click anywhere on the switch to toggle the LED on or off. The switch corresponds to the physical LED light that is above the card in the cage.

Port description
For FCP or FICON adapters, the user-supplied description, if any, of the adapter port. The description can be up to 1024 characters in length.

Vendor ID
For NVMe adapters, the vendor ID indicates the manufacturer of the installed SSD.

Subsystem vendor ID
For NVMe adapters, the subsystem vendor ID indicates the manufacturer of the installed SSD.

Model number
For NVMe adapters, the model number of the installed SSD.

Serial number
For NVMe adapters, the serial number of the installed SSD.

Capacity
For NVMe adapters, the size of the installed SSD in gibibytes (GiB).

Host Bus Adapters section

The Host Bus Adapters section contains a table that lists the HBAs to which changes to FCP adapters should apply. Each HBA appears in its own row in the table, and the information is arranged into the following columns.

The Host Bus Adapters table includes the following information.

Name
Name of the adapter.

Partition
Name of the adapter's partition. This value is a link that opens the **Partition Details** task.

Partition Active/Reserved
Whether the partition has been started, or if it is reserved.

Device Number
Four-digit hexadecimal value for the device.

WWPN
Worldwide port name of the device.

Description
User-defined description of the device.

The **Host Bus Adapters** table includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Connections section

The Connections section contains a table that lists storage groups and partitions that are using the target adapter, and a separate table that lists tape links and partitions that are using the same adapter.

Storage Groups table
The Storage Groups table is empty under the following conditions:

- The adapter is not configured as either FCP or FICON.
- The adapter is not being used by any storage groups.

Storage Group
Name of an FCP or FICON or NVMe storage group that is using this adapter. The name is a hyperlink that opens the Storage Group Details page of the **Configure Storage** task.

Partition
Name of the partition that is using this adapter through the attached storage group. The name is a link that opens the **Partition Details** task. This field is empty when none of the listed storage groups are attached to a partition.

Partition Active/Reserved
Indicates whether the partition is active or reserved. A check mark indicates that the partition is either active, reserved, or both; a dash indicates that the partition is not active or reserved.

HBA Name
Name of the host bus adapter through which the partition can access the adapter. This column is shown in the table for FCP adapters only.

WWPN
Worldwide port name of the HBA. This column is shown in the table for FCP adapters only.

Device Number
Four-digit hexadecimal device number for the HBA. This column is shown in the table for FCP adapters only.

Tape Links table
The Tape Links table is empty under the following conditions:

- The adapter is not configured as FCP.
- The adapter is not being used by any tape links.

Tape Link
Name of an FCP tape link that is using this adapter. The name is a hyperlink that opens the Tape Link details page of the **Configure Storage** task.

Partition
Name of the partition that is using this adapter through the attached storage group. The name is a link that opens the **Partition Details** task. This field is empty when none of the listed storage groups are attached to a partition.

Partition Active/Reserved
Indicates whether the partition is active or reserved. A check mark indicates that the partition is either active, reserved, or both; a dash indicates that the partition is not active or reserved.

HBA Name
Name of the host bus adapter through which the partition can access the adapter.

WWPN
Worldwide port name of the HBA.

Device Number
Four-digit hexadecimal device number for the HBA.

View or Modify zEDC Adapters

Use the **Adapter Details** page to view or modify the adapter settings for adapters of type zEDC, which are supported only by specific systems.

The name of the target adapter is displayed at the top of the window.

The **Adapter Details** page provides a **General** area, in which you can make modifications to general details about the adapters. It also includes a devices table, called **Virtual Functions**, that allows you to select the adapters to which those changes should apply.

View or Modify General Details

The following information is displayed in the **General** area for the target adapter. Modify the details here, as needed.

An asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Specifies the name of the target adapter, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. An adapter name must uniquely identify the adapter from all other adapters defined on the same system.

This field is updated dynamically, so that it always reflects the current name of the target adapter.

Description
Specifies the user-supplied description, if any, of the target adapter. The description can be up to 1024 characters in length. There are no character restrictions.

This field is updated dynamically, so that it always reflects the current description of the target adapter.

Object ID
Object ID of the target adapter. This is a read-only field.

System
Name of the system.

Status
Status of the target adapter. This field is updated dynamically, so that it always reflects the current status of the target adapter.

Detailed Status
Physical Channel ID (PCHID) status of the target adapter.

State
State of the adapter. This field is updated dynamically, so that it always reflects the current state of the target adapter.

Virtual function allocation
For adapters of type zEDC. Displays a progress bar that shows the percentage of virtual functions that can be defined on the adapter. This value includes only VFs of active or reserved partitions.

If you place your cursor over any of the allocation fields, two values are displayed, as follows.

- The progress bar value (percentage of virtual functions that can be defined on the target adapter, for active and reserved partitions only).
- The allocation for all defined partitions, including partitions that are inactive. The allocation value for all defined partitions can exceed 100 percent.

The **Virtual function allocation** field is updated dynamically, so that it always reflects the current allocation value of the target adapter.

Adapter ID
ID (four-character PCHID value) of the target adapter.

Adapter type
Adapter type of the target adapter.

Channel path ID (OSD, OSM, and HiperSockets adapters only)
Channel path ID of the adapter. The value shown is a link that opens the Reassign Channel Path IDs task. This field is updated dynamically, so that it always reflects the current channel path ID of the target adapter.

Card type
Card type of the adapter.

Location
Location of the target adapter.

LED
Current state of the target adapter's LED. Click anywhere on the switch to toggle the LED on or off. The switch corresponds to the physical LED light that is above the card in the cage.

Select Adapters

This page includes a devices table called **Virtual Functions**, which lists the zEDC adapters that have been assigned to the target adapter. After making changes in the **General** area of this page, use the table to select the adapters to which you want those changes to apply.

The **Virtual Functions** table provides details about adapters of type zEDC. Each adapter appears in its own row in the table, and the information is arranged into the following columns.

Name
Name of the adapter.

Partition
Name of the adapter's partition. This value is a link that opens the **Partition Details** task.

Partition Active/Reserved
Whether the partition has been started, or if it is reserved.

Port
Port that is used by the adapter.

Device Number
Four-digit hexadecimal value for the device.

Description
User-defined description of the device.

The **Virtual Functions** table includes the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

After making changes and selecting adapters, click one of the following buttons:

OK
To close the window, click **OK**. If you made changes in editable fields in the window, those changes are applied. This option is not displayed in view-only mode.

Apply
To apply changes you made in editable fields on the page, click **Apply**.If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to apply the changes or **Cancel** to return to the previous window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window. This option is not displayed in view-only mode.

View or Modify Crypto Adapters

Use the **Adapter Details** page to view or modify the adapter settings of type Crypto.

The name of the target adapter is displayed at the top of the window.

The **Adapter Details** page provides a **General** area, in which you can make modifications to general details about the adapters. It also includes a devices table, called **Assigned Domains**, that allows you to select the domains to which those changes should apply.

View or Modify General Details

The following information is displayed in the **General** area for the target adapter. Modify the details here, as needed.

An asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Specifies the name of the target adapter, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. An adapter name must uniquely identify the adapter from all other adapters defined on the same system.

This field is updated dynamically, so that it always reflects the current name of the target adapter.

Description
Specifies the user-supplied description, if any, of the target adapter. The description can be up to 1024 characters in length. There are no character restrictions.

This field is updated dynamically, so that it always reflects the current description of the target adapter.

Object ID
Object ID of the target adapter. This is a read-only field.

System
Name of the system.

Status
Status of the target adapter. This field is updated dynamically, so that it always reflects the current status of the target adapter.

Detailed Status
Physical Channel ID (PCHID) status of the target adapter.

State
State of the target adapter. This field is updated dynamically, so that it always reflects the current state of the target adapter.

Usage domain allocation
Usage domain allocation for adapters of type Crypto. Displays a progress bar that shows the percentage of usage domains that can be defined on the adapter. This value includes only domains of active or reserved partitions.

If you place your cursor over any of the allocation fields, two values are displayed, as follows.

- The progress bar value (percentage of usage domains that can be defined on the target adapter, for active and reserved partitions only).
- The allocation for all defined partitions, including partitions that are inactive. The allocation value for all defined partitions cannot exceed 100 percent.

The **Usage domain allocation** field is updated dynamically, so that it always reflects the current allocation value of the target adapter.

Adapter ID
ID (four-character PCHID value) of the target adapter.

Adapter type
Adapter type of the target adapter.

Card type
Card type of the adapter.

Location
Location of the target adapter.

LED
Current state of the target adapter's LED. Click anywhere on the switch to toggle the LED on or off. The switch corresponds to the physical LED light that is above the card in the cage.

Crypto number
Crypto adapter's AP number. This is a read-only value.

Crypto type
Crypto adapter type. Use the drop down menu to modify this value. The valid options are:

- **Accelerator**
- **CCA coprocessor**
- **EP11 coprocessor**.

Note: When changing the **Crypto type** from **Accelerator** to **CCA coprocessor**, the adapter is not zeroized. If the current **Crypto type** is **CCA coprocessor**, and you change it to **Accelerator**, you are prompted with a choice of whether to zeroize or not zeroize the crypto. For all other changes to the **Crypto type**, the adapter is automatically zeroized.

UDX-loaded
Whether the crypto is UDX-loaded or UDX-unloaded. One of the following values is displayed.

Yes
The crypto is UDX-loaded. After this value is known, it is remembered, which allows it to be displayed even if the crypto is offline.

No
The crypto is UDX-unloaded. After this value is known, it is remembered, which allows it to be displayed even if the crypto is offline.

Unknown
It is not known if it is UDX-loaded or UDX-unloaded.

Permit TKE commands
Permit the Trusted Key Entry (TKE) workstation to manage secure functions of the cryptographic coprocessor. To enable this function, select the check box. To disable this function, unselect the check box.

Note: Only enable this option if you will be using the TKE workstation. Permitting TKE access with the default TKE communication keys set can allow unauthorized access. For security reasons, you should immediately change the default value of the keys from the TKE workstation after permitting TKE commands.

When the value that is specified in the **Crypto type** field is:

- **EP11 coprocessor**, the check box is checked by default and is not editable (this option cannot be disabled if the crypto type is **EP11 coprocessor**).
- **Accelerator**, the check box is unchecked and is not editable (this option cannot be enabled if the crypto type is **Accelerator**.

Assigned Domains Table

The **Assigned Domains** table allows you to view the domains to which changes to Crypto adapters should apply. Each domain appears in its own row in the table, and the information is arranged into the following columns.

Domain Index
The domain index of the adapter.

Partition
Name of the adapter's partition. This value is a link that opens the **Partition Details** task.

Partition Active/Reserved
Whether the partition has been started, or if it is reserved.

Domain Type
Type of domain. Usage indicates Usage and Control. Control indicates strictly Control domain.

The **Assigned Domains** table includes the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

After making changes and selecting adapters, click one of the following buttons:

OK
To close the window, click **OK**. If you made changes in editable fields in the window, those changes are applied. This option is not displayed in view-only mode.

Apply
To apply changes you made in editable fields on the page, click **Apply**.If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to apply the changes or **Cancel** to return to the previous window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window. This option is not displayed in view-only mode.

Confirm Disruptive Action Dialog

Use the **Confirm Disruptive Action** dialog to confirm that you want to make the changes that you specified on the **Adapter Details** task window, even though those changes will affect active partitions.

The **Confirm Disruptive Action** dialog is displayed after you click **OK** or **Apply** on the **Adapter Details** task page, and the specified changes will affect the active operations of partitions. This dialog is displayed if one or both of the following disruptive changes are made:

- The **MTU/frame size** is changed, and the adapter backs active partitions
- The **Crypto type** is changed, and the adapter backs active partitions.

On the **Confirm Disruptive Action** dialog, do the following.

1. Review the **Disrupted Partitions** table, which provides information about all active partitions that have a device that is backed by the target adapter. The **Disrupted Partitions** table includes the following information.

   Name
   Name of the disrupted partition.

System
System that is associated with the disrupted partition.

Status
Status of the disrupted partition.

OS Name
Operating system name that is associated with the disrupted partition.

Confirmation Text
User confirmation that the action will disrupt a partition's operations. Type the partition's **Name** or **OS name** in this field to confirm.

2. If you agree with the changes that are described on this dialog, enter the HMC System Programmer (SYSPROG) password in the **SYSPROG password** field (required).
3. Click **Update Adapter** to make the updates to the adapter.

Additional functions on this window include:

Cancel

- To close the window without saving any changes, click **Cancel**.
- If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Create HiperSockets Adapter

HiperSockets, which provide high-speed communications between partitions within a single system, without the need for any physical cabling or external networking connections. The communication is through the system memory, so a HiperSockets adapter and switch provide access to an I/O channel that is analogous to an internal local area network (LAN).

A HiperSockets adapter supports several different maximum frame size (MFS) settings to accommodate different bandwidth requirements. Through the **Create HiperSockets Adapter** window, you can adjust the MFS setting. The MFS setting determines the size of the largest packet that TCP/IP can transmit; on activation, TCP/IP adjusts its maximum transmission unit (MTU) according to the value of the MFS setting. All partitions that use the same HiperSockets adapter for communication also use the same MFS setting.

Create one HiperSockets adapter and switch for each set of partitions that will use HiperSockets for communication. For example, on a single DPM-enabled system, you might have one set of partitions that support an internal company payroll application, and a different set of partitions that support a critical business application for external clients. To provide separate communication channels, you can define one HiperSockets adapter for the first set of partitions to use, and a different HiperSockets adapter for the other set. A DPM-enabled system supports up to 32 HiperSockets adapters.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

To create a HiperSockets adapter, provide values for the following fields on the **Create HiperSockets Adapter** window. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Enter a unique name for the new adapter, which can be 1 - 64 characters in length, and consist of alphanumeric characters, blanks, periods, underscores, dashes, or at symbols (@). The name cannot contain leading or trailing blanks.

Description
Optionally, provide a description for this new HiperSockets adapter. The description can be up to 1024 characters in length.

MTU/Frame size (KB)
Consider changing this setting, based on your knowledge of the workloads that require the use of this HiperSockets adapter.

By default, this field is set to the smallest size: an MTU of 8 and frame size of 16 kilobytes (KB), which is displayed as 8/16. Select a value based on your knowledge of the bandwidth requirements for partition-to-partition communication. In most workload environments, the default value provides the most efficient use of system resources; however, for workloads that require increased bandwidth, for tasks such as large-file transfers and file backup, select a higher value to improve performance.

Additional functions on this window include:

OK
After you have supplied all of the required values, click **OK** to create the adapter definition and close the **Create HiperSockets Adapter** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Reassign Channel Path IDs

Use the **Reassign Channel Path IDs** task to change the channel path IDs that are assigned to Dynamic Partition Manager (DPM) adapters.

The name of the target CPC is displayed at the top of the **Reassign Channel Path IDs** task main window.

The main window provides a table that lists all of the adapters of the target CPC that have channel path IDs (CHPIDs). Each adapter appears in its own row in the table and the information is arranged into columns. Use the **New Channel Path ID** column to reassign channel path IDs. After making changes, click **OK** to apply the changes.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

The **Reassign Channel Path IDs** table contains the following columns.

Name
Name of the adapter. This value is a link that opens the **Adapter Details** task.

Current Channel Path ID
Channel path ID that is currently assigned to the adapter.

New Channel Path ID
Drop down menu that allows you to select a new channel path ID. By default, this field is empty, which indicates that the channel path ID (CHPID) should not be modified. To choose a new CHPID, select a value from the drop down menu.

Note the following:

- If an adapter is assigned to a partition, its channel path ID cannot be modified.
- A channel path ID value can only be used by one adapter. If you select a value from the drop down menu, it cannot be specified as the new CHPID for another adapter, and it cannot be the current CHPID of an adapter whose value is not changing.

ID
ID of the adapter.

Type
Adapter type.

Card Type
Card type of the adapter.

Location
Location of the adapter.

Description
Description of the device.

The following icons are also displayed on the **Reassign Channel Path IDs** table:

Export all to CSV
Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Selects the columns that you want to display. All available columns are in the list by their column name. Select the columns that you want displayed or hidden by selecting or clearing the items in the list. When you complete the configuration, click **OK**. The columns are displayed in the table as you specified.

Additional functions on this window include:

OK
To close the window, click **OK**.If you made changes in editable fields in the window, those changes are applied. If any **Channel Path ID** value on this page is invalid, this option is disabled.

Cancel

- To close the window without saving any changes, click **Cancel**.
- If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Export WWPNs

Use the **Export WWPNs** task to export the worldwide port names (WWPNs) of the host bus adapters for one or more partitions.

WWPNs are automatically assigned to host bus adapters by the system and are unique identifiers in the network. WWPNs cannot be modified.

The name of the target CPC is displayed at the top of the **Export WWPNs** task main window.

To export WWPNs, do the following:

1. Choose a destination (FTP server or removable media).
2. Specify the name of the file that contains the WWPNs and the destination directory.
3. Click **Export**.

To export WWPNs from the console **remotely**, do the following:

1. Choose one of the following options from the **Opening wwpns.csv** window:
   a. Open the file with a program from the drop-down list.
   b. Save the file. The file is saved to your browser downloads.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

Choose a destination:

On the **Export WWPNs** page, choose the destination by clicking the radio button for either **FTP server** or **Removable media**.

If you specify that you want to export the WWPNs to an **FTP server**, enter values for the following fields.

Host name
Enter either the fully qualified domain name of the FTP server, or its IP address.

User name
Enter the user name on the target FTP server.

Password
Enter the password associated with the user name on the target FTP server.

Protocol
To transfer data to the FTP server, choose one of the following protocols.

FTP
Select this option if you want to use the standard File Transfer Protocol (FTP).

FTPS
Select this option if you want to use the FTP Secure (FTPS) protocol, which uses the Secure Socket Layer (SSL) protocol to secure data.

SFTP
Select this option if you want to use the Secure File Transfer Protocol (SFTP), which uses the Secure Shell (SSH) protocol to secure data.

If you specify that you want to export the WWPNs to **Removable media**, enter values for the following fields.

Device
Device to which the WWPN file should be exported. Use the drop down menu to select a device.

The drop down menu displays a list of all media that was detected when the **Export WWPNs** task was opened. Click the refresh icon to refresh the list of devices.

Specify the destination file name and directory:

After selecting a destination, specify the file name and the directory using the following fields:

Destination file name
Name of the WWPN file to be exported. By default, the name of the WWPN file is **wwpns.csv**. If you want to use another name, type over the default name in this field.

Destination directory
Directory where the exported WWPN file will be stored. This field is optional. Enter the directory name in this field. If you select the **FTP server** destination option and leave this field blank, the file is saved in the FTP home directory. If you select the **Removable media** destination option and leave this field blank, the file is saved in the root directory.

Export the WWPN file:

After specifying a destination, destination file name, and destination directory, click **Export** to export the file. A progress dialog is displayed as the file is saved. However, if the destination directory does not exist, or if the destination file already exists, a confirmation page is displayed, as follows:

- If the destination directory does not currently exist, you can continue by clicking **Create** on the **Confirm** dialog (or **Cancel** if you do not want to create the new directory).
- If the destination file currently exists, you can continue by clicking **Overwrite** on the **Confirm** dialog to overwrite the existing directory (or **Cancel** if you do not want to overwrite the existing file).

Additional functions on this window include:

Export
Writes the file to the specified destination. This option is disabled if any required field is not specified, or if any specified field is invalid.

Cancel

- To close the window without saving any changes, click **Cancel**.
- If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Manage Console Recovery

Accessing the Manage Console Recovery task

This task allows the Hardware Management Console (HMC) to load a selected target system with a selected recovery code load image remotely over the network. It also requires actions on this HMC and the selected target system.

The following requirements must be considered before loading images to a target recovery console.

- All Hardware Management Console customer LAN interfaces on this HMC must be configured as static. (Do not use DHCP to obtain addresses.)
- The targeted console system must be reachable on a local (same) subnet by using one of the HMC's customer LAN interfaces.
- The subnet to the target console system must not have a DHCP server on it.
- Multiple HMC servers running this task are allowed on the same subnet serving different targets, but is not recommended.

To perform a remote console recovery with a selected recovery code load image:

1. Open the **Manage Console Recovery** task. The Manage Console Recovery window is displayed.
2. Select a recovery image from the Recovery Images section of the window. If the image you want is not listed in the table, click **Import Image**. The Import Image window is displayed.
3. You can either download the image from an FTP server or the Remote Support Facility (RSF) if configured and allowed.
4. Once the image is imported, it is displayed in the Recovery Images table.
5. Select the image from the table that you want as the recovery code image.
6. From the Recovery Consoles section of the window, click **Select**, which appears next to **Target Recovery Console**. The Target Recovery Console Selection window is displayed.
7. Select a console from the discovered target console that you want the code load image downloaded to, then click **OK**. If the console that you want is not displayed, you can alternatively choose to manually enter a customer LAN MAC address or addresses of a target recovery console by selecting **Enter the MAC Address of the target console**, then click **OK**.
8. The selected target recovery console name and type, with MAC address or addresses, is displayed as the Recovery Console. If MAC addresses were manually entered, the name and type are not displayed. Click **Start Server**, the Starting Server message is displayed, then the Console Recovery Monitor window is displayed.
9. On the Console Recovery Monitor window, **Status** is **Running** and identifies which physical interfaces the server is allowing for connection to the targeted recovery console. Monitor the progress and perform the indicated actions that are specified in the window. There are actions that are required which need to be performed at the target recovery console and this HMC.

   Attention: Downloading the image can take some time. Do **not** power off or restart this HMC or the target recovery console system during this process.

   Note: When you are initially directed to go to the target recovery console, depending on the machine type and model of the targeted recovery console, use the appropriate BIOS procedures.
10. To close the task, click **Cancel**.

For more detailed instructions, see the "Loading images to a system from a network (electronic code load)" section of the *8561 Service Guide*, GC28-6998.

Manage Console Recovery

Use this task to allow the Hardware Management Console (HMC) to load a selected target console system with a selected recovery code load image remotely over the network. Begin by selecting a recovery code load image that you want for the remote console boot from the "Recovery Images" on page 946 section. Then, select the target recovery console from the "Target Recovery Console Selection" on page 948 window.

The following requirements must be considered before loading images to a target recovery console.

- All Hardware Management Console customer LAN interfaces on this HMC must be configured as static. (Do not use DHCP to obtain addresses.)
- The targeted console system must be reachable on a local subnet by using one of the HMCs customer LAN interfaces.
- The subnet to the target console system must not have a DHCP server on it.
- Multiple HMC servers are allowed on the same subnet serving different targets, but is not recommended.

Recovery Images

This section includes a table that displays the current recovery code load images on this console. You can select the image that is used to eventually load a remote system over the network.

The following information is displayed in the table. For a description of the table toolbar icons and how to use them, see "Using the Table Toolbar" on page 950.

Name
Specifies the name of the code load image on this console. The name is expected to end with `.iso`.

Type
Specifies the type of system that the code load image should be used for. The values can be **HMC**, **SE**, or **TKE**.

Version
Specifies the driver version of the code load image that will load on the targeted system.

Control Level
Specifies the control level of the code load image that will load on the targeted system.

Description
Specifies a summary description of the code load image.

Import Image
To import an image from either Remote Support Facility (RSF) or a server (FTP, FTPS, or SFTP), click **Import Image**.

Note: This is required if the code load image that you want is not listed already.

Delete Image
To remove an image from this console, click **Delete Image**.

Note: Since there is limited space on the HMC's hard disk drive for storing code load images, use this option to free up space.

Recovery Consoles

This section of the task window allows you to select the target recovery console system from the "Target Recovery Console Selection" on page 948 window that this Hardware Management Console downloads the selected code load image to, over the network. When a target recovery console (or manually entered MAC addresses) has been selected, the information for that console is displayed.

Target Recovery Console
To select a target recovery console, click **Select**. When a recovery image has been selected, it is identified here.

Start Server
When the target recovery console and recovery image have been selected and identified, click **Start Server**. The “Console Recovery Monitor” on page 949 window is displayed. While this is running, you need to go to the specified target recovery console and perform a network boot in the target's BIOS or equivalent window on the appropriate interface.

Cancel
To close the window and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Import Image

Use this window to import images from either an FTP server or the Remote Support Facility (RSF).

Import from FTP server
To import an image from an FTP server, select **Import from FTP server**. The “Import Image from FTP” on page 947 window is displayed.

Change FTP Settings
To change the FTP settings of a selected image, click **Change FTP Settings**. You can update any of the fields, then click **Connect**.

Import from Remote Support Facility (RSF)
To import an image from RSF for downloading to this console, select **Import from Remote Support Facility (RSF)**. When this selection is made, the console is collecting support system information. Provide a **Driver**, **Type**, and **Control Level**.

Note: Use the **Customize Outbound Connectivity** task to ensure that your Hardware Management Console is enabled for RSF.

Import
To proceed with your selection, click **Import**.

Cancel
To close the window without making a selection and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Import Image from FTP

Use this window to configure FTP settings when you use an external server to download images from.

Host name
Specify the host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.

- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Connect
To connect to the specified server and display a list of acceptable images to download to the console, click **Connect**. If the FTP server information is incorrect, then a message is displayed that the connection cannot be made to the specified FTP server. If it is determined that an SSH key is needed to connect to a specified server, then a hyperlink to the **Manager SSH Keys** task is provided.

Clear
To remove the information from the input areas, click **Clear**.

Cancel
To close the window without proceeding with the selection and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Target Recovery Console Selection

Use this window to select a target recovery console that this Hardware Management Console previously discovered. These target recovery consoles are (or were within the last 7 days) reachable from the local (same) customer LAN subnet of this HMC. Alternatively, you can manually enter a recovery console's MAC address or addresses.

Select a discovered target console
To choose to select a target console from the table, select **Select a discovered target console** and select the recovery console from the table. After you click **OK** for this selection, the information for the target recovery console is displayed in the Recovery Consoles section of the window. If you need to select a different target recovery console from the table, click **Select** from the Recovery Consoles section.

The following information is displayed in the table. For a description of the table toolbar icons and how to use them, see “Using the Table Toolbar” on page 950.

The table consists of the following information:

Name
Identifies the name of the discovered console.

Type
Specifies the type of discovered console. (The values can be **HMC**, **Primary SE**, **Alternate SE**, or **TKE**.)

MAC Address
Displays the media access control (MAC) address or addresses of the discovered console. Generally, two MAC addresses are available, which are from the customer LAN interfaces of the discovered console.

Enter the MAC address of the target console
If the target console that you want is not available from the **Select a discovered target console** table, select **Enter the MAC address of the target console** to manually enter the customer LAN MAC address or addresses. Only one **MAC address** is required in the MAC address input area. The MAC address must be for a customer LAN interface of the targeted recovery console that has connectivity to this Hardware Management Console over a local (same) subnet.

Even though only one MAC entry is required, you are allowed to enter the two MAC addresses associated with both customer LAN interfaces. This ensures that you do not have to restart the server to enter the other customer LAN MAC address if you entered only one MAC address and it was not for the interface with connectivity to this HMC over the local (same) subnet.

The MAC address is made up of six two-digit hexadecimal numbers, which are separated by colons (:) or hyphens (-).

A MAC address for an interface can be identified and located in the target console's BIOS window (or equivalent Virtual Support Element) as follows:

- For a target system without a DVD drive (BIOS - Insyde):
  - If the target console is an HMC or TKE, use LAN 1 (or LAN 2 or both) interface from the Boot Manager window.
  - If target console is an SE, use LAN 3 (or LAN 4 or both) interface from the Boot Manager window..
  - If the target console is a Hardware Management Appliance, use LAN 5 (or LAN 6 or both) interface from the Boot Manager Window.
- For a target system with a DVD drive (BIOS - American Megatrends):
  - The target console can only be an HMC or TKE. Specify the first (or second or both) interface from the line that includes **I350** from the **Advanced** tab.
- For an SE in a Hardware Management Appliance, use the **Virtual Support Element Management** task on the Hardware Management Console and specify LAN interface 1 (or LAN interface 2 or both), which is listed in the **Install SE** section of the task window.

For more information about the requirements, see "Accessing the Manage Console Recovery task" on page 945.

OK
To proceed with your selection, click **OK**.

Cancel
To close the window without making a selection and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Console Recovery Monitor

This window is used to monitor the progress of the targeted recovery console.

Status
Displays the status of the boot server.

Running (*xxx*)
Identifies which physical interfaces (*xxx*) the server is allowing for connections with the targeted recovery console.

Recovery Image
Specifies the name of the recovery image.

Target Recovery Console
Identifies the targeted recovery console by:

Name
Specifies the name of the targeted recovery console if you selected a discovered target console.

Note: The name does not appear if you manually entered a MAC address or addresses.

Type
Specifies the type of the targeted recovery console. (The values can be **HMC**, **Primary SE**, **Alternate SE**, or **TKE**.)

Note: The type does not appear if you manually entered a MAC address or addresses.

MAC
Displays the media access control (MAC) address or addresses of the targeted recovery console. Generally, two MAC addresses are available.

Connected Client
Displays the state of the connection to the targeted recovery console. During the upload, the target recovery console toggles between connection and disconnection status.

Step Elapsed Time
Identifies the amount of time you have been in a certain **Progress** step.

Boot Server Uptime
Identifies the amount of time the server has been running.

Progress
Describes the progress of the server, which is generally identified by steps.

Action
Describes any action that you need to take on the target recovery console while the file is being uploaded.

Cancel (or Close)
While the status of the server is **Running** and loading an image on the target recovery console, you can stop the server and exit the Console Recovery Monitor window by clicking **Cancel**. A message is displayed before you completely stop the boot server. To confirm that you want to stop the boot server and end console recovery, click **OK**.

When the image load is complete, the boot server is automatically stopped and **Close** (replaces **Cancel**) is displayed on the Console Recovery Monitor window. To close the Console Recovery Monitor window, click **Close**. No further confirmation is required.

Help
To display help for the current window, click **Help**.

Using the Table Toolbar

The toolbar at the top of the table contains icons to select, filter, and sort the table. If you place your cursor over an icon, the icon description is displayed.

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this downloaded CSV file into most spreadsheet applications.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the **^** in the column header to change from ascending to descending order.

Clear All Sorts
Returns to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns that you want displayed or hidden by checking or unchecking the list box and by using the arrow buttons to the right of the list to change the order of the selected column.

Select Action
Contains a list of the actions that you can perform on this table.

Filter

Use the quick filter function to enter a filter string in the Filter input field, and then press Enter to apply the filter. By default all the columns are filtered, showing only rows containing a cell whose value includes the filter text. Clicking the arrow displays a menu that restricts the columns to which the filter is applied.

Manage Coupling Facility Port Enablement

Accessing the Manage Coupling Facility Port Enablement task

This task is used to enable or disable a selected coupling facility port.

Note: Depending on your user task role, you may only be able to view this task.

1. Select a CPC.
2. Open the **Manage Coupling Facility Port Enablement** task. The Manage Coupling Facility Port Enablement window is displayed.
3. Select a port to enable or disable. When you select a port it is identified as an enabled or disabled port. Click **Enable** or click **Disable** depending on the enablement you want for that port.
4. When you have finished with this task, click **Close** to exit the task.

Management Coupling Facility Port Enablement

This task allows you to enable or disable a selected coupling facility port from the list of coupling VCHIDs that are displayed. You can make a selection but note that the state must be Online and the enablement or disablement to this channel also affects other channels that have the same adapter ID and port number.

Note: Depending on your user task role, you may only be able to view this task.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions in the table:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Enable
To enable the selected coupling facility port that is currently disabled, click **Enable**.

Disable
To disable the selected coupling facility port that is currently enabled, click **Disable**.

Close
To close this window and exit the task, click **Close**.

Help
To display help for the current window, click **Help**.

Manage Flash Allocation

Accessing the Manage Flash Allocation task

This task displays the current Flash allocation summary on the CPC. You can use the window to create and change Flash allocation increments for selected logical partitions.

1. Select an object.

   Note: This is only available when you are targeting IBM z13, IBM z13s, or prior objects.
2. Open the **Manage Flash Allocation** task. The Manage Flash Allocation window is displayed.
3. Use the Partitions table to add or remove the current and maximum Flash allocations for the selected logical partition.
4. Use the **Selection Action** list from the table tool bar to perform the following actions:

   Add allocation
   Adds new Flash allocations to a logical partition.

   Remove allocation
   Removes current Flash allocations from the selected logical partition.

   View Partition to PCHID Map
   Displays the logical partition to PCHID assignments when determining Flash Express allocations.

   Configure Columns
   Selects which columns you want to display. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. Your configuration changes are saved and reloaded the next time that you launch this task.

Manage Flash Allocation

Use this window to display the current Flash allocation summary available on the CPC. Use the Partitions table to create and change Flash allocation increments for selected logical partitions.

Note: This is only available when you are targeting IBM z13, IBM z13s, or prior objects.

Allocated
Displays the amount of Flash allocation currently assigned to the CPC.

Available
Displays the amount of Flash allocation currently available on the CPC.

Uninitialized
Displays the amount of Flash allocation currently uninitialized on the CPC.

Unavailable
Displays the amount of Flash allocation currently unavailable on the CPC.

Total
Displays the current total amount of all the Flash allocations on the CPC.

Storage increment
Displays the current maximum Flash storage increment on the CPC.

Rebuild complete
Displays the completion percentage of the new Flash allocations rebuild.

Additional functions are available from this window:

Partitions Table

Use the Partitions table to change or remove the current and maximum Flash allocations for the selected logical partition.

Partition Name
Displays the name of the logical partitions assigned to the CPC with Flash allocations.

Status
Displays the status of the logical partitions. The status can be: **Active** or **Inactive**.

IOCDS
Displays the logical partition names with Flash allocations.

Allocated (GB)
Displays the current amount of Flash storage allocated for the logical partitions. Select the logical partition to change the initial Flash allocation increment.

Maximum (GB)
Displays the maximum amount of Flash storage allocated for the logical partitions. Select the logical partition to change the maximum Flash allocation increment.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions in the Partitions table:

Add allocation
Adds new Flash allocations to a logical partition.

Remove allocation
Removes current Flash allocation from the selected logical partition.

View Partition to PCHID Map
Displays the logical partition to PCHID assignments.

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

Refresh
To update the displayed Flash allocations with the current allocations, click **Refresh**.

OK
To perform the selected operation, click **OK**.

Apply
To save and display the new Flash allocations as the current allocations, click **Apply**.

Cancel
To exit the current window, click **Cancel**.

Help
To display help for the current window, click **Help**.

New Flash Allocation

Use this window to enter new Flash allocations for the selected new or existing logical partition.

Partition
Specify the logical partition name to which Flash should be allocated.

New
Enter the name of the logical partition manually. This can be either an existing logical partition name or a logical partition which is not currently defined in any IOCDS.

Use existing
Use the down arrow to select a logical partition name defined in any IOCDS for the allocation.

Allocation
Enter the allocation values for the specified partition name. The allocations are:

Initial (GB)
Enter the initial Flash allocation to be used for the logical partition.

Maximum (GB)
Enter the maximum Flash allocation to be used for the logical partition.

Storage increment (GB)
Displays the Flash increment value.

Available (GB)
Displays the amount of Flash memory currently available.

Cancel
To exit the current window, click **Cancel**.

OK
To perform the selected operation, click **OK**.

Help
To display help for the current window, click **Help**.

View Partition to PCHID Map

Use this window to view the logical partition to PCHID assignments.

View Partition to PCHID Map

The View Partition to PCHID Map table displays the logical partition names which currently have Flash allocations and the Flash PCHIDs associated with those logical partitions. You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Partition Name
Displays the name of the logical partition assigned to the Flash adapter PCHIDs.

Status
Displays the status of the logical partition. The status can be: **Active** or **Inactive**.

Adapter A PCHID
Displays the first adapter PCHID number that is associated with the logical partition.

Adapter B PCHID
Displays the second adapter PCHID number that is associated with the logical partition.

The icons perform the following functions in the Partitions table:

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Close
To exit the current window, click **Close**

Help
To display help for the current window, click **Help**.

Manage Key Manager Connections

Accessing the Manage Key Manager Connections task

The **Manage Key Manager Connections** task guides you through the process of establishing connections between one or more endpoint-security-enabled systems (CPCs) and key managers, in order to secure the connections between the systems and Fibre Channel storage devices.

With **Manage Key Manager Connections**, you can do the following.

- Understand the topology of the installation
- Determine the status of systems and related key managers, as well as the connections between them
- Connect systems to key managers
- Configure system policies
- Create certificate signing requests
- Create self-signed certificates
- Edit certificates
- Export certificates to key managers
- Import key manager certificates
- Import signed certificates
- Remove key manager connections
- View adapter security information

You can access the **Manage Key Manager Connections** task from the main Hardware Management Console (HMC) page by selecting the Systems Management node, by selecting a specific system, or by selecting the task in the **Tasks Index**. Use the ACSADMIN user ID for full access to the **Manage Key Manager Connections** task.

Manage Key Manager Connections

Use the **Manage Key Manager Connections** task to establish connections between one or more endpoint-security-enabled systems (CPCs) and key managers.

The main window of the **Manage Key Manager Connections** task includes the following elements.

- A graphical **Topology view**, to help you understand the available endpoint-security-enabled systems, the configured key managers, and the connections between them.
- The **system toolbar**, which provides tools for viewing and obtaining status about the various elements in the **Topology view**.
- The **Actions** area, for choosing actions to perform against the specified systems and related key managers.

For more information about the elements of the **Manage Key Manager Connections** main window, use the following links.

- “Topology view” on page 955
- “Topology toolbar” on page 958
- “Actions” on page 960

Topology view

Use the **Topology view** of the **Manage Key Manager Connections** window to understand the relationship of the systems (CPCs) in your configuration that are enabled for endpoint security, the related key managers, and the connections between them.

In the **Topology view**, the systems in your installation are displayed vertically within the **Systems** area. Key managers that are connected to systems are displayed in the **Key managers** area. In the topology display, the lines that extend from systems to key managers show the connections between them.

When you first start the **Manage Key Manager Connections** task, if there are no connections between systems and key managers, **Configure Systems for Endpoint Authentication** is displayed in the main window. Click **CONNECT SYSTEMS TO KEY MANAGERS** to begin the process.

For more information about the elements of the **Topology view**, use the following links.

- "Get information about systems" on page 956
- "Get information about key managers" on page 957
- "Get information about the connections between systems and key managers" on page 957
- "Get help for using Manage Key Manager Connections" on page 958

Get information about systems

In the **Topology view**, each system (CPC) is represented by its own rectangle. Multiple systems are displayed vertically in the topology within the **Systems** area, and the related key managers are displayed within the **Key managers** area. The lines that extend from the systems (CPCs) to the key managers represent the connections between them.

The health of each system is immediately apparent in the **Topology view**. Systems that are outlined in red contain one or more errors, and systems that are outlined in yellow contain one or more warnings. For more information about getting the overall status of the configuration, see "Get configuration status" on page 959.

To get more details about a system, click the system's rectangle in the main window. The **System details** window opens, which provides information about the following.

System
Displays the name of the system.

Connection status
Current connection status of the system (OK, Warning, or Error). When the system has errors or warnings, click the **This system has** *number* **errors** link, at the top of the **System details** window to get more information. The **Errors** window opens and displays information about the system's warnings and errors. For more information about the **Errors** window, see "Getting information about all warnings or errors in the topology" on page 959.

View adapter security
Launches the **View adapter security** window, which displays information about the FICON Express adapters that are defined for the system and their security capabilities.

The table includes the following information for each adapter.

ID
PCHID that is assigned to the FICON Express adapter

Card type
Type of FICON Express adapter

Status
Status of the FICON Express adapter

Security capabilities
One of the following security capabilities:

Basic
The hardware is not capable of making authenticated or encrypted connections.

Authentication
The hardware is capable of having authenticated connections.

Encryption
The hardware is capable of having both authenticated and encrypted connections.

View certificate details (link)
Launches the **View certificate details** window, which contains basic information about the system's endpoint security certificate. The information in this window is different, depending on whether it is a self-signed or certificate authority (CA)-signed certificate.

To see more extensive information about the certificate, click the drop-down icon beside **See additional certificate details**. The full list of attributes for the certificate are displayed below the **See additional certificate details** option. Use the scroll bar on the right side of the window to view the entire list.

For CA-signed certificates, The tree hierarchy of the certificate chain is displayed at the top of the **View certificate details** window, immediately below the window title. At the top of the tree is the root certificate authority. The next tier down contains between 1 and 3 intermediate certificate authorities, and at the bottom of the tree is the certificate that was signed by the intermediate certificate authorities. Use the scroll bar to see the full list of certificate details.

When you are finished reviewing the certificate's information, click **CLOSE** on the **View certificate details** window to return the **Topology view**.

Connect system to key managers (link)
This link is displayed only if the system is not yet configured to a key manager. Use this link to launch the **Connect system to key managers** action and configure this system to a key manager. This system is automatically selected in the **Choose Systems** window of the **Connect system to key managers** action.

Get information about key managers

In the **Topology view**, each key manager is represented by its own rectangle. Multiple systems (CPCs) are displayed vertically in the topology within the **Systems** area, and the related key managers are displayed within the **Key managers** area. The lines that extend from the systems to the key managers represent the connections between them.

The health of each key manager is immediately apparent in the Topology view. Key managers that are outlined in red contain one or more errors, and key managers that are outlined in yellow contain one or more warnings. For more information about getting overall status of the configuration, see “Get configuration status” on page 959.

To get more details about a key manager, click the key manager's rectangle in the main window. The **Key manager details** window opens, which provides information about the following.

Key manager
Name of the key manager.

Key manager hostname
Hostname of the key manager.

Key manager port
Key manager port number. The default value is 5696.

Authentication status
Current connection status of the key manager (OK, Warning, or Error).

When the key manager has errors or warnings, click the **This key manager has** *number* **errors** link, at the top of the **Key manager details** window to get more information. The **Errors** window opens and displays information about the key manager's warnings and errors. For more information about the **Errors** window, see “Getting information about all warnings or errors in the topology” on page 959.

To close the **Key manager details** window, click **x**.

Get information about the connections between systems and key managers

In the **Topology view**, the lines that extend from the systems (CPCs) to the key managers represent the connections (links) between them.

Hover over a link to highlight that link and the systems and key managers to which it is connected. To see details about a connection, click the line or the icon that is displayed over the highlighted link (lowercase I in a blue circle or exclamation point in a red circle).

The **Connection details** window opens and provides the following information for each connection.

System
Name of the system to which the key manager is connected.

Key manager
Name of the key manager to which the system is connected.

Connection status
Current status of the connection between the system and the key manager (OK, Warning, or Error).

HMC connection status
The status of the HMCs that are associated with the connection between a system and key manager. The status of each HMC is indicated by a status icon (green or red circle) after its name. A green circle indicates that the system can communicate with the key manager through the HMC. A red circle indicates that the system cannot communicate with the key manager through the HMC.

When the connection has errors or warnings, click the **This connection has** *number* **errors** link, at the top of the **Connection details** window to get more information. The **Errors** window opens and displays information about the connection's warnings and errors. For more information about the **Errors** window, see “Getting information about all warnings or errors in the topology” on page 959.

To close the **Connection details** window, click **x**.

Get help for using Manage Key Manager Connections

To access help for using the functions and features of the **Manage Key Manager Connections** task, click **Help**.

Topology toolbar

Use the **Topology toolbar** to adjust the display of the topology and get the status of the systems (CPCs), key managers, and connections in the installation.

For more information about the **Topology toolbar**, use the following links.

- “Adjust the topology view” on page 958
- “Get details about the configuration” on page 958
- “Get configuration status” on page 959

Adjust the topology view

The **Topology toolbar** includes the following elements for adjusting the display of the topology. Use these controls to optimize your view.

Zoom In
Enlarges images in the topology view.

Zoom Out
Shrinks images in the topology view.

Fit to Width
Fits the content of the topology within the Connected Systems and Connected key managers frames.

Zoom by Percentage
Enlarges or shrinks the content of the topology frame based on a number that you select. Use the drop-down list to change the topology size in increments of 25 percent (the default is 100 percent).

The changes that you make to the topology view do not persist from session to session.

Get details about the configuration

The **Topology toolbar** displays the following details about the configuration.

Time
Displays the time of the configuration. The time is updated on every refresh.

Date
Displays the date of the configuration.

Time zone
Displays the time zone of the configuration.

Status
Displays the overall health of the configuration. For more information, see “Get configuration status” on page 959.

Get configuration status

Use the **Status** icon on the topology toolbar to determine the overall health of the configuration.

Status icon is green

If the topology contains no errors, a green circle and check mark icon are displayed in the **Status** field. Click this icon to display an information window that explains the status. To close the information window, click the green **Status** icon again.

Status icon is yellow (warning)

If the topology contains a system (CPC) or key manager that has one or more warnings, the following changes occur in the topology view.

- The **Status** icon on the topology toolbar changes to a yellow exclamation mark inside a yellow circle. The **Status** icon also displays a number, which indicates the number of warnings. Click the **Status** icon to see more details about the warnings. For more information, see “Getting information about all warnings or errors in the topology” on page 959.
- The outline of the system or key manager's rectangle in the topology view changes to yellow, and displays a yellow exclamation mark.

Status icon is red (error)

If the topology contains a system (CPC) or key manager that has one or more errors, the following changes occur in the topology view.

- The **Status** icon on the topology toolbar changes to a red exclamation mark inside a red circle. The **Status** icon also displays a number, which indicates the number of errors. Click the **Status** icon to see more details about the errors. For more information, see “Getting information about all warnings or errors in the topology” on page 959.
- The outline of the system or key manager's rectangle in the topology view changes to red, and displays a red exclamation mark.

Getting information about all warnings or errors in the topology

To get information about all of the warnings or errors in the topology, click the **Status** icon on the topology toolbar, which opens the **Errors** window. The **Errors** window displays information about each of the warnings or errors in the topology, in drop-down list style. If the topology has both warnings and errors, the **Errors** window contains the errors first, followed by the warnings.

The **Errors** window provides the following information for each error.

- Name of the system or manager that is the source of the error
- Error message
- Error description
- Error message number (displayed for errors only)

To close the **Errors** window, click the **Status** icon again.

Actions

The **Actions** area of the **Manage Key Manager Connections** main window includes a number of actions that you can perform against systems (CPCs) and key managers. Hover over an action to see a short description.

Note: Depending on user permissions, one or more actions might not be available to certain users. In this situation, the actions that are unavailable are not displayed under **Actions**.

For more information about the **Actions**, use the following links.

- “Connect system to key managers” on page 960
- “Edit certificates” on page 971
- “Export certificates to key managers” on page 975
- “Create self-signed certificate” on page 970 (available only when certificate authority (CA)-signed certificates exist)
- “Import key manager certificate” on page 978
- “Import signed certificate” on page 980
- “Configure system policies” on page 967
- “Remove key manager connections” on page 982
- “Create certificate signing request” on page 968
- “View adapter security” on page 983

Connect system to key managers

The **Connect system to key managers** action guides you through the process of connecting one or more systems (CPCs) to one or more key managers.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

To start the **Connect system to key managers** action, go to “Step 1: Choose Systems” on page 960.

Step 1: Choose Systems

Use the **Choose Systems** window to select one or more systems (CPCs) to connect to key managers. The Connect Systems table shows the systems that support Fibre Channel endpoint security and the key managers to which they are connected.

Note that if you select multiple systems, each system must have the same key managers defined as all the other systems. Selections that do not meet this rule are highlighted in red in the table and an error status icon is displayed beside them.

1. In the table, select the systems that you want to connect to one or more key managers. The table includes the following information for each system.

   Name
   System name.

   Configured Key Managers
   Name of key managers that are currently defined to the system that is displayed in this table row.
2. If there are no errors after selecting one or more systems, click **NEXT** to go to the next step.

Step 2: Choose Key Managers

Use the table in the **Choose Key Managers** window to select the authentication key managers that you would like to connect to the systems (CPCs) that you chose in “Step 1: Choose Systems” on page 960.

In this step, you define the key managers from which the systems will fetch the shared secret keys that used to secure the endpoints of their Fibre Channel connections.

Note: After making changes, if you click **x** to close the **Choose Key Managers** window, a message window is displayed to warn you that all new key manager definitions will be retained, but systems might not be able to communicate with the key managers. This is because the system certificates have not yet been exported to the key managers, and the key manager certificates have not been imported into the systems. Do one of the following.

- Click **PROCEED ANYWAY** to close the **Choose Key Managers** window.
- Click **CANCEL** to reopen to the **Choose Key Managers** window.

The Choose Key Managers table provides the following information for key managers that are currently defined. If no key managers are defined, the table is empty.

Name
Name of the key manager.

Description
Description of the key manager.

Hostname or IP Address
Fully-qualified domain name (FQDN), or IP address of the key manager.

Port
Key manager port number. The default value is 5696.

Note: You can select a maximum of four key managers.

The **Current Selections** area, in the lower right corner of the window, displays the systems that have already been selected.

The process that you use to select key managers depends on whether there are any key managers that are already defined for your installation. Select the following option that matches your situation.

- “Choosing key managers when no defined key managers are available” on page 961 (the Choose Key Managers table is empty)
- “Choosing key managers when previously-defined key managers are available” on page 962

Choosing key managers when no defined key managers are available

The table in the **Choose Key Managers** window provides a list of the authentication key managers that are currently connected to systems in your installation. In this situation, there are no key managers defined, so the initial table is empty. Use the following steps to define and add a key manager.

Note: A minimum of two key managers are recommended for high availability.

1. Go to “Add Key Manager” on page 963 and follow the instructions provided there for adding a key manager. When you are finished, return here and proceed to step 2.
2. After adding a key manager, review its entry in the Choose Key Managers table. If you want to add another key manager, return to step 1.

   Note: If only one key manager is defined, a message is displayed to warn you that *A minimum of two key managers are recommended for high availability*.
3. When you have finished defining key managers, you can optionally test the connections between the key managers and the selected systems. To do this, click **TEST CONNECTIVITY**. The number of selected systems is displayed in parentheses with the **TEST CONNECTIVITY** option.

   After clicking **TEST CONNECTIVITY**, the **Testing connectivity** message is displayed to indicate the progress of the test. When the test is complete, the **Test Connectivity** window is displayed. The **Test Connectivity** window provides the following information.

   - A hierarchical list of the key manager-to-system connections, as well as the system-to-HMC connections. (Systems can communicate with key managers through the HMC).

- Connection status for each system-to-key manager connection (OK, Warning, and Error). Click **Error** or **Warning** to see a description of the issue.
- Connection status for each system-to-HMC connection. The status values are as follows.

  OK
  The system can communicate with the key manager through the HMC.

  Error
  The system cannot communicate with the key manager through the HMC.

  After the connectivity test is complete, and the status of all selected key managers is **OK**, click **CLOSE** on the **Test Connectivity** window to return to the **Choose Key Managers** window.

4. On the **Choose Key Managers** window, click **NEXT** to go to the next step.

Choosing key managers when previously-defined key managers are available

The table in the **Choose Key Managers** window provides a list of the key managers that are currently connected to other systems in your installation. In this situation, there are one or more key managers that are already defined.

Note: A minimum of two key managers are recommended for high availability.

If you want to add a key manager, in addition to the key managers that are already defined, click **ADD KEY MANAGER**. Refer to "Add Key Manager" on page 963 for instructions. After adding the key manager, return here and proceed to Step 1, in this help topic.

To choose key managers, do the following.

1. Select one or more key managers that you want to connect to the systems that you chose in "Step 1: Choose Systems" on page 960.

   You can use the **Same key manager definition as** option, immediately above the Choose Key Managers table, to choose the same key managers as another system. Do the following.

   a. Open the **Same key manager definition as** drop-down menu to choose a system. For example, if the currently selected system is **CPC2**, and you want CPC2 to use the same key managers as **CPC1**, you could use the **Same key manager definition as** drop-down menu to choose **CPC1**.

   b. After choosing a system, you can verify the key managers that are associated with that system by clicking on **Show** *system_name* **details**.

   c. Select the **Same key manager definition as** selection box to apply the definition of the system that is selected in the drop-down menu to the systems that are listed in the **CURRENT SELECTIONS** area (which were selected in "Step 1: Choose Systems" on page 960.

   CAUTION: If a key manager in the **Choose Key Managers** table is selected, and is defined only for the selected systems, deselecting it (unchecking its selection box) results in the removal of that key manager definition.

2. Optionally, click **TEST CONNECTIVITY** to test the connections between the selected key managers and the chosen systems. The number of selected key managers is displayed in parentheses with the **TEST CONNECTIVITY** option.

   After clicking **TEST CONNECTIVITY**, the **Testing connectivity** message is displayed to indicate the progress of the test. When the test is complete, the **Test Connectivity** window is displayed. The **Test Connectivity** window provides the following information.

   - A hierarchical list of the key manager-to-system connections, as well as the system-to-HMC connections. (Systems can communicate with key managers through the HMC).
   - Connection status for each system-to-key manager connection (OK, Warning, and Error). Click **Error** or **Warning** to see a description of the issue.
   - Connection status for each system-to-HMC connection. The status values are as follows.

     OK
     The system can communicate with the key manager through the HMC.

Error
The system cannot communicate with the key manager through the HMC.

After the connectivity test is complete, and the status of all selected key managers is **OK**, click **CLOSE** on the **Test Connectivity** window to return to the **Choose Key Managers** window.

3. On the **Choose Key Managers** window, click **NEXT** to go to the next step.

Note: If only one key manager is defined, a message is displayed to warn you that *A minimum of two key managers are recommended for high availability*. Do one of the following.

- To add another key manager, click **CLOSE** on the message window, which returns you to the Choose Key Managers window. Select additional key managers or click **ADD KEY MANAGER** to define the additional key manager. Refer to "Add Key Manager" on page 963 for instructions.
- To continue with only one key manager defined, click **CONTINUE** on the message window to go to the next step.

Add Key Manager

Use the **Add key manager window** to define one or more key managers.

Note: Be aware that if you add one or more key managers using these instructions and then navigate back to previous steps in the **Choose Key Managers** action, the added key managers will continue to be included in the topology, but might not be operational.

1. On the **Choose Key Managers** window, click **ADD KEY MANAGER**.
2. On the **Add key manager** window, provide the following information.

Name
Name of the key manager that you want to add. This is a required field.

The name must comply with the following rules.

- Must not be the name of another key manager
- Must be between 1 and 64 characters long
- Can contain alphanumeric characters, blanks, periods, underscores, dashes, and the @ sign. Note that the name must not start or end with a blank.

Description
Description of the key manager that you want to add.

Hostname or IP Address
Fully-qualified domain name (FQDN), or IP address of the key manager that you want to add. This is a required field.

Port number
Port number of the key manager that you want to add. The default port number is 5696. This is a required field.

3. Click **CONNECT**. The **Connecting to** *key_manager* **on** *port_number* message dialog is displayed.

Do one of the following.

- If the connection cannot be completed, you are returned to the **Add key manager** window. Text that describes the error is displayed in red. Correct the problem and then click **CONNECT** again.
- If the connection is successful and the key manager is already trusted, you are finished adding the key manager and are returned to the **Choose Key Managers** window. The key manager you added is now displayed in the Choose Key Managers table. Return to Step 2 in "Choosing key managers when no defined key managers are available" on page 961 or Step 1 in "Choosing key managers when previously-defined key managers are available" on page 962 to continue with the **Choose Key Managers** step.
- If the connection is successful but the key manager is not yet trusted, the **Trust and import key manager certificate** window is displayed, which provides basic information about the certificate and an option for importing it. Do the following.

a. Review the certificate's details to verify that you want to trust it. In addition to displaying basic information about the certificate, the **Trust and import key manager certificate** window provides the option to view a full list of the certificate's attributes and their settings. Do one of the following.
   - If you do not want to review the full list of certificate attributes and their current settings, skip this step and proceed to step b.
   - To see more extensive information about the certificate before importing it, click the drop-down icon beside **See certificate details**. The full list of attributes for the certificate is displayed below the **See certificate details** option. Use the scroll bar to view the entire list.

b. Import the certificate by clicking **TRUST AND IMPORT CERTIFICATE**. The **Choose Key Managers** window is displayed, and the table now includes the information for the newly-defined key manager.

   If you do not want to import the certificate, click **CANCEL** on the **Trust and import key manager certificate** window to return to the **Choose Key Managers** window.

4. Review the information in the Choose Key Managers table and then, to continue with the **Choose Key Managers** step, do one of the following.
   - Return to step 2 of "Choosing key managers when no defined key managers are available" on page 961.
   - Return to step 1 of "Choosing key managers when previously-defined key managers are available" on page 962.

Step 3: Export to Key Managers

Use the **Export Certificates to Key Managers** window to export the certificates of the systems that you chose in "Step 1: Choose Systems" on page 960 to the key managers that you chose in "Step 2: Choose Key Managers" on page 960. (A key manager must import a system certificate in order to establish a mutually-authenticated connection to that system.)

The currently-selected systems and key managers are displayed in the **Current Selections** area.

1. To export the system certificate to the key manager, select one of the following options.

   Export directly to key managers
   Use this option to export the selected system certificates to key managers. In order to use this option you must have network access to the key managers. If you do not have access to the key managers, choose a different option for exporting the certificates.

   Export to USB
   Use this option to export the system certificates to a USB flash drive. This option is only available if you are logged into a local HMC. It is not available for remote users.

   Export to file system
   Use this option to download the system certificates to your workstation. The **Export to file system** option is available only to users who are on a workstation that is connected remotely.

   Email to key manager administrator
   Use this option to send the system certificate to a key manager administrator in an email.

   Export to FTP server
   Use this option to export certificates from systems to an FTP server.

2. After selecting an export option, click **CONTINUE**.
3. Depending on the export option you chose, do one of the following.
   - If you chose the **Export directly to key managers** option, the **Export to key manager** window is displayed.

     a. Provide information for the key manager in the following fields of the **Export to key manager** window.

If you chose more than one key manager, you must fill out the fields in this window for each key manager. The progress bar at the top of the window displays the name of each key manager as a step (sorted from left to right by name). When you successfully complete the information for the first key manager, the window is displayed again so you can enter information for the next key manager, and so on.

User name
Key manager REST API user name. This is a required field.

Password
Key manager REST API password. This is a required field.

REST port number
HTTPS port number that was configured during IBM Security Key Lifecycle Manager (ISKLM) installation for accessing the ISKLM graphical user interface and REST services. The ISKLM default values are **9443** for ISKLM 4 or **443** for ISKLM 3.0.1.

b. Click **CONNECT AND EXPORT**, then do one of the following.

– If you are exporting to a single key manager, do one of the following.

- If the certificate was successfully exported, the **Export to** *key_manager_name* **successful** message window is displayed. Click **CLOSE**.
- If the certificate was **not** successfully exported, a message that explains the error is displayed in red text on the **Export to key managers** window. Correct the error (such as entering a new user name and password) and then click **CONNECT AND EXPORT** again.

– If you are exporting to multiple key managers, do one of the following.

- If the certificate was successfully exported to the first key manager, the **Export to***key_manager_name***successful** message is displayed. Click **CLOSE**, then do the following.

1) Fill out the fields of the **Export to key managers** window for the next key manager, then click **CONNECT AND EXPORT**. Note that the names of the selected key managers are displayed at the top of the **Export to key managers** window. As you move from one key manager to the next, the related key manager name is highlighted.
2) If the certificate was successfully exported, the **Export to** *key_manager_name* **successful** message is displayed. Click **CLOSE**.
3) Repeat the preceding steps for all of the chosen key managers.

- If the certificate was **not** successfully exported to the first key manager, a message that explains the error is displayed in red text on the **Export to key managers** window. Correct the error (such as entering a new user name and password) and then click **CONNECT AND EXPORT** again. Or, if you wish to skip this key manager and proceed to the next key manager instead, click **NEXT**. The **Export to key managers** window is displayed for the next key manager.

  Repeat the preceding steps for all of the chosen key managers.

c. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Connect to key managers** action and return to the main **Topology view**. The **Topology view** now displays the specified systems and key managers, and the connections between them.

- If you chose the **Export to USB** option, the **Export to USB** window is displayed. A list of certificates that are associated with the systems that you chose in “Step 1: Choose Systems” on page 960 is displayed.

  This option is only available if you are logged into a local HMC. It is not available for remote users.

  a. In the **Export to USB** window, click **BROWSE** to specify the USB device and file path into which the certificate will be exported.

  Note: If this directory already contains a file that has the same name as the certificate that you are exporting, the existing file is overwritten by the exported certificate file.

  b. In the **Browse USB File Paths** window, select a USB device and file path, then click **OK**.

c. In the **Export to USB** window, the **File path** field now contains the file path you chose. Click **EXPORT**.

d. If the certificates are successfully exported to the USB device, the **Export to USB successful** message is displayed. Click **CLOSE**.

e. On the **Export successful** final confirmation message window, click **CLOSE** to close the **Connect to key managers** action and return to the main **Topology view**. The **Topology view** now displays the specified systems and key managers, and the connections between them.

- If you chose the **Export to file system** option, the **Export to file system** dialog is displayed, which launches a browser window for your local file system. The browser allows you to save the certificates associated with the systems that you chose in "Step 1: Choose Systems" on page 971. If the browser download does not start, click the link to restart the export.

  By default, the format of a single certificate name is ***system_name.extension*** (for example **CPC1.pem**). However, if you are exporting multiple certificates, they are compressed into a single file, and the format of the name is ***system_name*_certs.*extension*.zip** (for example, **CPC1_certs.extension.zip**).

  To export the certificates to the file system, do the following.

  a. Use the local browser window to save the certificates.

     – If the certificates are successfully exported to the file system, the **Export to file system successful** message is displayed. Click **CLOSE**.

     – If the certificates are not successfully exported to the file system, the **Export to file system failed** message is displayed, which includes a description of the error. Click **CLOSE**. Correct the error and then click **EXPORT** again.

  b. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Connect to key managers** action and return to the main **Topology view**. The **Topology view** now displays the specified systems and key managers, and the connections between them.

- If you chose the **Email to key manager administrator** option, the **Email to key manager administrator** window is displayed.

  This option is used to create an email request to import the certificates to the specified key managers and send that email to a key manager administrator's email address. The subject of the email is *Import and trust system certificates*.

  a. If the HMC's SMTP server has not already been configured using the **Monitor System Events** or **Configure Storage** task, the SMTP (Simple Mail Transfer Protocol) server must be configured before an email can be sent to the key manager administrator. Provide information for the following fields of the **Email to key manager administrator** window.

     SMTP server
     SMTP server name. This is a required field.

     SMTP port
     SMTP port. The default is 25.

  b. Click **SAVE**. The **Saving SMTP Server inputs** dialog indicates the progress of the save. When the save is successful, the **SMTP server successfully configured** message is displayed. Click **CLOSE**.

  c. On the **Email to key manager administrator** window, provide the key manager administrator's email address in the **Email address** field, and then provide it again in the **Confirm email address** field.

  d. Click **SEND**. The **Export by email successful** message is displayed, which indicates the email address you provided. Click **CLOSE**.

  e. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Connect to key managers** action and return to the main **Topology view**. The **Topology view** now displays the specified systems and key managers, and the connections between them.

- If you chose the **Export to FTP server** option, the **Export to FTP server** window is displayed, which allows you to identify the FTP server and specific file path into which the certificates should be exported. The names of the certificates are displayed near the top of the window.

  a. Provide information for the following fields of the **Export to FTP server** window.

  Host name
  Host name of the FTP server. This is a required field.

  User name
  User name associated with the specified FTP server. This is a required field.

  Password
  Password associated with the specified user name. This is a required field.

  Protocol
  The protocol to be used for exporting the certificates. **FTP**, **FTPS**, or **SFTP** can be selected using the drop-down menu. The default value is **FTP**.

  File path
  An existing directory on the FTP server, into which the certificates will be exported.

  b. Click **EXPORT**. The **Export to FTP server successful** message is displayed. Click **CLOSE**.

  c. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Connect to key managers** action and return to the main **Topology view**. The **Topology view** now displays the specified systems and key managers, and the connections between them.

Configure system policies

The **Configure system policies** action guides you through the process of updating the Fibre Channel endpoint security policies of selected systems. The systems' security policies define expiration times for the authentication key and encryption key that are used to authenticate the endpoints and encrypt the data that flows across the Fibre Channel link.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

To start the **Configure system policies** action, go to “Step 1: Choose Systems” on page 967.

Step 1: Choose Systems

Use the **Choose Systems** window to select one or more systems (CPCs).

1. The table displays only systems that are connected to configured key managers. Select one or more systems to update their security policies.

   Note: The systems you choose are not required to have common key managers or encryption and authentication endpoint key expiration values.

   The table includes the following information.

   Name
   System name.

   Configured Key Managers
   Name of one or more key managers that are currently connected to the system that is displayed in this table row.

   Authentication key expiration(hrs)
   Fibre Channel endpoint device authentication key expiration time, in hours. Valid values are from 1 to 360 hours. The default value is 168.

   Encryption key expiration(hrs)
   Fibre Channel endpoint device encryption key expiration time, in hours. Valid values are from 1 to 24 hours. The default value is 8.

2. Click **NEXT**.

Step 2: Choose Security Policy

Use the **Choose Security Policy** window to specify a security policy for the selected systems. The **Same security policy as** option and system drop-down selection box allow you to select an existing system and apply its security policy to all of the systems you chose in "Step 1: Choose Systems" on page 967.

1. Choose a security policy using one of the following options.
   - Use the same security policy as another system:
     a. Select the **Same security policy as** option.
     b. Use the drop-down list to choose a system. For example, if you selected system **CPC2** in the previous step and you want **CPC2** to have the same policy that is used by system **CPC1**, you would use the system drop-down list to choose **CPC1**.
     c. After choosing a system, if you would like to review details about the security policy of that system, click **Show** *system_name* **details**.
   - Define a custom security policy for the chosen system:
     a. Specify an expiration value in the **Choose expiration time for the Fibre Channel endpoint device authentication key** field. Valid values are from 1 to 360 hours. The default value is 168 hours.
     b. Specify an expiration value in the **Choose expiration time for the Fibre Channel endpoint device encryption key** field. Valid values are from 1 to 24 hours. The default value is 8 hours.
2. Click **SAVE**. The **Save confirmation** window is displayed, which shows you the systems that will be updated. To confirm that you want to apply the policy to the selected systems, click **CONTINUE**.
3. If the configure is successful, the **Configure successful** message window is displayed.

   If the configure is not successful, the **Configure failed** message window is displayed, which includes a description of the problem.

   Click **CLOSE** to exit the **Configure system policy** action and return to the **Topology view**.

Create certificate signing request

The **Create certificate signing request** action guides you through the process of requesting CA-signed certificates from a certificate signing authority.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

To start the **Create certificate signing request** action, go to "Step 1: Choose Systems" on page 968.

Step 1: Choose Systems

Use the **Choose Systems** window to select one or more systems (CPCs). Only the systems that meet the requirements for endpoint authentication are included in the table. In this step, you can create multiple signing requests by choosing multiple systems.

1. In the Choose Systems table, select one or more systems. The table displays all of the supported systems and includes the following information for each one.

   Name
   Name of the system.

   Configured Key Managers
   Name of one or more key managers that are currently defined to the system that is displayed in this table row.

   Certificate Type
   Type of certificate; **Self-signed** or **CA-signed** (certificate authority-signed).
2. Click **NEXT** to go to the next step.

Step 2: Export Certificate Signing Request

Use the **Export Certificate Signing Request** window to export the certificate signing requests of the systems that you chose in "Step 1: Choose Systems" on page 968. The **Current Selections** area displays the specified systems.

1. To export the certificate signing requests to the certificate authority for signing, select one of the following options.

   Export to USB
   Use this option to export the certificate signing requests to a USB flash drive. This option is only available if you are logged into a local HMC. It is not available for remote users.

   Export to file system
   Use this option to export the certificate signing requests to a file system. The **Export to file system** option is available only to users who are on a workstation file system that is connected remotely.

   Email to certificate signing authority
   Use this option to send the certificate signing requests to the certificate signing authority in an email.

   Export to FTP server
   Use this option to export the certificate signing requests to an FTP server.
2. After selecting an export option, click **CONTINUE**.
3. Depending on the export option you chose, do one of the following.
   - If you chose the **Export to USB** option, the **Export to USB** window is displayed. A list of certificate signing requests that are associated with the systems that you chose in "Step 1: Choose Systems" on page 968 is included in the window.

     This option is only available if you are logged into a local HMC. It is not available for remote users.

     a. In the **Export to USB** window, click **BROWSE** to specify the USB device and file path into which the certificate will be exported.

        Note: If this directory already contains a file that has the same name as the certificate signing requests that you are exporting, the existing file is overwritten by the exported certificate file.

     b. In the **Browse USB File Paths** window, select a USB device and file path, then click OK.

     c. In the **Export to USB** window, the **File path** field now contains the file path you chose. Click **EXPORT**.

     d. If the certificate signing requests are successfully exported to the USB device, the **Export to USB successful** message is displayed. Click **CLOSE**.
   - If you chose the **Export to file system** option, the **Export to file system** dialog is displayed, which launches a browser window for your local file system. The browser allows you to save the certificate signing requests that are associated with the systems that you chose in "Step 1: Choose Systems" on page 968 and submit them to a certificate authority for signing. If the browser download does not start, click the link to restart the export.

     By default, the format of a single certificate signing request name is ***system_name.extension*** (for example **CPC1.csr**). However, if you are exporting multiple certificate signing requests, they are compressed into a single file, and the format of the name is ***system_name*_certs.zip** (for example, **CPC1_certs.zip**).

     To export the certificate signing request to a file system, do the following.

     a. Use the local browser window to save the certificates for signing.

     b. If the certificate signing requests are successfully exported to the file system, the **Export successful** message is displayed. Click **CLOSE**.
   - If you chose the **Email to certificate signing authority** option, the **Email to certificate signing authority** window is displayed.

This option is used to submit a certificate signing request to a certificate authority by way of email. The subject of the email is *Exported files*, and the body of the email is *Please see the attached exported files*.

a. The SMTP (Simple Mail Transfer Protocol) manager must be configured before an email can be sent to the certificate signing authority. Provide information for the following fields of the **Email to certificate signing authority** window.

SMTP server
SMTP server name. This is a required field.

SMTP port
SMTP port. The default is 25.

b. Click **SAVE**. The **Saving SMTP Server inputs** dialog indicates the progress of the save. When the save is successful, the **SMTP server successfully configured** message is displayed. Click **CLOSE**.

c. On the **Email to certificate signing authority window**, provide the certificate signing authority's email address in the **Email** field, and then provide it again in the **Confirm email** field.

d. Click **SEND**. The **Export by email successful** message is displayed, which indicates the email address you provided. Click **CLOSE**.

- If you chose the **Export to FTP server** option, the **Export to FTP server** window is displayed, which allows you to identify the FTP server and specific file path into which the certificate signing requests should be exported. The names of the certificates are displayed near the top of the window.

a. Provide information for the following fields of the **Export to FTP server** window.

Host name
Host name of the FTP server. This is a required field.

User name
User name associated with the specified FTP server. This is a required field.

Password
Password associated with the specified **User name**. This is a required field.

Protocol
The protocol to be used for exporting the certificate. **FTP**, **FTPS**, or **SFTP** can be selected using the drop-down menu. The default value is **FTP**.

File path
An existing directory on the FTP server, into which the certificate will be exported.

b. Click **EXPORT**. The **Export to FTP server successful** message is displayed. Click **CLOSE**.

4. When the signing request is successfully created, the **Create certificate signing request successful** window is displayed. Click **CLOSE** to exit the **Create certificate signing request** action and return to the **Topology view**.
5. After receiving the signed certificate, update the certificate on the system's configured key managers and then use the **Import signed certificate** action to update the certificate on the system.

Create self-signed certificate

The **Create self-signed certificate** action guides you through the process of using a system's existing certificate to create a self-signed certificate. This action is only available when there are systems with certificate authority (CA)-signed certificates.

Note: Creating a self-signed certificate causes the configured key managers to lose their ability to authenticate with the specified system. After completing this action, use the **Export certificates to key manager** action to export the self-signed certificate to the configured key managers.

Use the **Create Self-Signed Certificate** window to select a system (CPC).

1. In the table, select the system for which you want to create a self-signed certificate. The table includes the following information.

Name
System name.

Configured Key Managers
Names of key managers that are currently connected to the system that is displayed in this table row.

Certificate Type
Type of certificate. Only **CA-signed** (certificate authority-signed) certificates are displayed in the table. If there are no systems that have CA-signed certificates, the **Create self-signed certificate** action is not available.

2. Click **CREATE**.The **Create self-signed certificate confirmation** window is displayed, which warns you that creating a self-signed certificate causes the configured key managers to lose their ability to authenticate with the specified system.

   To continue creating the self-signed certificate, click **CONTINUE**. Otherwise, click **CANCEL** to return to the **Create Self-Signed Certificate** window.
3. If the self-signed certificate was created successfully, the **Create successful** message window is displayed. Click **CLOSE** to exit the **Create self-signed certificate** action and return to the **Topology view**
4. Use the **Export certificates to key managers** action to export the self-signed certificate to the configured key managers.

Edit certificates

The **Edit certificates** action guides you through the process of changing the properties of a self-signed certificate, such as its expiration date and time.

Notes:

- After editing a system certificate, you must export it to all of the key managers that are configured to the system. This is because the key managers lose their ability to authenticate with the system after a certificate has been changed.
- In order to complete this action, at least one key manager must be connected to a system.
- Only self-signed certificates can be edited using this action.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

To start the **Edit certificates** action, go to “Step 1: Choose Systems” on page 971.

Step 1: Choose Systems

Use the **Choose Systems** window to select one or more systems (CPCs). The table contains only the systems that meet the requirements for endpoint authentication.

Note that if you select multiple systems, any key managers that are defined must be the same for all of the specified systems.

1. In the table, select the systems whose certificates will be edited. The table includes the following information for each system.

   Name
   System name.

   Configured Key Managers
   Name of one or more key managers that are currently defined the system that is displayed in this table row.
2. If there are no errors after selecting one or more systems, click **NEXT** to go to the next step.

Step 2: Edit Certificates

Use the **Edit System Certificates** window to view and edit the details of a system's self-signed certificate.

Note: After editing a system certificate, you must export it to all of the key managers that are configured to the system. This is because the key managers lose their ability to authenticate with the system after a certificate has been changed.

Note: Only the **Valid until (Date** and **Time** only) fields are currently editable. The **Valid until** field is used to control the expiration information for a certificate.

To edit a system certificate, do the following.

1. If you selected multiple systems in "Step 1: Choose Systems" on page 971, click the drop-down menu near the top of the window and select the system that you want to edit. This menu contains all of the systems that you selected in "Step 1: Choose Systems" on page 971. If you chose only one system, this menu is not displayed.

   The **Edit System Certificates** window displays the certificate of the system you choose. If information has not be defined for a field, the field is displayed as empty.

   Click the **See additional certificate details** drop-down icon to see the full list of details for a certificate. Use the scroll bar on the right to view the entire list.
2. To update a certificate's expiration information, edit the **Valid until** (**Date** and **Time** only) field of the **Edit System Certificate** window, as needed. Note that the date and time that you provide must be at least 30 days in the future. **Valid until** is a required field.

   If you selected multiple systems in "Step 1: Choose Systems" on page 971, click the drop-down menu again, select the next system, and edit its certificate. Repeat these steps for each of the selected systems.
3. After completing the editing changes, click **NEXT**. Note that **NEXT** is not enabled until all of the selected systems certificates have been edited.
4. The **Save system certificates** window is displayed to warn you that, after saving the certificates, the key managers will not be able to authenticate those systems until the certificates are exported to all key managers. Click **SAVE** to save the edited certificates.
5. Proceed to the next step, "Step 3: Export to Key Managers" on page 972.

Step 3: Export to Key Managers

Use the **Export Certificates to Key Managers** window to export the self-signed certificates to key managers. You must have network access to the key managers.

1. To export the self-signed certificates to the key managers, select one of the following options.

   Export directly to key managers
   Use this option to export the system certificates to key managers. In order to use this option you must have network access to the key managers. If you do not have access to the key managers, choose a different option for exporting the certificates.

   Export to USB
   Use this option to export the system certificates to a USB flash drive. This option is only available if you are logged into a local HMC. It is not available for remote users.

   Export to file system
   Use this option to download the system certificates to your workstation. The **Export to file system** option is available only to users who are on a workstation that is connected remotely.

   Email to key manager administrator
   Use this option to send the system certificates to a key manager administrator in an email.

   Export to FTP server
   Use this option to export certificates from systems to an FTP server.
2. After selecting and export options, click **CONTINUE**.

3. Depending on the export option you chose, do one of the following.

   - If you chose the **Export directly to key managers** option, the **Export to key managers** window is displayed.

     a. In the **Export to key manager** window, provide information for the key managers in the following fields.

        If you chose more than one key manager, you must fill out the fields in this window for each key manager. The progress bar at the top of the window includes the name of each key manager as a step (sorted from left to right by name). When you successfully complete the information for the first key manager, the window is displayed again so you can enter information for the next key manager, and so on.

        Username
        Key manager REST API user name

        Password
        Key manager REST API password

        REST port number
        HTTPS port number that was configured during IBM Security Key Lifecycle Manager (ISKLM) installation for accessing the ISKLM graphical user interface and REST services. The ISKLM default values are **9443** for ISKLM 4 or **443** for ISKLM 3.0.1.

     b. Click **CONNECT AND EXPORT**, then do one of the following.

        – If you are exporting to a single key manager, do one of the following.

          - If the certificate was successfully exported, the **Export to** *key_manager_name* **successful** message is displayed. Click **CLOSE** to close the **Edit certificates** action and return to the **Topology view**.
          - If the certificate was **not** successfully exported, a message that explains the error is displayed in red text on the window. Correct the error (such as entering a new user name and password) and then click **CONNECT AND EXPORT** again.

        – If you are exporting to multiple key managers, do one of the following.

          - If the certificate was successfully exported to the first key manager, the **Export to** *key_manager_name* **successful** message is displayed. Click **CLOSE**, then do the following.

            1) Enter information into the fields of the **Export to key managers** window for the next key manager, then click **CONNECT AND EXPORT**.
            2) If the certificate was successfully exported, the **Export to** *key_manager_name* **successful** message is displayed. Click **CLOSE**.
            3) Repeat the preceding steps for all of the chosen key managers. After the last key manager is successfully exported, click **CLOSE** to close the **Edit certificates** action and return to the **Topology view**.

          - If the certificate was **not** successfully exported to the first key manager, a message that explains the error is displayed in red text on the **Export to key managers** window. Correct the error (such as entering a new user name and password) and then click **CONNECT AND EXPORT** again. Or, if you wish to skip this key manager and proceed to the next key manager instead, click **NEXT**. The **Export to key managers** window is displayed for the next key manager.

   - If you chose the **Export to USB** option, the **Export to USB** window is displayed. A list of certificates that are associated with the systems that you chose in “Step 1: Choose Systems” on page 971 is displayed.

     This option is only available if you are logged into a local HMC. It is not available for remote users.

     a. In the **Export to USB** window, click **BROWSE** to specify the USB device and file path into which the certificates will be exported.

Note: If this directory already contains a file that has the same name as a certificate that you are exporting, the existing file is overwritten by the exported certificate file.

b. In the **Browse USB File Paths** window, select a USB device and file path, then click **OK**.

c. In the **Export to USB** window, the **File path** field now contains the file path you chose. Click **EXPORT**.

d. If the certificates are successfully exported to the USB device, the **Export to USB successful** message is displayed. Click **CLOSE**.

e. On the **Export successful** final confirmation message window, click **CLOSE** to close the **Edit certificates** action and return to the main **Topology view**.

- If you chose the **Export to file system** option, the **Export to file system** dialog is displayed, which launches a browser window for your local file system. The browser allows you to save the certificates associated with the systems that you chose in "Step 1: Choose Systems" on page 971. If the browser download does not start, click the link to restart the export.

  By default, the format of a single certificate name is ***system_name.extension*** (for example **CPC1.pem**). However, if you are exporting multiple certificates, they are compressed into a single file, and the format of the name is ***system_name*_certs.*extension*.zip** (for example, **CPC1_certs.extension.zip**).

  To export the certificates to the file system, do the following.

  a. Use the local browser window to save the certificates.

  – If the certificates are successfully exported to the file system, the **Export to file system successful** message is displayed. Click **CLOSE**.

  – If the certificates are not successfully exported to the file system, the **Export to file system failed** message is displayed, which includes a description of the error. Click **CLOSE**. Correct the error and then click **EXPORT** again.

  b. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Edit certificates** action and return to the main **Topology view**.

- If you chose the **Email to key manager administrator** option, the **Email to key manager administrator** window is displayed.

  This option is used to create an email request to import the certificates to the specified key managers and send that email to a key manager administrator's email address. The subject of the email is *Import and trust system certificates*.

  a. If the HMC's SMTP server has not already been configured using the **Monitor System Events** or **Configure Storage** task, the SMTP (Simple Mail Transfer Protocol) server must be configured before an email can be sent to the key manager administrator. Provide information for the following fields of the **Email to key manager administrator** window.

  SMTP server
  SMTP server name. This is a required field.

  SMTP port
  SMTP port. The default is 25.

  b. Click **SAVE**. The **Saving SMTP Server inputs** dialog indicates the progress of the save. When the save is successful, the **SMTP server successfully configured** message is displayed. Click **CLOSE**.

  c. On the **Email to key manager administrator** window, provide the key manager administrator's email address in the **Email address** field, and then provide it again in the **Confirm email address** field.

  d. Click **SEND**. The **Export by email successful** message is displayed, which indicates the email address you provided. Click **CLOSE**.

  e. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Edit certificates** action and return to the main **Topology view**.

- If you chose the **Export to FTP server** option, the **Export to FTP server** window is displayed, which allows you to identify the FTP server and specific file path into which the certificates should be exported. The names of the certificates are displayed near the top of the window.

  a. Provide information for the following fields of the **Export to FTP server** window.

  Host name
  Host name of the FTP server. This is a required field.

  User name
  User name associated with the specified FTP server. This is a required field.

  Password
  Password associated with the specified user name. This is a required field.

  Protocol
  The protocol to be used for exporting the certificates. **FTP**, **FTPS**, or **SFTP** can be selected using the drop-down menu. The default value is **FTP**.

  File path
  An existing directory on the FTP server, into which the certificates will be exported.

  b. Click **EXPORT**. The **Export to FTP server successful** message is displayed. Click **CLOSE**.

  c. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Edit certificates** action and return to the main **Topology view**.

Export certificates to key managers

The **Export certificates to key managers** action guides you through the process of selecting and exporting system certificates, which will be imported by key managers.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

To start the **Export certificates to key managers** action, go to “Step 1: Choose Systems” on page 975.

Step 1: Choose Systems

Use the **Choose Systems** window to select one or more systems (CPCs). Only the systems that meet the requirements for endpoint authentication are included in the table.

Note that if you select multiple systems, each system must have the same key managers defined as all the other systems. Selections that do not meet this rule are highlighted in red in the table and an error status icon is displayed beside them.

1. In the table, select one or more systems. The table includes the following information.

   Name
   Name of the system.

   Configured Key Managers
   Name of one or more key managers that are currently defined to the system that is displayed in this table row.

   Note that if you select multiple systems, any key managers that are defined must be the same for all of the selected systems. Selections that do not meet these rules are highlighted in red in the table and an error status icon is displayed beside them.

2. If there are no errors after selecting one or more systems, click **NEXT** to go to the next step.

Step 2: Export to Key Managers

Use the **Export Certificates to Key Managers** window to export the certificates of the systems that you chose in “Step 1: Choose Systems” on page 975 to key managers. You must have network access to the key managers.

1. To export the self-signed certificates to the key managers, select one of the following options.

Export directly to key managers
Use this option to export the system certificates to key managers. In order to use this option you must have network access to the key managers. If you do not have access to the key managers, choose a different option for exporting the certificates.

Export to USB
Use this option to export the system certificates to a USB flash drive. This option is only available if you are logged into a local HMC. It is not available for remote users.

Export to file system
Use this option to download the system certificates to your workstation. The **Export to file system** option is available only to users who are on a workstation that is connected remotely.

Email to key manager administrator
Use this option to send the system certificates to a key manager administrator in an email.

Export to FTP server
Use this option to export certificates from systems to an FTP server.

2. After selecting an export option, click **CONTINUE**.
3. Depending on the export option you chose, do one of the following.

- If you chose the **Export directly to key managers** option, the **Export to key managers** window is displayed.

  a. In the **Export to key manager** window, provide information for the key managers in the following fields.

  If you chose more than one key manager, you must fill out the fields in this window for each key manager. The progress bar at the top of the window includes the name of each key manager as a step (sorted from left to right by name). When you successfully complete the information for the first key manager, the window is displayed again so you can enter information for the next key manager, and so on.

  User name
  Key manager user name.

  Password
  Key manager password.

  REST port number
  HTTPS port number that was configured during IBM Security Key Lifecycle Manager (ISKLM) installation for accessing the ISKLM graphical user interface and REST services. The ISKLM default values are **9443** for ISKLM 4 or **443** for ISKLM 3.0.1.

  b. Click **CONNECT AND EXPORT**, then do one of the following.

  – If you are exporting to a single key manager, do one of the following.

  - If the certificate was successfully exported, the **Export to** *key_manager_name* **successful** message window is displayed. Click **CLOSE**.
  - If the certificate was **not** successfully exported, a message that explains the error is displayed in red text on the **Export to key managers** window. Correct the error (such as entering a new user name and password) and then click **CONNECT AND EXPORT** again.

  – If you are exporting to multiple key managers, do one of the following.

  - If the certificate was successfully exported to the first key manager, the **Export to** *key_manager_name* **successful** message is displayed. Click **CLOSE**, then do the following.

    1) Enter information into the fields of the **Export to key managers** window for the next key manager, then click **CONNECT AND EXPORT**.
    2) If the certificate was successfully exported, the **Export to** *key_manager_name* **successful** message is displayed. Click **CLOSE**.
    3) Repeat the preceding steps for all of the chosen key managers.

- If the certificate was **not** successfully exported to the first key manager, a message that explains the error is displayed in red text on the **Export to key managers** window. Correct the error (such as entering a new user name and password) and then click **CONNECT AND EXPORT** again. Or, if you wish to skip this key manager and proceed to the next key manager instead, click **NEXT**. The **Export to key managers** window is displayed for the next key manager.

c. On the **Export successful** final confirmation message window, click **CLOSE** to close the **Export certificates to key managers** action and return to the main **Topology view**.

- If you chose the **Export to USB** option, the **Export to USB** window is displayed. A list of certificates that are associated with the systems that you chose in "Step 1: Choose Systems" on page 975 is displayed.

  This option is only available if you are logged into a local HMC. It is not available for remote users.

  a. In the **Export to USB** window, click **BROWSE** to specify the USB device and file path into which the certificates will be exported.

     Note: If this directory already contains a file that has the same name as a certificate that you are exporting, the existing file is overwritten by the exported certificate file.

  b. In the **Browse USB File Paths** window, select a USB device and file path, then click **OK**.

  c. In the **Export to USB** window, the **File path** field now contains the file path you chose. Click **EXPORT**.

  d. If the certificates are successfully exported to the USB device, the **Export to USB successful** message is displayed. Click **CLOSE**.

  e. On the **Export successful** final confirmation message window, click **CLOSE** to close the **Export certificates to key managers** action and return to the main **Topology view**.

- If you chose the **Export to file system** option, the **Export to file system** dialog is displayed, which launches a browser window for your local file system. The browser allows you to save the certificates associated with the systems that you chose in "Step 1: Choose Systems" on page 975. If the browser download does not start, click the link to restart the export.

  By default, the format of a single certificate name is ***system_name.extension*** (for example **CPC1.pem**). However, if you are exporting multiple certificates, they are compressed into a single file, and the format of the name is ***system_name*_certs.*extension*.zip** (for example, **CPC1_certs.extension.zip**).

  To export the certificates to the file system, do the following.

  a. Use the local browser window to save the certificates.

     – If the certificates are successfully exported to the file system, the **Export to file system successful** message is displayed. Click **CLOSE**.

     – If the certificates are not successfully exported to the file system, the **Export to file system failed** message is displayed, which includes a description of the error. Click **CLOSE**. Correct the error and then click **EXPORT** again.

  b. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Export certificates to key managers** action and return to the main **Topology view**.

- If you chose the **Email to key manager administrator** option, the **Email to key manager administrator** window is displayed.

  This option is used to create an email request to import the certificates to the specified key managers and send that email to a key manager administrator's email address. The subject of the email is *Import and trust system certificates*.

  a. If the HMC's SMTP server has not already been configured using the **Monitor System Events** or **Configure Storage** task, the SMTP (Simple Mail Transfer Protocol) server must be configured before an email can be sent to the key manager administrator. Provide information for the following fields of the **Email to key manager administrator** window.

SMTP server
SMTP server name. This is a required field.

SMTP port
SMTP port. The default is 25.

b. Click **SAVE**. The **Saving SMTP Server inputs** dialog indicates the progress of the save. When the save is successful, the **SMTP server successfully configured** message is displayed. Click **CLOSE**.

c. On the **Email to key manager administrator** window, provide the key manager administrator's email address in the **Email address** field, and then provide it again in the **Confirm email address** field.

d. Click **SEND**. The **Export by email successful** message is displayed, which indicates the email address you provided. Click **CLOSE**.

e. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Export certificates to key managers** action and return to the main **Topology view**.

- If you chose the **Export to FTP server** option, the **Export to FTP server** window is displayed, which allows you to identify the FTP server and specific file path into which the certificates should be exported. The names of the certificates are displayed near the top of the window.

a. Provide information for the following fields of the **Export to FTP server** window.

Host name
Host name of the FTP server. This is a required field.

User name
User name associated with the specified FTP server. This is a required field.

Password
Password associated with the specified user name. This is a required field.

Protocol
The protocol to be used for exporting the certificates. **FTP**, **FTPS**, or **SFTP** can be selected using the drop-down menu. The default value is **FTP**.

File path
An existing directory on the FTP server, into which the certificates will be exported.

b. Click **EXPORT**. The **Export to FTP server successful** message is displayed. Click **CLOSE**.

c. On the **Export successful** final confirmation message window. Click **CLOSE** to close the **Export certificates to key managers** action and return to the main **Topology view**.

Import key manager certificate

The **Import key manager certificate** action guides you through the process of trusting and importing one or more new or changed key manager certificates.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

To start the **Import key manager certificate** action, go to “Step 1: Select Source” on page 978.

Step 1: Select Source

Use the **Select Source to Import** window to specify the location of the key manager certificate to be imported.

The certificate can be imported from a key manager, a workstation file system that is connected remotely, or from the HMC USB when connected locally. Refer to one of the following sections, depending on the source of the certificate.

- “Select the source of the certificate directly from a key manager (local or remote users)” on page 979
- “Select the source of the certificate from a USB device (local users only)” on page 979

- “Select the source of the certificate from a file system (remote users only)” on page 979

Select the source of the certificate directly from a key manager (local or remote users)

In the **Select Source to Import** window, do the following.

1. In the **Source** field, select **Import from key manager**. A table of key managers is displayed, which includes the following information.

   Name
   Name of the key manager.

   Description
   Description of the key manager.

   Hostname or IP Address
   Fully-qualified domain name (FQDN), or IP address of the key manager.

   Port
   Key manager port number. The default value is 5696.
2. In the table, choose one key manager.
3. On the **Select Source to Input** window, click **NEXT**.
4. Proceed to “Step 2: Choose Systems” on page 980 in this online help.

Select the source of the certificate from a USB device (local users only)

Note: This option is only available if you are logged into a local HMC. It is not available for remote users.

In the **Select Source to Import** window, do the following.

1. In the **Source** field, select **Import from USB**.
2. In the **Certificate file** field, use **BROWSE** to select the USB device and file path of the certificate.
   a. In the **Browse USB Files** window, select one certificate file. The **Browse USB Files** window displays the files in the following table columns. All of the files that are available on USB devices and have the required **.cer**, **.crt**, **.der**, **.p7b**, or **.pem** certificate file extension are included.

      Important: The certificate files must be smaller than 1 MB.

      Media Label
      USB device name.

      Name
      Certificate file name.
   b. Click **OK**. The **Select Source to Import** window returns. The **Certificate file** field now displays the certificate file that you selected.
   c. On the **Select Source to Import** window, click **OK**.
   d. Proceed to “Step 2: Choose Systems” on page 980 in this online help.

Select the source of the certificate from a file system (remote users only)

Note: This option is available only to users who are on a workstation file system that is connected remotely.

1. In the **Source** field, select **Import from file system**.
2. In the **Certificate file** field, click **BROWSE** to select one certificate file. The remote file system browser opens and displays the files with **.cer**, **.crt**, **.der**, **.p7b**, or **.pem** file extensions. Navigate to the file and select it.
3. In the **Select Source to Import** window, the **Certificate file** field now displays the file that you selected.

4. Click **NEXT**.
5. Proceed to "Step 2: Choose Systems" on page 980 in this online help.

Step 2: Choose Systems

Use the **Choose Systems** window to specify one or more systems to which the key manager certificate will be imported. Only the systems that are enabled for endpoint authentication, and are available for selection, are included in the table. The key manager that is the source of the certificate is displayed in the **Current Selections** area.

1. In the table, select one or more systems to which you want to import the key manager certificate. The table includes the following information.

   Name
   System name.

   Configured Key Managers
   Name of one or more key managers that are currently defined to the system that is displayed in this table row.
2. Click **IMPORT**.
3. On the **Import confirmation** window, click **CONTINUE** to proceed with the import.
4. If the certificate is already trusted by the specified systems, the **Certificate already trusted** message window is displayed. Click **CLOSE** to return to the **Choose Systems** window and deselect all of the systems that were listed in the message.
5. Use the **Trust and import key manager certificate** window to trust and import the key manager certificate to the specified systems, as follows.
   a. Review the certificate details. In addition to displaying basic information about the certificate, the **Trust and import key manager certificate** window provides the option to view a full list of the certificate's attributes and their settings. Do one of the following.
      - To see more extensive information about the certificate before importing it, click the drop-down icon beside **See certificate details**. The full list of attributes for the certificate are displayed below the **See certificate details** option. Use the scroll bar to view the entire list.
      - If you do not want to review the full list of certificate attributes and their current settings, skip this step and proceed directly to Step b.
   b. Import the key manager certificate by clicking **TRUST AND IMPORT CERTIFICATE**.

      If you chose multiple systems on the **Choose Systems** window, the certificate is trusted for all chosen systems at the same time.
   c. If the certificate is successfully imported, the **Import successful** message is displayed. Click **CLOSE** to close the **Import key manage certificate** action and return to the **Topology view**.

Import signed certificate

The **Import signed certificate** action guides you through the process of replacing a system certificate with a certificate authority (CA)-signed certificate. You can import the certificate from a USB device (only if you are logged into a local HMC) or a file system (only if you are on a workstation file system that is connected remotely).

Important: Before continuing with this action, ensure that the signed certificate was imported to the key managers for the specified system. Otherwise, continuing with this action will cause the existing key manager certificate for this system to become invalid.

Use the **Import Signed Certificate** window to specify the directory path and file name of the signed certificate that will be imported.

If you are logged into a local HMC, you must import the certificate from a USB device. If you are logged in remotely, you must import the certificate from a file system. On the **Import Signed Certificate** window, the **Source** field detects your access mode and displays either the **USB** or **File system** option on the automatically.

Refer to the following help section that matches your modes of access.

- “Import the signed certificate from a USB device” on page 981
- “Import the signed certificate from a file system” on page 981

Import the signed certificate from a USB device

To import the signed certificate from a USB device, do the following.

1. In the **Certificate file** field of the **Import Signed Certificate** window, click **BROWSE** to select the file to import.
2. In the **Browse USB Files** window, select a certificate file. The **Browse USB Files** window displays all of the files on the available USB devices that have the **.cer**, **.crt**, **.der**, **.p7b**, or **.pem** certificate file extension. The table contains the following fields.

   Media Label
   USB device name.

   Name
   Name of the certificate file.
3. Click **OK**.
4. In the **Import Signed Certificate** window, the **Certificate file** field now displays the file that you selected. Click **CONTINUE**.
5. The **Import signed certificate confirmation** window is displayed. It contains basic information about the certificate, reminds you that the signed certificate must be imported to the key manager before importing it to the system, and asks you to confirm that you want to import it. To see more extensive information about the certificate, click the drop-down icon beside **See certificate details**. The full list of attributes for the certificate are displayed below the **See certificate details** option. Use the scroll bar to view the entire list.

   If you are sure that you want to import the certificate, click **IMPORT** on the **Confirm import signed certificate** window.
6. If the import is successful, the **Import successful** message window is displayed. Click **CLOSE** to exit the **Import signed certificate** action and return to the **Topology view**.

Import the signed certificate from a file system

To import the signed certificate from a file system, do the following.

1. In the **Certificate file** field, of the **Import Signed Certificate** window, click **BROWSE** to select the file to import. The remote file system browser is displayed.
2. In the remote file system browser, navigate to the file and select it.
3. In the **Import Signed Certificate** window, the **Certificate file** field now displays the file you selected. Click **CONTINUE**.
4. The **Import signed certificate confirmation** window is displayed. It contains basic information about the certificate, reminds you that the signed certificate must be imported to the key manager before importing it to the system, and asks you to confirm that you want to import it. To see more extensive information about the certificate, click the drop-down icon beside **See certificate details**. The full list of attributes for the certificate are displayed below the **See certificate details** option. Use the scroll bar to view the entire list.

   If you are sure that you want to import the certificate, click **IMPORT** on the **Import Signed Certificate Confirmation** window.
5. If the import is successful, the **Import successful** message window is displayed. Click **CLOSE** to exit the **Import signed certificate** action and return to the **Topology view**.

Remove key manager connections

The **Remove key manager connections** action guides you through the process of removing the secure connection between a key manager and one or more systems (CPCs).

Important: Removing key managers might be disruptive to running workloads. When the connections between a key manager and systems are removed, that key manager definition is deleted.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

To start the **Remove key manager connections** action, go to "Step 1: Choose Key Manager" on page 982.

Step 1: Choose Key Manager

Use the **Choose Key Managers** window to select a key manager from which you want to remove one or more system connections.

1. In the table, select the key manager. Note that only one key manager can be selected at a time. The table includes the following information.

   Name
   Name of the key manager.

   Description
   Description of the key manager.

   Hostname or IP Address
   Fully-qualified domain name (FQDN), or IP address of the key manager.

   Port
   Key manager port number. The default value is 5696.

   Note: If no key managers are defined, the table is empty.
2. Click **NEXT**.

Step 2: Choose Systems

Use the **Choose Systems** window to select one or more systems (CPCs). The table displays only systems that have connections to the key manager that you chose in "Step 1: Choose Key Manager" on page 982. The **Current Selections** area displays the specified key manager.

1. In the table, select the systems that you want to disconnect from the key manager. The table includes the following information.

   Name
   Name of the system.

   Configured Key Managers
   Name of one or more key managers that are currently defined to the system that is displayed in this table row.

   Note: If all of the systems that are connected to the specified key manager are selected for removal, a yellow warning icon is displayed beside each system. When you hover over the icon, a message warns you that removing all connections to the key manager causes its definition to be deleted.
2. Click **REMOVE**.
3. The **Disruptive Configuration Confirmation** window is displayed, which tells you to check the storage configuration policies to ensure that the key manager-to-system connections can be removed without disrupting the data flow between the specified systems and storage. To proceed with removing the key manager connections, enter your password in the **Password** field, then click **CONTINUE**.

4. If the remove is successful, the **Remove successful** message window is displayed. Click **CLOSE** to exit the **Remove key manager connections** action and return to the **Topology view**. The **Topology view** no longer displays the specified key manager.

View adapter security

The **View adapter security** action guides you through the process of viewing the security capabilities of the Fibre Channel endpoints for the IBM FICON Express adapters associated with a specified system (CPC).

1. Use the **Choose system** window to select a system. The table contains only the systems that meet the requirements for endpoint authentication.
   a. In the table, select a Fibre Channel Endpoint Security-enabled system.
   b. If there are no errors after selecting a system, click **NEXT** to go to the next step.
2. Use the **View adapter security** window to review information about the FICON Express adapters that are defined for the specified system.
   a. Review the FICON Express adapter information in the table.

      ID
      PCHID that is assigned to the FICON Express adapter

      Card type
      Type of FICON Express adapter

      Status
      Status of the FICON Express adapter

      Security capabilities
      One of the following security capabilities:

      Basic
      The hardware is not capable of making authenticated or encrypted connections.

      Authentication
      The hardware is capable of having authenticated connections.

      Encryption
      The hardware is capable of having both authenticated and encrypted connections.

   b. After reviewing the FICON Express adapter information, click **CLOSE** to close the **View adapter security** action and return to the main **Topology view**.

Manage PCI System Services

Accessing Manage PCI System Services task

To manage the PCI Resource Group:

1. Open the **Manage PCI System Services** task.

   The Manage PCI System Services window displays.

Manage PCI System Services

Use this window to manage the PCI Resource Groups to:

- Perform an activation of a PCI Resource Group that is not operating.
- Perform an update to a PCI Resource Group.

PCI system service table:

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Select
Indicates the PCI Resource Group selected.

Target
Indicates the PCI Resource Group.

Status
Indicates the current status of PCI Resource Group.

Partition Changes Pending Install and Activate
Indicates there are staged MCL updates which causes the Update Pending condition once an Install/Activate is performed for the selected PCI Resource Group. It is recommended to use the **Change Internal Code** task prior to updating the selected PCI Resource Group.

Note: This column displays for SERVICE mode only.

Update Pending
Indicates an update is pending for the selected PCI Resource Group. The selected PCI Resource Group must be operating.

The icons perform the following functions in the PCI Resource Group table:

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

PCHIDs defined table:

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

PCHID
Indicates the PCHID that is affected by a disruptive update to the selected PCI Resource Group.

State
Indicates the current state of the PCHID.

Status
Indicates the status of the PCHID.

Partition
Indicates the owning partition for this PCHID.

Partition Status
Indicates the current status of the owning partition.

The icons perform the following functions in the PCHIDs defined table:

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this downloaded CSV file into most spreadsheet applications.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Cancel
To exit the current task, click **Cancel**.

Help
To display help for the current window, click **Help**.

PCI Resource Group Update

This window displays all Online ID(s) and their associative partitions that will be affected during this PCI Resource Group disruptive update. It is recommended that you verify these ID(s) redundancy prior to performing the update. Use the **Configure On/Off** task to configure the Channel and Function ID (FIDs).

Channel and FIDs online table

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

ID
Indicates the ID that is affected by the PCI Resource Group disruptive update

State
Indicates the operational state of the ID

Status
Indicates the status of the ID

Type
Indicates the adapter type of ID

Partition
Indicates the owning partition of the ID

Partition Status
Indicates the current status of the owning partition

PCHID
Indicates the PCHID the ID is mapped to.

The icons perform the following functions for the FIDs Online table:

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this downloaded CSV file into most spreadsheet applications.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
The **Edit Sort** button is used to perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column

sorting can be performed by selecting the **^** in the column header to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Update Resource Group Firmware
To continue with the update resource group process, click **Update Resource Group Firmware**.

Cancel
To exit the current task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Manage Power Service State

Accessing the Manage Power Service State task

This task sets the power service status for either Power Distribution Units (PDUs) or Bulk Power Adapters (BPAs) for the selected systems.

To set the service status:

1. Select one or more systems.
2. Open the **Manage Power Service State** task. The Manage Power Service State window is displayed.
3. Select the option to enable or disable the power service state for either Power Distribution Units (PDUs) or Bulk Power Adapters (BPAs). You can disable the power service state to ensure that hardware errors are reported when the system's Power Distribution Units (PDUs) or Bulk Power Adapters (BPAs) lose power or you can select to enable power to a group of Power Distribution Units (PDUs) or Bulk Power Adapters (BPAs) to ensure that loss of power errors are not reported.
4. Click **Apply** to proceed with your selection, or click **Cancel** to exit this task.

Manage Power Service State

Use this window to set the power service state for system Power Distribution Units (PDUs) or Bulk Power Adapters (BPAs).

You can enable or disable the power service state for system PDUs or BPAs by selecting the following power service states:

Disabled
To ensure that hardware errors are reported when system PDUs or BPAs lose power, select **Disabled**.

Enabled for *xxx*
To enable power service state for this group of PDUs or BPAs to ensure that loss of power errors are not reported while maintenance is in progress, select **Enabled for *xxx***, where *xxx* identifies either the location of a BPA or the PDUs. As you make a selection, the location is highlighted in the diagram.

Enabled for *xxx*
To enable power service state for this group of PDUs or BPAs to ensure that loss of power errors are not reported while maintenance is in progress, select **Enabled for *xxx***, where *xxx* identifies either the location of a BPA or the PDUs. As you make a selection, the location is highlighted in the diagram.

Refer to the **GUIDANCE** section for more information.

Additional functions are available from this window:

CANCEL
To exit this window without making changes, click **CANCEL**.

APPLY
To proceed with the selection, click **APPLY**.

HELP
To display help for the current window, click **HELP**.

Manage Print Screen Files

Accessing the Manage Print Screen Files task

Note: If you access this task remotely you can only view or delete the print screen files that appear in the task window.

This task allows you to create screen captures of the entire contents of the console or of individual task windows. You can then manage these files by viewing, copying to media, or deleting.

To capture and manage the print screen files:

1. Open the **Manage Print Screen Files** task. The Manage Print Screen Files window is displayed.
2. Specify a file name and select a file type from the list that you prefer to have the screen capture saved as.
3. You can capture a window or screen by clicking one of the following options:

   Print Window
   Creates a copy of a task window and gives it a unique file name and the selected file type. A message window is displayed explaining how to get the preferred window to the foreground.

   Print Screen
   Creates a copy of the entire contents of the screen and gives it a unique file name and the file type you selected. A message window is displayed explaining the amount of time you have to arrange the windows on the screen before it is captured.

   Your screen capture is displayed in a table within the task window once the process is complete.
4. You can select a file from the table and then proceed with an option to view the file, copy the file to media, convert to a different file type, delete the file, or rename the file.
5. When you are done and ready to exit, click **Cancel**.

Manage Print Screen Files

Use this task to manage the console's print screen files.

This window lists the print screen files which currently exist on the console. If no files currently exist then the list will be empty.

You can select one or more files from the list, then click **View...**, **Copy...**, **Convert**, or **Delete** to perform that action on the selected file or files. If copying or converting a single file, you can specify a new file name as well.

You can select one file from the list, specify a new file name, then click **Rename** to rename the selected file.

To create new print screen files for the specified file name and file type, click **Print Window** or **Print Screen**. If a file name is not specified, a system generated file name will be used.

File name
To assign a file name for the print screen file, specify up to twenty alphanumeric characters. When creating a print screen file, if a file name is not specified a system generated name will be used. The file name can be specified when copying, converting, renaming or creating a print screen file.

Note: This option is not available when you are accessing the console remotely and no print screen files exist.

File type
To assign a file type of the print screen file, select the down arrow for a list of supported file types, then click on one of the file types in the list to select it.

Note: This option is not available when you are accessing the console remotely and no print screen files exist.

View...
To view one or more print screen files, select the files, then click **View...**. This displays the View Print Screen Files window.

Note: This option is not available if print screen files do not exist.

Copy...
To copy one or more print screen files to media, select the files, then click **Copy...**. The **Select Media Device** window is displayed where you can choose the media to which the files will be copied. If there is enough space available on the media, the files will be copied to that media. If files already exist on the media with the same file name as the selected files, the files on the media will be replaced with the selected files. If just one print screen file is selected, a file name can be specified to give the copied print screen file a new file name.

Note: This option is not available when you are accessing the console remotely or if no print screen files exist. On a remote session screen where files do exist, right click on the thumbnail to save it locally.

Convert
To convert one or more print screen files, select the files and select the file type, then click **Convert**. Selected print screen files which are already of the selected file type will be ignored. If just one print screen file is selected, a file name can be specified to give the converted print screen file a new file name.

Note: This option is not available if no print screen files exist.

Rename
To rename a print screen file, select the file, specify a new file name, then click **Rename**.

Note: This option is not available if no print screen files exist.

Delete
To remove one or more print screen files, select the files, then click **Delete**. You are prompted to confirm the delete to ensure the files are not deleted accidentally.

Note: This option is not available if no print screen files exist.

Print Window
To create a print screen file for a specific window, click **Print Window**. A message is displayed that explains how to use the Alt+Tab keyboard keys to get the window you want to come to the foreground. Then move the mouse cursor, which has changed to crosshairs, to any spot on that window and click on the window to create the print screen file. The list of files is updated to include the new print screen file.

Note: This option is not available when you are accessing the console remotely.

Print Screen
To create a print screen file for the entire screen, click **Print Screen**. A message is displayed that explains that you have a set amount of time to use the Alt+Tab keyboard keys to arrange the windows on the screen before the print screen file is created. The list of files is updated to include the new print screen file.

Note: This option is not available when you are accessing the console remotely.

Refresh
To refresh the list of print screen files, click **Refresh**. If you create print screen files using Alt+Print Screen or Shift+ Print Screen, then click **Refresh** to get the list of files updated. Shift+Print Screen prints the entire screen to a file, Alt+Print Screen selects a specific window to print to a file.

Note: You cannot use the Shift+Print Screen or Alt+Print Screen keyboard functions if you are accessing the console remotely.

OK
To save your changes, click **OK**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

View Print Screen Files

Use this window to view one or more print screen files. If more than one file is selected, the files are displayed in a tabbed format, with the file names displayed on the tabs. When large window or full screen files are displayed you may need to use the window scroll bars to navigate throughout the window.

Cancel
To close the view print screen files window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Media Device

Use this window to select the device to which the files will be copied.

OK
To continue the task with the selected media, click **OK**.

Refresh
To update the device list, click **Refresh**.

Cancel
To exit this window without making any changes and to return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Manage Processor Sharing

Accessing the Manage Processor Sharing task

Use the **Manage Processor Sharing** task to set weights, weight capping, and absolute capping for the partitions with shared processors on a Dynamic Partition Manager (DPM)-enabled system.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

To access the **Manage Processor Sharing** task:

1. Select a DPM-enabled system.
2. From the **Operational Customization** task group, open the **Manage Processor Sharing** task. This action opens the Manage Processor Sharing window.

Manage Processor Sharing

The **Manage Processor Sharing** task provides the controls through which you can set weights, weight capping, and absolute capping for partitions with shared processors on a specific Dynamic Partition

Manager (DPM)-enabled system. You can also use this task to define one or more groups of partitions to set absolute capping limits.

The main window of the **Manage Processor Sharing** task contains the following elements:

- The Processors table lists details about each partition and the partition cap group, if any, to which the partition belongs. If all of the partitions on the DPM system have the same processor type, the **Manage Processor Sharing** window displays one Processors table that lists details about all partitions. Otherwise, the **Manage Processor Sharing** window displays two tables:
  - The IFL Processors table lists details about each partition that has an IFL processor type.
  - The CP Processors table lists details about each partition that has a CP processor type. You might need to scroll down the main window to view the CP Processors table.

  Through the **Actions** menu on the Processor table, you can select the following menu items. All of these menu items are also available through the row menu when you right-click a table entry. A subset are also available through icons in the table toolbar.
  - **New Group**, through which you can define a new group of partitions, for the purpose of setting an absolute cap that limits the number of physical processors that active partitions in this group can use.
  - **Delete Group**, through which you can delete only one selected partition group.
  - **Add to Group**, through which you can add one or more partitions to the same partition group.
  - **Remove from Group**, through which you can remove one or more partitions from the same partition group.
  - **Group Details**, through which you can view information about only one selected partition group.
  - **Partition Details**, through which you can open the **Partition Details** task in a separate window. If you select more than one partition, a separate window is opened for each selected partition.

  For more details about the Processors table, see "Processors table" on page 991.
- To the right of each Processor table is an area in which you can display pie charts by selecting one or more partitions, or one or more partition groups, in the Processor table.
  - The Shared Processors pie chart shows the relative distribution of virtual processors for the selected partitions or groups in the Processors table.
  - The Processing Weights pie chart shows the relative distribution of weights for selected partitions or groups in the Processors table.

  For more details about the pie charts, see "Pie charts display" on page 994.
- Under the Processor table is a list of system processor properties for the DPM system. If the partitions on the DPM system have different processor types, the labels for these system properties include the processor type. For more details about the system processor properties, see "System processor properties display" on page 995.
- Under the system properties display is a link that opens the **System Details** task for the DPM system.

You can find more detailed help on the following elements of this window:

OK
To close the window, click **OK**. If you made changes in editable fields in the window, those changes are applied.

Apply
To apply changes you made in editable fields on the page, click **Apply**.If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to apply the changes or **Cancel** to return to the previous window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Processors table

The Processors table lists details about each partition on a specific DPM system, and also provides details about the partition group, if any, to which each partition belongs. Each partition can have only one defined processor type: either Central Processor (CP) or Integrated Facility for Linux (IFL), depending on the processor types that are installed on the system.

If all of the partitions on the DPM system have the same processor type, the **Manage Processor Sharing** window displays one Processors table that lists details about all partitions. Otherwise, the **Manage Processor Sharing** window displays two tables:

- The IFL Processors table lists details about each partition that has an IFL processor type.
- The CP Processors table lists details about each partition that has a CP processor type. You might need to scroll down the main window to view the CP Processors table.

In each table, partitions that do not belong to a group are listed before any table entries for a partition group. If a partition is a member of a group, its table entry is listed only under the group to which it belongs. By default, all group rows are expanded to show the table entry for each member partition.

The following topics describe the content, controls, and additional displays related to the Processors table.

- "The Processors table toolbar" on page 991
- "Columns in the Processors table" on page 993
- "Pie charts display" on page 994
- "System processor properties display" on page 995

The Processors table toolbar

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New Group
Opens the New Group window, through which you can define a new group of partitions, for the purpose of setting an absolute cap that limits the number of physical processors that active partitions in this group can use. If you selected any partitions in the Processors table, all of those selected partitions are added to the new group. The New Group function is not enabled if you have selected any partitions that are already members of a group.

The New Group window contains the following fields and controls. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Enter a unique name for the partition group.

Description
Enter a description for the partition group.

Absolute cap
Enter the maximum number of physical processors that active partitions in the group can use. Valid values range from 0.01 - 255.0, in increments of 0.01.

Short name
Enter the unique name by which the operating system can identify this partition group.

If you do not enter a value for this field, a unique short name is automatically generated after you click **Create** to create the new partition group.

Create
After you have supplied all of the required values, click **Create** to create the new partition group. The resulting table display shows the selected partitions listed under the newly created group.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Delete Group
Opens a confirmation window through which you can delete only one selected partition group. The Delete Group function is not enabled if you have selected more than one group, or have selected one or more partitions.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected group. The resulting Processors table display no longer contains a row for the deleted group, and the partitions that were members of the deleted group are listed in individual rows that precede any group rows.
- Click **Cancel** to return to the **Manage Processor Sharing** window without deleting the group.

Add to Group
Opens the Add to Group window, through which you can add one or more partitions to the same partition group. The Add to Group function is not enabled if you have selected any partitions that are already members of a group.

The Add to Group window contains the following fields and controls:

Group
From the Group list, select the partition group to which you want to add the selected partitions. To display the names of defined partition groups, click the arrow.

Add
After you have selected one partition group, click **Add** to add the selected partitions to this group. The resulting Processors table display shows an entry for each of the selected partitions under the table entry for the selected partition group.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Remove from Group
Opens a confirmation window through which you can remove one or more partitions from the same partition group. The Remove from Group function is not enabled unless the selected partitions all belong to the same group.

In the confirmation window, click **Remove** to confirm that you want to remove the selected partitions from the group, or click **Cancel** to return to the Manage Processor Sharing window without removing the partitions from the group.

Group Details
Opens the Group Details window, through which you can view information about only one selected partition group. The Group Details function is not enabled if you have selected more than one group, or have selected one or more partitions.

The Group Details window contains the following fields and controls. You can edit any of the values. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Specifies the unique name for the partition group.

Description
Specifies the user-supplied description, if any, of the partition group.

Absolute cap
Indicates the maximum number of physical processors that active partitions in the group can use. If you edit this value, enter a value from 0.01 - 255.0, in increments of 0.01.

Short name
Specifies the user-supplied or system-generated unique name by which the operating system can identify this partition group.

OK
To close the window, click **OK**. If you made changes in editable fields in the window, those changes are applied.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Partition Details
Opens the **Partition Details** task in a separate window. If you select more than one partition, a separate window is opened for each selected partition. The Partition Details function is not enabled if you have selected a partition group.

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions:

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Columns in the Processors table

The Processors table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a partition or a partition group. Partitions that do not belong to a group are listed before any table entries for a partition group. If a partition is a member of a group, its table entry is listed only under the group to which it belongs. By default, all group rows are expanded to show the table entry for each member partition.

- The name of each partition is a hyperlink through which you can open the **Partition Details** task.
- The name of each group is a hyperlink through which you can open the **Group Details** window.

Active
Indicates whether or not the partition is active. If the partition is active, a check mark is displayed in this column.

Number of Processors
Specifies the number of processors that are defined to the partition. The number of defined processors ranges from the minimum value of 1 to a maximum value of the total number of entitled processors on the system.

Weight
Indicates the relative amount of processor time that a specific active partition receives when it is in contention with other active partitions that share the same pool of processor resources. The suggested practice is to specify a processing weight that satisfies the peak workload requirements of the partition.

If you edit this value, enter an integer from 1 - 999. Integer values at the low end of the value range result in less relative processor time; integers at the higher end of the value range result in more relative processor time.

Weight Capping
Indicates whether weight capping is in effect for a specific partition. When weight capping is enabled, the partition cannot use more processor time than its weight, relative to other partitions that share the same pool of processor resources, even when additional processor resources are available.

A check mark in this column indicates that weight capping is enabled for a partition. To change the setting for weight capping, select or clear the check box in this column.

Absolute Capping
Indicates whether absolute capping is in effect for a specific partition or for a partition group. When absolute capping is enabled, an active partition, or active partitions in a group, cannot use any more than a specified number of physical processors. The switch in this column indicates whether absolute capping is enabled. If the switch is on, this column also contains the absolute capping value, which indicates the maximum number of physical processors that an active partition, or active partitions in a group, can use.

If you edit this value, enter a value from 0.01 - 255.0, in increments of 0.01. An absolute capping value is required for a partition group.

Description
Displays the user-provided description, if any, of the partition or partition group.

Pie charts display

To the right of each Processor table is an area in which you can display pie charts by selecting one or more partitions, or one or more partition groups, in the Processor table.

- The Shared Processors pie chart shows the relative distribution of virtual processors for the selected partitions or groups in the Processors table.
- The Processing Weights pie chart shows the relative distribution of weights for selected partitions or groups in the Processors table.

To the right of each pie chart, a color legend identifies each of the selected partitions by name. If you selected a partition group in the table, the legend lists partitions in the group individually, and the pie chart contains one wedge for each partition in the group.

To view details for a specific partition in a pie chart, hover your cursor over the pie wedge with the same color as shown in the legend, next to the partition name. The pie wedge is slightly enlarged and a tooltip displays details for the partition.

- For a wedge in the Shared Processors pie chart, the tooltip displays the partition name, the number of processors for that partition, and its relative percentage of the total shared partitions, rounded to two decimal places.

- For a wedge in the Processing Weights pie chart, the tooltip displays the partition name, its weight value, and its relative percentage of the total processing weight, rounded to two decimal places.

System processor properties display

Under the Processor table is a list of system processor properties for the DPM system. If the partitions on the DPM system have different processor types, the labels for these system properties include the processor type.

- If all partitions on the system have the same processor type, the following system properties are displayed.

  Active virtual processors
  This value is the number of processors that are assigned to active partitions.

  Shared physical processors
  This value is the size of the shared processor pool for the DPM system. This value reflects the total number of entitled processors for the system minus the number of dedicated processors, if any.

  Virtual/Physical
  This percentage value is the ratio of the number of virtual processors on active partitions to the number of entitled, shared physical processors for the DPM system.
- If one or more partitions have a different processor type, the same system properties are displayed in a set for each type, with each set under its corresponding table: IFL Processors or CP Processors. The property labels indicate the processor type, as shown in the following lists.

  For the IFL Processors table

  Shared virtual IFL processors
  Shared physical IFL processors
  Virtual/Physical IFLs

  For the CP Processors table

  Shared virtual CP processors
  Shared physical CP processors
  Virtual/Physical CPs

Manage Product Engineering Access Control File

Accessing the Manage Product Engineering Access Control File task

This task is used by a service representative or a user that has service representative task roles access. Use this task to import an access control file which allows product engineering access to this console.

1. Open the **Manage Product Engineering Access Control File** task. The Manage Product Engineering Access Control File window is displayed.
2. Select the location of the access control file you want to import.

   Note: The options for importing the access control file depend upon how you are accessing the console.
3. Click **IMPORT** to import the specified access control file.

Manage Product Engineering Access Control File

Use this window to specify the location of the access control file.

If you are accessing this task locally on the console, select the location of the access control file from an FTP server or from removable media.

If you are accessing the console remotely, select the location of the access control file from an FTP server or from a remote file system.

FTP server
To select a file from an FTP sever, select **FTP server**. Provide the following information if you are providing an access control file from an FTP server.

Host name:
Specify the host name address or destination. This is a required field.

User name:
Specify the user name for the target FTP destination. This is a required field.

Password:
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol:

Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)
- **SFTP** (SSH File Transfer Protocol)

Removable media
To import the access control file from a USB flash memory drive, select **Removable media**. To see a list of the available USB flash memory drives, use the drop-down and then select the USB flash memory drive for importing the access control file. To make sure you have the currently available USB flash memory drives, click **Refresh**. This option is only available when this task is accessed locally on the console.

Note: If you're using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

File system
To select the access control file from a remote file system, select **File system**.

Note: This option is only available if you are accessing the console remotely.

Control file:
Specify the file name of the access control file or click **BROWSE** to select the access control file that you want to import.

CANCEL
To close this window and end the task without importing an access control file, click **CANCEL**.

IMPORT
To import the selected access control file, click **IMPORT**.

HELP
To display help for the current window, click **HELP**.

Manage Remote Connections

Accessing the Manage Remote Connections task

Note: The Hardware Management Console's call-home server service must be enabled for you to use this task.

This task allows you to view or manage remote connections. The Hardware Management Console manages remote connections automatically. It puts requests on a queue and processes them in the order in which they are received. However, this task allows you to manage the queue manually, if necessary. You can stop transmissions, move priority requests ahead of others, or delete requests.

To manage remote connections:

1. Open the **Manage Remote Connections** task. The Manage Remote Connections window is displayed.
2. This window lists active requests (being transmitted) and those that are waiting. You can select requests in the lists. You can display options by clicking **Options** on the menu bar. The options permit you to:
   - Prioritize a selected request (move it to the top of the queue)
   - Cancel selected requests
   - Cancel all active requests (those being transmitted)
   - Cancel all waiting requests
   - Hold the queue (puts queue on hold after completing current active request)
   - Release the queue
   - Close the window and exit.
3. Select **Options** (from the menu bar), **Exit** when you have completed the task.

Manage Remote Connections

If the Hardware Management Console's call-home server service is enabled, use this window to manually manage the console's remote connections.

The console manages its remote connections automatically. It puts requests on a queue and processes them in the order in which they are received. But you can use this window to manage the queue manually, if necessary, to stop transmissions, move priority requests ahead of others, or delete requests.

Review the window's console information and transmission information, then make selections from Options menu bar to manage the console's remote connection requests.

To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Options

Prioritize Selected Request
Select a connection request from the **Waiting Requests** list, then select **Prioritize Selected Request** to move it to the top of the queue. Moving the selected request to the top of the queue makes it the next to be processed.

Cancel Selected Requests
Select a connection request from the **Waiting Requests** list, then select **Cancel Selected Requests** to remove it from the queue.

Cancel All Active Requests
To attempt to cancel all current connection requests, if any, shown in the **Transmitting Requests** list, select **Cancel All Active Requests**. After the current request is canceled successfully, the console begins processing the next request in the queue.

Cancel All Waiting Requests
To cancel all connection requests in the **Waiting requests** list, select **Cancel All Waiting Requests**.

Hold the Queue
To put the queue on hold after completing the current request being performed, if any, select **Hold the Queue**. The active request will be allowed to complete, but no other request will become active until **Release the Queue** is selected.

Release the Queue
To release the queue from hold status and make it active again, select **Release the Queue**.

Exit
To close this window and return to Hardware Management Console workplace, select **Exit**.

Queue Status

Indicates whether the remote connection services queue is active or on hold. The console queues and processes transmission requests while the queue is active. The console only queues connection requests while the queue is on hold.

Select **Hold the Queue** and **Release the Queue** from **Options** to change the queue state.

Transmitting Requests

Transmitting Requests lists information about the current requests being processed, if any. It displays the following information about the requests:

System
Identifies the central processor complex or Hardware Management Console that requested the connection.

Priority
Displays the priority that is associated with the request.

Date
Displays the date the request was originated.

Time
Displays the time the request was originated.

Description
Displays a brief description of the request.

Waiting Requests

Waiting Requests lists the transmission requests currently in the console's remote connection services queue. It displays the following information about the transmission requests:

System
Identifies the central processor complex or Hardware Management Console that requested the transmission.

Priority
Displays the priority that is associated with a transmission request currently in the queue. The priority value is used by the console when making queuing decisions with multiple requests.

Date
Displays the date the request was originated.

Time
Displays the time the request was originated.

Description
Displays a brief description of the request.

Manage Remote Support Requests

Accessing the Manage Remote Support Requests task

This task views or manages call-home requests that the console has submitted.

1. Open the **Manage Remote Support Requests** task. The Manage Remote Support Facility Requests window is displayed.
2. This window lists active requests (being transmitted) and waiting requests. You can select requests in the lists. You can display options by clicking **Options** on the menu bar. The options permit you to:
   - View all Hardware Management Consoles that are configured as call-home servers for this console
   - Cancel selected requests
   - Cancel all active requests (those being transmitted)
   - Cancel all waiting requests

- Close the window and exit.

3. Select **Options** (from the menu bar), **Exit** when you have completed the task.

Manage Remote Support Facility Requests

Use this window to view or manage call-home requests submitted by the console that are either being processed or waiting to be processed.

Click **Options** on the menu bar to:

- **"View All Call-Home Servers" on page 1000** to view a list of all consoles that are configured as call-home servers for this console.
- **Cancel Selected Requests** to remove the selected request from the list.
- **Cancel All Active Requests** to cancel all requests in the Active Requests list.
- **Cancel All Waiting Requests** to cancel all requests in the Waiting Requests list.
- **Exit** to close this window and return to the console workplace.

Click **Help** on the menu bar to display help for the current window.

Active Requests

The Active Requests table provides the following information about call-home requests being processed:

Status
The status of a request that is being processed can be:

Submitted
This request has been accepted and processing for it is being arranged (on either this machine or another machine).

Handling
The request is being processed.

Canceling
Someone has canceled this request.

Reporting
The result of the request is reported back through the programming interface to the submitter.

Call-Home Server
The actual machine where the call-home request is being processed. A call-home server is a console that provides internet connectivity to request service or transmit hardware serviceability data to the support system.

Date
The date the call-home request was submitted.

Time
The time the call-home request was submitted.

Description
A brief description of the request from the programming interface through which it was submitted.

Waiting Requests

The Waiting Requests table provides the following information about call-home requests waiting for processing:

Date
The date the call-home request was submitted.

Time
The time the call-home request was submitted.

Description
A brief description of the request from the programming interface through which it was submitted.

View All Call-Home Servers

Use this window to view a list of all consoles that are configured as Call-Home Servers for this console.

Manage SSH Keys

Accessing the Manage SSH Keys task

This task allows you to install the public key for a host used for secure transfers. It associates a public key with a host address and allows a secure FTP connection from a Hardware Management Console FTP client to an FTP server location.

To manage the SSH keys:

1. Open the **Manage SSH Keys** task. The Manage SSH Keys window is displayed.
2. Specify an IP address that you want associated with a secure host key, then click **Add**. This IP address and its corresponding key is displayed in the **Known Host Keys** table.
3. You can select an existing IP address from the table, then click **Delete** to remove it.
4. When you are done with this task, click **Close**.

Manage SSH Keys

Use this task to associate a public key with a host address. You can add a public key or manage the ones that are existing. This task allows a secure FTP connection from a Hardware Management Console FTP client to an FTP server location.

You can work with the table by using the table icon or the **Select Action** list from the table toolbar. If you place your cursor over the icon, the icon description appears. The toolbar performs the following functions:

Configure Columns
Selects the columns that you want displayed. Arrange the columns in the table in the order you want or hide certain columns from view. All available columns are listed in the Columns list by their column name. Select the columns that you want displayed or hidden by selecting or clearing the items in the list and by using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified.

Following are descriptions for the columns that are displayed in the **Known Host Keys** table:

Select
Use this column to make selections. No rows are selected when the table is first displayed. You can select any number of rows.

IP Address
Specifies the IP address that is associated with the secure host key.

Key Type
Specifies the SSH key type. The accepted SSH key types include the following:

- ECDSA
- ED25519
- RSA

Key Fingerprint
Specifies the secure host key that is associated with the IP address.

The following functions are also available from this window.

Delete
To remove the selected host from the Known Host Keys table, click **Delete**.

Address
Specify the IP address of the host to retrieve the public key. A port can be specified along with the IP address by separating it with a colon (for example, '192.168.1.4:1234'). If a port must be specified for an IPv6 address, the address must be enclosed in square brackets (for example, '[2002:93c:ffb:1:210:18ff:fe15:12b8]:11234')

Add
To add a new host key to the Known Host Keys table, click **Add**.

Close
To end the task when you have finished working in it, click **Close**.

Help
To display help for the current window, click **Help**.

Manage Syslog Servers

Accessing the Manage Syslog Servers task

Use this task to manage the syslog servers to which syslog messages will be sent. This task displays the syslog servers that are set up to receive syslog messages over TCP for logs, events, and messages from the Hardware Management Console (HMC) and managed systems that support the remote syslog capability. Each server includes a name, if it is enabled for logging, if it requires a secure SSL connection, a hostname or IP address, a port, and a description.

To set up a server for it to receive logs, events, and messages from the HMC and systems:

1. Open the **Manage Syslog Servers** task. The Manage Syslog Servers window is displayed.
2. Click **ADD SERVER**. The Add Syslog Server window is displayed.
3. Provide the required input: Name the server, provide the hostname or IP address, port, and select whether logging is enabled and whether a secure SSL connection is required.
4. Select the logs, events, or messages that you want to send to the server from each system or HMC.
5. When you have completed your input and selections, click **SAVE**.
6. Now the server is set up to receive the selected logs, events, or messages.

Manage Syslog Servers

Use this task for managing the syslog servers to which syslog data will be sent. This window displays the syslog servers that are set up to receive syslog messages over TCP for logs, events, and messages from the Hardware Management Console (HMC) and managed systems that support the remote syslog capability. Each server includes name, if it is enabled for logging, if it requires a secure SSL connection, hostname or IP address, port, and description.

ADD SERVER
To add a server for the syslog data to be sent to, click **ADD SERVER**. The Add Syslog Server window is displayed. Provide the following information in the input area for each server.

Name
Specify a name. This field is required.

Description
Provide a description.

Hostname or IP
Specify the hostname or IP address. This field is required.

Port
Specify a port. This field is required.

Logging enabled
If you want logging enabled for this server, then select **Logging enabled**. A checkmark is displayed if you want logging enabled. The Manage Syslog Servers table displays **Yes** if logging is enabled and **No** if logging is not enabled.

Connect with SSL
If you require a secure SSL connection between the HMCs and the syslog servers, then select **Connect with SSL**. A checkmark is displayed if you require a secure SSL connection. The Manage Syslog Servers table displays **Yes** for a secure SSL connection and **No** if a secure SSL connection.

Note: If this option is selected, the HMC attempts to make SSL TLS secured connections with the syslog server. If the option is selected and such a secured connection cannot be made for any reason, then no connection is made to the server. For such a secured connection to work, the server's trusted signing certificate must be imported to the HMC using the Manage Trusted Signing Certificates option on the Advanced menu in the **Certificate Management** task. Also, Support Elements (SE) that are connecting to a syslog server do not do so directly, but rather through a managing HMC. Therefore, the trusted signing certificate is required on the HMC both for connecting on the HMCs own behalf, and for connecting on behalf of any managed SEs.

For each system or HMC, select the type of logs, events, and audit information that you want sent to the server.

- Audit logs
- Security logs
- Event logs
- Hardware Messages
- WS API Requests
- BCPii Logs

When you are done adding the server, click **SAVE** to proceed or **CANCEL** to return to the task window.

EDIT SERVER
To change the values of an existing server, select the server, then click **EDIT SERVER**. Make the appropriate changes, then click **SAVE** to proceed or **CANCEL** to return to the task window.

REMOVE SERVER
To remove a server from the list, select the server, then click **REMOVE SERVER**. A message appears alerting you that the server will be removed and that the corresponding event logging settings will be removed. You can click **REMOVE** to proceed or you can click **CANCEL** to return to the task window.

CLOSE
To close the window and exit this task, click **CLOSE**.

HELP
To display help for the current window, click **HELP**.

Manage System Time

Accessing the Manage System Time task

The **Manage System Time** task guides you through the process of viewing or setting up time synchronization for a server that uses the Server Time Protocol (STP).

Note: Depending on your user task role, you may only be able to view this task.

You can access this task from the main Hardware Management Console (HMC) page by selecting the Systems Management node, by selecting a specific system, or by selecting the task in the Tasks index. You can use either the default SYSPROG user ID or a user ID that a system administrator has authorized to this task through customization controls in the **User Management** task.

Note: Manage System Time is considered a disruptive task. If the object is locked, you must unlock it before continuing.

Manage System Time

Use the **Manage System Time** task to view or set up time synchronization for a server that uses the Server Time Protocol (STP).

Note: Depending on your user task role, you may only be able to view this task.

Server Time Protocol is a time synchronization architecture that is designed to provide the capability for multiple servers to maintain time synchronization with each other and to form a Coordinated Timing Network (CTN). STP is a message-based protocol that allows timekeeping information to be sent between servers and Coupling Facilities over:

- InfiniBand (IFB) Type CIB (HCA3-O (Host Channel Adapter3-optical)) or HCA3-O LR (Long Reach) links (IBM z13® or IBM z14® only)
- InfiniBand (IFB) Type CS5 (ICA SR (Integrated Coupling Adapter Short Reach)) links (IBM z13® or IBM z14 only)
- Coupling Express Long Reach (CE LR), channel type CL5 links (IBM z13®, IBM z13s®, or IBM z14 only).

The main window of the **Manage System Time** task includes the following elements.

- The **Global CTN details** area, for specifying a Coordinated Timing Network (CTN) to work with and for getting details about the servers and systems in the CTN.
- A graphical **topology view**, to help understand the elements and structure of the specified CTN.
- The **topology toolbar**, which provides tools for viewing and setting up time synchronization for the specified CTN's Current® Time Server (CTS).
- The **STP Actions** area, for choosing actions to perform against the specified CTN.

The **Manage System Time** task also includes a built-in dictionary, which provides definitions for select terms that are used in its windows. Click (select) any term that is displayed with a blue dotted line beneath it to see its definition.

The **Export CTN data** STP action provides the ability to export information about the current CTN to a Microsoft Excel spreadsheet. The resulting .xsl file can be downloaded and used with a screen reader for enhanced accessibility. For information about exporting CTN data to a file, see the help topic “Export CTN data” on page 1040.

For more information about the elements of the **Manage System Time** main window, use the following links.

Topology view

Use the **Topology view** of the **Manage System Time** window to understand the topology for a Coordinated Timing Network (CTN). The **Topology view** displays the various elements of the CTN's topology. It shows the External Time Sources (ETS), the servers and systems, and the links between them.

For more information, use the following links.

Understand the hierarchical structure of the topology

The topology view displays the CTN's elements in *stratums*. The stratum level indicates the hierarchy of an element within the CTN. Stratum 1 is the highest stratum, while Stratum 4 is the lowest (Stratum 3 for IBM z/13 and earlier). A stratum level of 0 indicates that the server has no time source. A stratum level of 2, 3, or 4 indicates that the server is respectively 1, 2, or 3 hops away from Stratum 1.

The External Time Sources always sit above the highest stratum (Stratum 1). The Current Time Server (CTS) is always in Stratum 1. Servers, which have special roles, occupy Stratum 1 (the CTS) and Stratum 2. (However, in some rare situations, a roled Stratum 1 or Stratum 2 server can become a Stratum 3 server). Other non-roled systems occupy Stratum 2 or the lower stratums. The Preferred Time Server (PTS) and the Backup Time Server (BTS), which are roled servers, will also be the Current Time Server.

If the CTN has systems that occupy the lower stratums, including Stratum 0, they might not be immediately visible in the topology. Depending on the size and makeup of your topology, only the External

Time Source and the higher stratums might be visible; Stratum 0 could be completely hidden, or a lower stratum could be only partially visible. In this situation, click (select) the down arrow at the bottom edge of topology view, or manually scroll down to see the hidden elements of the topology.

Get information about the servers and systems in the CTN's topology

Each server and system is represented by its own rectangle in the topology display. To get more details about a server or system in the topology, do the following.

Note: These instructions do not pertain to the External Time Source (ETS). To get more information about the ETS, see "Get information about the CTN's External Time Sources" on page 1007.

- Hover over a server or system's rectangle in the topology display. The server or system, and all of its connections to other elements in the topology are highlighted.
- Click (select) the server or system. The **STP Status** window opens, which provides information about the following.

  Server role
  Specifies the role that the server plays in the topology. The roles are as follows.

  – PTS: Preferred Time Server
  – BTS: Backup Time Server
  – ARB: Arbiter
  – CTS: Current Time Server

  For more information about server roles, see "Determine the servers that have roles in the CTN" on page 1006.

  This field applies to systems with roles (servers) only. For systems that do not have roles, this field is empty.

  Timing state
  Indicates the timing state in which the server or system is operating. If it has a value of anything other than **Synchronized**, then the server or system is not actively participating in a CTN. The possible **Timing state** values are **Unsynchronized**, **Synchronized**, or **Stopped**.

  Usable clock source
  Indicates whether a usable STP clock source is available to synchronize the server time of day (TOD). This value can be either **Yes** or **No**.

  Maximum timing stratum level
  Specifies a number that indicates how far a server can be from the Current Time Server and still be in a synchronized state. If the maximum timing stratum level is 3 (three), a server can be two hops away.

  Maximum STP version
  Specifies a number that indicates the maximum level of STP facility code that is supported by this server.

  See local uninitialized STP links

  Number of local uninitialized STP links.

  Click **See local uninitialized STP links** to display the **Local Uninitialized STP Links** window, which provides a table of information about the server or system's coupling links that can be used to exchange STP messages with other servers. If there are no uninitialized STP links, **There are no local uninitialized STP links** appears as a field name only (it is not an active link). The table shows the **Local STP Link ID** (PCHID address), the **STP Link Type**, and the reason why the link is uninitialized (**Reason code sent** and **Reason code received**). All links in the table are in an uninitialized state.

  The possible reason codes are:

  Allowable paths exceeded
  Greater than 512 STP paths are being activated. Contact next level of support.

Busy
A busy condition or resource contention was detected. This should be a temporary condition. Contact next level of support if the condition persists.

CF response
The attached server does not support STP.

Communication error
A communication timeout is recognized for the attached server, which indicates that the attached server stopped sending STP timing information.

Configuration error
This server detected a different CTN ID on the attached server. The CTN ID must match the CTN ID of this server to be a member of the same STP-only CTN.

Disagree on CTN members allowed
This server disagrees with the attached server about which servers are allowed to participate in the STP-only CTN. One or both servers might have specified which servers are allowed to participate in the CTN.

Fenced
The link is operational, but it is in a fenced state and cannot be initialized for STP communication. Remove the link from the fenced state.

Initialization is not complete
The physical link is operational, but link initialization has not been attempted or is in progress. This might be a temporary condition.

Invalid operation parameters
An invalid STP command was sent. Contact next level of support.

Link failure
A link failure is detected on the physical link. Determine the reason for the failure or contact next level of support.

Network configuration error
This server and the attached server do not have the same network configuration. They might have the same servers configured, but disagree on who is the Current Time Server. Verify the configuration at each server to determine why they disagree. Contact next level of support if the condition persists.

Node descriptor error
The node descriptor on the physical link is not valid.

No response
An attempt was made to communicate with the attached server, but it did not respond within the allowed time. Verify the links. Contact next level of support if the condition persists.

Not allowed to join CTN
The attached server is not allowed to join the same STP-only CTN as this server. This server might have specified which servers are allowed to participate in the CTN.

Offline
The physical link is in the offline state on this server. Configure the link online.

Removed path
The attached server sent a command to remove the STP path. This might be a temporary condition. Contact next level of support if the condition persists.

Self-coupled server
The link is attached from this server to itself.

STP is not enabled
The attached server does not have the STP feature enabled. STP communication with the server is not possible.

Takeover active state
The Current Time Server is being reassigned. This might be the result of a recovery action. Verify the status of the Preferred Time Server and Backup Time Server. This condition should be temporary. Contact next level of support if the condition persists.

Unsupported version (min=x, max=y)
The attached server is running with an STP version that is incompatible with this server's STP version. The minimum and maximum STP version is identified.

ASSUME CTS
If a system that is not the Current Time Server (the PTS or the BTS) needs to take over as the Current Time Server (CTS), the **ASSUME CTS** option is displayed in the **STP Status** window.

Console-assisted recovery uses the HMC in an attempt to determine the status of the PTS (when initiated by the BTS) or the status of the BTS (when initiated by the PTS). Console-assisted recovery helps to determine whether the BTS can take over as CTS, or the PTS can take back its role as the CTS.

When STP configuration cannot be restored through console-assisted recovery from either the PTS or BTS, an outage for both servers can occur until link path connectivity is re-established between the two servers. In this situation, if the status of the servers can be determined manually, you can force one of the servers to assume the CTS role without permanently reconfiguring the CTN.

To force the specified server (PTS or BTS) to assume the CTS role, do the following.

1. Verify that there is no system functioning as the Current Time Server for the CTN.
2. Click **ASSUME CTS**.
3. In the "Assume Current Time Server confirmation" window, click **CONTINUE**.
4. Read the conditions and options that are presented to you in the "Assume Current Time Server confirmation" window carefully. If you are certain that you want this system to assume the role of CTS, click **YES**. Otherwise, click **NO**.

Note: When a system is added or removed from a CTN, or its role in the CTN changes, the topology in the main window is automatically refreshed.

Determine the servers that have roles in the CTN

Throughout the help for the **Manage System Time** task, the systems that have special roles are referred to as **servers**. These servers are also marked with one of the following labels, which identifies their roles.

"CTS" (Current Time Server)
Server that is the active stratum 1 server for the CTN. In most cases, the Current Time Server is also the Preferred Time Server.

Note: There can be only one active stratum 1 server in an STP-only CTN, and only the Preferred Time Server or the Backup Time Server can be assigned to be the active stratum 1 server.

"PTS" (Preferred Time Server)
Server that has preference to be the stratum 1 server of an STP-only CTN. In most cases, the Preferred Time Server is also the Current Time Server. The PTS must have connectivity to the Backup Time Server and the Arbiter, as well as to all servers that are planned to be stratum 2 servers. The connectivity can be:

- InfiniBand (IFB) Type CIB (HCA3-O (Host Channel Adapter3-optical)) or HCA3-O LR (Long Reach) links (IBM z13® or IBM z14 only)
- InfiniBand (IFB) Type CS5 (ICA SR (Integrated Coupling Adapter Short Reach)) links (IBM z13® or IBM z14 only)
- Coupling Express Long Reach (CE LR), channel type CL5 links (IBM z13®, IBM z13s®, or IBM z14 only).

"BTS" (Backup Time Server)
The BTS is optional, but strongly recommended. For CTNs that contain two or more systems, the BTS is assigned to take over as the stratum 1 server if the PTS fails. A BTS (or Arbiter) cannot be assigned for CTNs that contain only one server.

The Backup Time Server is a stratum 2 server that must have connectivity to the Preferred Time Server and the Arbiter (if one is configured), as well as to all other stratum 2 servers that are connected to the Preferred Time Server.

Note: Running without a Backup Time Server is not advisable because the Preferred Time Server becomes a single point of failure in the CTN.

"ARB" (Arbiter)
Optional server that provides additional means for the Backup Time Server to determine whether it should take over as the Current Time Server when unplanned events affect the CTN. The Arbiter is a stratum 2 server that must have connectivity to both the PTS and the BTS.

Note: Although it is optional, if a CTN contains three or more systems, including an Arbiter is strongly recommended to increase the reliability of the CTN.

Systems that do not have special roles in the CTN are referred to as *systems* throughout the **Manage System Time** help.

Get information about the CTN's External Time Sources

Each External Time Source (ETS), if one is configured, is represented by its own rectangle in the topology display.

Get details about the External Time Source status

To get more details about an External Time Source (ETS), click (select) its rectangle in the topology view. The **ETS Status** window opens and provides the following information.

If the ETS is an NTP server, the **ETS status** window contains the following information:

Stratum
Indicates the NTP stratum in which the ETS is operating.

Note: The NTP stratum level is independent of the STP stratum level. Although both NTP and STP use the term *stratum*, there is no direct relationship between them.

Source
Indicates the NTP clock source for the ETS.

If the ETS is a PTP interface, the **ETS status** window contains the following information:

Grandmaster ID
Indicates the identifier of the grandmaster, which is a derivative of the MAC address.

To close the ETS Status window, click **x** or anywhere outside the status window.

Get details about the External Time Source links

Hover over the link between the ETS and the Preferred Time Server (PTS) or Backup Time Server (BTS) to highlight that link and the server to which it is connected. To see details about the connection between the two systems, click the information icon (lowercase I in a blue circle), which is displayed over the highlighted link. The "Active connection details" window is displayed.

The "Active connection details" window contains different information, depending on whether the ETS is a PTP or NTP server.

If the ETS is a PTP interface, the "Active connection details" window contains the following information:

Ethernet interface
Preferred Ethernet interface that was chosen when PTP was configured.

Grandmaster ID
Identifier of the grandmaster, which is a derivative of the MAC address.

Pulse per second (PPS) status
PPS status for ETS type of **PTP with PPS** (pulse per second). Possible values are **Detected** and **Not detected**. This field is not displayed when the ETS type is **PTP**.

Port *port_number* status
Status for the active port (Port 0 or Port 1) for ETS type of **PTP with PPS** (pulse per second). This field is not displayed when the ETS type is **PTP**.

For a list of the possible port status messages that can be displayed for this field, refer to "Port status messages" on page 1008.

If the ETS is an NTP server, the "Active connection details" window contains the following information:

Address
Ethernet address of the ETS (NTP) server.

ETS type
Type of ETS, which can be **NTP** or **NTP with PPS** (pulse per second).

Pulse per second (PPS) status
PPS status for ETS type of **NTP with PPS**. Possible values are **Detected** and **Not detected**. This field is not displayed when the ETS type is **NTP**.

Port *port_number* status
Status for the active port (Port 0 or Port 1) for ETS type of **NTP with PPS**. This field is not displayed when the ETS type is **NTP**.

For a list of the possible port status messages that can be displayed for this field, refer to "Port status messages" on page 1008.

To close the "Active connection details" window, click **x**.

Port status messages

Not configured

Message:
Not configured

Explanation:
The PPS port has not been configured to receive pulse per second signals from an NTP time server.

Action:
Use the **Configure External Time Source** STP action to configure the PPS port.

Not configured, no PPS signal detected

Message:
Not configured, no PPS signal detected

Explanation:
The PPS port has not been configured to receive pulse per second signals from an NTP time server. PPS signals are not being received at the PPS input port of the server at this time.

Action:
Determine why PPS signals are not detected. Use the **Configure External Time Source** STP action to configure the PPS port.

Not configured, PPS signal detected

Message:
Not configured, PPS signal detected

Explanation:
The PPS port has not been configured to receive pulse per second signals from an NTP time server. PPS signals are being received at the PPS input port of the server at this time. This indicates the PPS signal will be available when the PPS port is configured for use.

Action:
Use the **Configure External Time Source** STP action to configure the PPS port.

No PPS signal detected

Message:
No PPS signal detected

Explanation:
The PPS port is configured to receive pulse per second signals from an NTP time server, but PPS signals are not being received at the PPS input port of the server.

Action:
Verify that the cable is attached from the PPS output port on the NTP time server (that was specified in the **Configure External Time Source** STP action) to the PPS input port of the server. PPS signals cannot be received if the cable is not attached at both ends. If the cable is attached, verify that the connections are solid or you can try a new cable to ensure that there is not a problem with the cable. If the status still shows **No PPS signal detected**, verify that the External Time Server hardware is powered on and has a functioning PPS output port, and that any necessary configuration required to use PPS has been completed. Contact the vendor of the NTP time server for more information.

Acquiring consistent NTP information

Message:
Acquiring consistent NTP information

Explanation:
The PPS port is receiving pulse per second signals from an NTP time server assigned to the port. However, in order to determine the correct time, NTP information is also required from the NTP time server that is assigned to the port. The NTP information was not received or the NTP information received for this port is inconsistent with the information received for the port whose status is **Tracking to PPS signal**. In order for this port to have a status of **Capable of tracking to PPS signal**, valid NTP information must be continuously received.

Action:
This status might be the result of problems contacting the NTP time server from the NTP client on the support element. Use the **Configure External Time Source** STP action to verify the status of the NTP time server. After selecting the NTP server and specifying the External Time Source (**NTP with PPS**), the connectivity of the specified NTP server is automatically tested. The result of the test is displayed under **Connection status** in the "Verify Network Time Protocol servers" window. If the status is **Error**, click the caret to expand the explanation and then follow the suggested action that is provided there. If the status of the NTP time server is **No errors**, use the **View Console Events** task to determine if there are inconsistencies between this port and the port that is **Tracking to PPS signal**. The inconsistency might be logged as either of the following:

PPS port [0/1] offset differs by more than the amount allowed from the PPS port that is **Tracking to PPS signal**.

Or

PPS port [0/1] offset on the backup system differs by more than the amount allowed from the PPS port that is **Tracking to PPS signal**.

Configuration error

Message:
Configuration error

Explanation:
The PPS port is receiving pulse per second signals from an NTP time server, but the PPS information disagrees with the NTP information from the NTP time server that is assigned to that port. The STP facility is not capable of tracking to the PPS signal until the NTP information agrees with the PPS information.

Action:
For any PPS port reporting this status, verify that the NTP time server that was assigned to the port in the **Configure External Time Source** STP action is correct and configured. Verify that the cable is attached from the PPS output port on the specified NTP time server to the PPS input port of the server. If both PPS ports are reporting **Configuration error**, the cables are most likely swapped. If only one PPS port is configured and it is reporting **Configuration error**, the cable might be attached to the wrong NTP time server.

Note: A configured PPS port cannot be assigned to a Hardware Management Console NTP time server because there is no PPS output on the Hardware Management Console.

Adjusting for PPS signal

Message:
Adjusting for PPS signal

Explanation:
The PPS port is receiving pulse per second signals from the NTP time server that is assigned to the port, but a time offset needs to be steered out before the port has a status of **Tracking to PPS signal** or **Capable of tracking to PPS signal**. The CTN time source is **NTP**, **NTP (Preferred Time Server)**, or **NTP (Backup Time Server)** until the offset is steered out.

Action:
No action required. When the offset has been steered out, the status of the port is **Tracking to PPS signal** or **Capable of tracking to PPS signal**.

Capable of tracking to PPS signal

Message:
Capable of tracking to PPS signal

Explanation:
The PPS port is receiving pulse per second signals from the NTP time server that is assigned to the port and is capable of providing redundancy of an External Time Source. In the event that the PPS port that is currently **Tracking to PPS signal** is no longer usable, this port can be used to provide highly accurate adjustments to the Coordinated Server Time for the STP-only Coordinated Timing Network (CTN).

Action:
No action required. The port will be used, if necessary. However, if you want this PPS port to be used to provide highly accurate adjustments to the Coordinated Server Time for the STP-only Coordinated Timing Network (CTN), use the **Configure External Time Source** STP action to select it.

Tracking to PPS signal

Message:
Tracking to PPS signal

Explanation:
Pulse per second (PPS) signals from this PPS port are being used to provide highly accurate adjustments to the Coordinated Server Time for the STP-only Coordinated Timing Network (CTN).

Action:
No action required.

Fenced

Message:
Fenced

Explanation:
The PPS port is fenced by Licensed Internal Code.

Action:
After fixing the problem that caused the PPS port to become fenced, the PPS port needs to be reset. Attempt to reset the PPS port by doing one of the following:

1. Use the **Control Pulse Per Second signal** STP Diagnostic action to reset the port. Deselect the **Fenced by Licensed Internal Code** option to enable the port to receive PPS signals from an External Time Source.

   Note: The **Control Pulse Per Second signal** STP action can be used only by support system personnel.
2. Otherwise, if the port is not configured, use the **Configure External Time Source** STP action to configure it.
3. If the PPS port is configured, use the **Configure External Time Source** STP action to disable it. In the **Verify NTP** step, click the **Enabled** icon (switch) for this port until it is in the disabled position. Then, after the port is disabled, use the **Configure External Time Source** action to reconfigure it.

If the PPS port returns to **Fenced** after performing one of the above actions, contact next level of support.

Test

Message:
Test

Explanation:
An internal diagnostic test can be performed using the **Control Pulse Per Second signal** STP Diagnostic action. The port's status is currently **Test**.

Action:
The PPS port cannot be used while it is in the **Test** state. To use the PPS port, open the **Control Pulse Per Second signal** STP action, select the appropriate system, and in the" Control Pulse Per Second signal" window, select **Allow PPS port to receive PPS signals from ETS (default)** for this port. Refer to the help for the **Control Pulse Per Second signal** action, if necessary.

Note: The **Control Pulse Per Second signal** STP action can be used only by support system personnel.

Get information about the links between elements in the CTN

The lines that are drawn between the servers and systems in the topology indicate the links (connections) between them.

Note: These instructions do not pertain to the External Time Source (ETS). To get more information about the ETS, see “Get information about the CTN's External Time Sources” on page 1007.

Hover over a link to highlight that link and the systems to which it is connected. To see details about the connection between the two systems, click (select) the information icon (lowercase I in a blue circle), which is displayed over the highlighted link.

The "Active connection details" window contains two pages. The first page shows you the details for the system that is in the higher stratum level. The second page shows you the same details for the system that is in the lower stratum level. If both systems are in the same stratum level, the first page contains the details for the system that is furthest to the left in the topology.

To move between the pages, use the arrow icons at the bottom of the window, which are also labeled with the system names. The arrow icon and system name are available only for the page that you are not currently on.

The "Active connection details" window provides the following information for each link.

Connected system
Name and stratum level of the system to which the local STP identifiers are connected.

Remote directly attached system type-MFG-plant-sequence
Node descriptor for the attached system.

See active local STP links

Number of active local STP links.

Click **See active local STP links** to display the "Active local STP links" window, which provides a table of information about the local STP links for the connected systems. The table includes information about the **Channel Type**, the **AID** (adapter ID), the **Port**, and the **VCHID**. The table is sorted by channel type in alphabetical order by default. To toggle between ascending and descending order, click the **Channel Type** down-arrow.

Some table rows can be expanded to display additional information about the port and VCHID. The rows that are expandable include a caret (^) at the beginning of the row. Rows that are not expandable do not include a caret, and display a dash (-) in the **Port** and **VCHID** columns. Only one row can be expanded at a time. Click anywhere on a row to expand it. When expanded, the port and VCHID information is displayed. Click anywhere on the expanded row to collapse it.

Note: The VCHID for the last active STP link is marked with an asterisk (*).

To close the "Active local STP links" window, click **x**.

To close the **Local Uninitialized STP Links** window, click **x** or anywhere outside the window.

Topology toolbar

Use the **Topology toolbar** to adjust the display of the topology or view and modify the time synchronization of a CTN's Current Time Server.

The **Export CTN data** STP action provides the ability to export information about the current CTN to a Microsoft Excel spreadsheet. The resulting .xsl file can be downloaded and used with a screen reader for enhanced accessibility. For information about exporting CTN data to a file, see the help topic “Export CTN data” on page 1040.

For more information about the **Topology toolbar**, use the following links.

Adjust the topology view

The **Topology toolbar** includes the following elements for adjusting the display of the topology. Use these controls to optimize your view.

Zoom In
Enlarges images in the topology view.

Zoom Out
Shrinks images in the topology view.

Fit to Width
Fits the content of the topology within the topology frame.

Zoom by Percentage
Enlarges or shrinks the content of the topology frame based on a number that you select. Use the drop-down list to change the topology size in increments of 25 percent (the default is 100 percent).

The changes that you make to the topology view do not persist from session to session.

Get details about the configuration

The **Topology toolbar** displays the following details about the configuration of the specified CTN.

Time
Displays the time for the Current Time Server (CTS). The time is updated on every refresh. If the CTN is inactive, **Inactive CTN** is displayed in this field.

Date
Displays the date for the Current Time Server. If the CTN is inactive, **Inactive CTN** is displayed in this field.

Time zone
Displays the time zone for the Current Time Server. If the CTN is inactive, **Inactive CTN** is displayed in this field.

Current time details
Opens the **System Time** window, which provides timing details for the current CTN.

The **System Time** window contains two pages, and initially opens to page 1. To move back and forth between page 1 and page 2, use the page number toggle at the bottom of the window.

If the CTN is inactive, the values for the fields of the **System Time** window are displayed as **Not available**.

The "Current network configuration" area, on page 1 of the **System Time** window, contains the following details.

Configured at (UTC)
Displays the UTC time at which this configuration was applied.

The Coordinated Server Time area, on page 1 of the **System Time** window, contains the following details.

Time zone
Displays the time zone that is currently in effect for the CTN.

Currently
Specifies the time zone that is being observed (for example, EST or EDT).

Adjust time
Link that opens the **Adjust time** action. For more information, see “Adjust time” on page 1015.

Adjust time zone offset
Link that opens the **Adjust time zone offset** action. For more information, see “Adjust time zone offset” on page 1016.

The Offsets area, on page 1 of the **System Time** window, contains the following details.

Leap second
Displays the current number of leap seconds (+-) that are in effect for the network. This value is shown for all network types.

Time zone offset from UTC
Displays the standard time zone offset from UTC (+-) for an STP-only CTN with a time zone assigned.

Daylight saving time (hours : minutes)
Displays the current offset (+-) for daylight saving time in an STP-only CTN for which a time zone assigned. If the time zone does not use daylight saving time, or daylight saving time is not in effect, the value is 0 (zero). This offset is added to the time zone offset from UTC to reflect the current offset from UTC.

Adjust leap second offset
Link that opens the **Adjust leap second offset** action. For more information, see “Adjust leap second offset” on page 1019.

The Adjustment Steering area, on page 2 of the **System Time** window, provides detailed steering information for the CTN. If the clock needs to be adjusted, each system gradually adjusts its clock by steering towards the new time that is specified in the **Adjust time** link.

Adjustment steering allows the time at the Current Time Server to be changed by up to +/- 60 seconds. Adjustments greater than 60 seconds can be implemented manually, by way of the **Adjust time** link in multiple increments of +/- 60 seconds.

Note: STP can steer out a little more than three seconds a day, so a time adjustment of 60 seconds takes approximately three weeks.

The specified offset is gradually incorporated into the STP messages in small enough increments or decrements so that the operating systems, subsystems, and applications are unaware that time is speeding up or slowing down.

The Adjustment Steering area, on page 2 of the **System Time** window contains the following details.

Status

Specifies the status while the server is gradually adjusting its clock by steering towards the new time. The status can display one of the following:

Steering completed
Indicates that the adjustment steering has completed.

Steering in progress
Indicates that the adjustment steering is progressing.

Tracking to PPS signal
Indicates that pulse per second signals are continuously providing highly accurate adjustments to the Coordinated Server Time.

Amount (seconds)
Specifies the value that is provided in the most recent **Adjust time** amount that was specified from the console. This could be the result of dialing out to an External Time Source through the Hardware Management Console, or from entering an amount using the **Adjust time** action.

Start time (UTC)
Specifies the time at which the steering is to be initiated.

Estimated finish time (UTC)
Specifies the estimated time when the amount will be steered out. Because adjustments are continuous, this field is not available when the CTN time source is **NTP with pulse per second** or **PTP with pulse per second**.

CTN time source
Identifies the clock source according to the STP facility, which indicates where the adjustment originated from. Possible values are as follows.

- **Time set manually on console**
- **NTP**
- **NTP with pulse per second**
- **PTP**
- **PTP with pulse per second**

NTP stratum level (NTP or NTP with pulse per second only)
Identifies the accuracy of the time at the NTP server that is used as the External Time Source for the CTN. This field only appears for an STP-only CTN that has **NTP** or **NTP with pulse per second** as the CTN time source. A stratum level of 1 (one) indicates that the NTP server obtained its time directly from a reference time source. A stratum level of *n* indicates that the NTP timeserver is n-1 hops away from the time source.

Ethernet interface (PTP or PTP with pulse per second only)
Indicates the name of the preferred Ethernet interface.

NTP source ID (NTP or NTP with pulse per second only)
Identifies the location of the clock source, according to the NTP server. This field only appears for an STP-only CTN that has **NTP** (with a stratum level of 1 (one)) or **NTP with pulse per second** (with a stratum level of 1 (one)) as the CTN time source.

Grandmaster ID (PTP or PTP with pulse per second only)
Indicates the identifier of the grandmaster, which is a derivative of the MAC address.

To close the **System Time** window, click (select) **x**.

Adjust time

The **Adjust time** action guides you through the process of adjusting the current Coordinated Server Time (CST) for the CTN.

Without regular adjustment, the time within the CTN slowly drifts, which might or might not be acceptable, depending on the time accuracy requirements. You can make time adjustments manually by applying an adjustment offset. Adjustments are made in small enough increments that the operating system and subsystem software are unaware that time is speeding up or slowing down. This is called *steering*. In an STP-only CTN, adjustment steering is applied at the rate of approximately a one-second adjustment every seven hours.

Note that you can make time adjustments from the Current Time Server (CTS) only, which propagates them throughout the CTN.

Adjusting the time

Use the "Adjust time" window to adjust the current Coordinated Server Time (CST) for the CTN, or to modify or delete a previous time adjustment that is still in progress. The value that you enter is gradually steered out by the STP facility, causing no disruption to running programs.

To adjust the time, do the following.

1. Specify a value in the **Adjustment amount** field. You can type in the adjustment amount manually, or you can use the **ACCESS ETS** option to calculate and specify the value automatically.

   Adjustment amount
   To provide a value manually, specify the number of seconds by which to adjust the time in the **Adjustment amount** field.

   Note: When you use this field, it is presumed that you previously determined the required offset correction. Therefore, you need to provide an appropriate correction value only, with a positive (+) or negative (-) direction indicator, in this field.

   Valid values are between -60.000000 and +60.000000 seconds. A positive value results in a gradual speeding up. A negative value results in a gradual slowing down. You do not need to include the plus (+) sign for positive values.

   ACCESS ETS
   If it is installed and configured, an External Time Source (ETS) can be used to accurately calculate the adjustment offset and place it in the **Adjustment amount** field. To do this, select **ACCESS ETS**. An ETS request is submitted to calculate the time difference between the UTC time that is returned from the External Time Source and the Current Time Server time.

   After selecting **ACCESS ETS**, the **Accessing External Time Source** message window is displayed, which indicates the progress of the request.

   If the access is successful, the time difference is placed in the **Adjustment amount** field automatically, and the "Adjustment value updated" message window is displayed. Click **CLOSE** to return to the "Adjust time" window.

   If the access is not successful, the time difference is not placed in the **Adjustment amount** field, and the "Adjustment value could not be updated" message window is displayed. Select **CLOSE** to return to the "Adjust time window.

   Note: The adjustment amount that is calculated by the ETS might not be within the +/- 60-second requirement of the "Adjust time" window. The value that is returned must be reviewed for validity before you select **APPLY**. Values that are larger than +/- 60 seconds need to be applied in multiple increments until the total offset adjustment is accounted for.

2. After you specify the adjustment time, do one of the following.

   - To apply the time adjustment, select **APPLY**. The "Sending adjustment value to CTS" window is displayed, which indicates the progress of the change. Depending on the situation, one of the following messages is displayed.

"The time adjustment started successfully"
This message is displayed if the adjustment is successful. To close the **Adjust time** action, select **CLOSE**.

"Adjustment is being stopped"
This message is displayed if you specified a time adjustment value of 0 (zero) (to remove the previous time adjustment). To close the **Adjust time** action, select **CLOSE**.

"The time adjustment could not be started"
This message is displayed if the access is not successful. In this case, the previous adjustment value remains unchanged. To close the **Adjust time** action, select **CLOSE**.

- To close the **Adjust time** action, select **CANCEL**.

Adjust time zone offset

The **Adjust time zone offset** action guides you through the process of adjusting the time zone offset of the current Coordinated Server Time (CST) for the CTN.

Note: Adjusting the time zone while programs are running might cause the program to see local time *jump* forward or backward and could cause undesirable results. Use caution when modifying the time zone offset on running systems.

Use the "Adjust time zone offset" window to view or change the current time zone offset, time zone, Daylight Saving Time offset, scheduled time zone adjustment, or scheduled Daylight Saving Time adjustment.

Adjusting the time zone offset

1. Use the following options in the "Adjust time zone offset" area to adjust the time zone offset.

   Time zone
   Displays the time zone that is in effect for the CTN. If a time zone is not defined for the CTN, "No time zone specified" is displayed in this field.

   The **Time zone** field is read-only, but it displays a list of supported, selectable time zones. Select the drop-down list arrow to view them. If a time zone is not defined, you can select one from this list. Each of the supported time zone entries includes a defined offset from UTC and the Daylight Saving Time offset for that entry, if applicable.

   If the time zone you need does not appear in the list, select one of the five user-defined time zones (initially UD1 to UD5) at the bottom of the list and then select **Define** to create the time zone.

   Define
   Use this option to define a time zone and optionally, the automatic clock adjustment algorithms for Daylight Saving Time when the time zone you need is not available in the **Time zone** drop-down list.

   To create a user-defined time zone, do the following.

   a. Select one of the five user-defined time zones (UD1 to UD5) at the bottom of the **Time zone** field's drop-down list. After you select a user-defined time zone, the **Define** option becomes available.
   b. Select **Define** to create the time zone. The "Define time zone" window is displayed. Use this window to define the settings for the new time zone.
   c. Go to “Define a time zone” on page 1018, complete the steps there for defining a time zone, then return here (a link is provided).

2. Use the following options in the "Clock adjustment for daylight saving time" area to adjust the clock for Daylight Saving Time.

   Daylight saving time offset (hours : minutes)
   Displays the Daylight Saving Time offset of the selected time zone. If a time zone is not specified, or the selected time zone does not have Daylight Saving Time, the offset is 0 (zero).

Automatically adjust
To support automatic adjustment of Daylight Saving Time, select **Automatically adjust**.

If the specified time zone indicates that it supports automatic adjustment of Daylight Saving Time, then this option is selected by default. If a time zone is not specified, or the time zone does not support automatic adjustment of Daylight Saving Time, this option is disabled. If this option is enabled but not selected, you can select **Automatically adjust** to turn on the automatic adjustment of Daylight Saving Time for the CTN.

Set standard time
To change to standard time, select **Set standard time**. If the specified time zone does not support automatic adjustment of Daylight Saving Time, then this option is selected by default. Note that it is the operator's responsibility to manually change the **Set standard time** option (or schedule it to change) at the appropriate times.

Set daylight saving time
To change to Daylight Saving Time, select **Set daylight saving time**. Note that it is the operator's responsibility to manually change the **Set daylight saving time** option (or schedule it to change) at the appropriate times.

3. Use one of the following options of the "Schedule change on" area to adjust the schedule for clock adjustment.

   Schedule change on
   To have the time zone or clock adjustment for Daylight Saving Time take place on a specific date and local time, select **Schedule change on**. Specify the date and time in the **Date** and **Time** fields that follow. To select the date instead of typing it in the **Date** field, select the calendar icon. This option is selected by default.

   Change immediately
   To have the time zone or clock adjustment for Daylight Saving Time take place immediately, select **Change immediately**.

4. If you previously set up a scheduled clock adjustment to account for Daylight Saving Time, the "Scheduled clock adjustment for daylight saving time" area is displayed in the window. If you did not previously set up a scheduled clock adjustment to account for Daylight Saving Time, skip this step.

   The "Scheduled clock adjustment for daylight saving time" area displays the local time name, the Daylight Saving Time offset, and the time at which the scheduled adjustment occurs. Review this information as needed.

5. If you previously set up a scheduled time zone change, the "Scheduled time zone" area is displayed in the window. If you did not previously set up a scheduled time zone change, skip this step.

   The "Scheduled time zone" area displays the time zone and the time at which the scheduled adjustment occurs. Review this information as needed.

6. After you set the time zone offset, do one of the following.

   - To apply the changes, select **APPLY**. The "Time zone change confirmation" window is displayed, which contains information about either the time zone or Daylight Saving Time settings that you specified. Use this window to either confirm that you want to make the changes, or to cancel the changes. Do one of the following.
     - To confirm, select **CONTINUE**. The "Sending adjustment value to CTS" window is displayed, which indicates the progress of the change. If the changes are successful, the "Time zone definition adjusted successfully" window is displayed. Click **CLOSE**.
     - If you decide that you do not wish to make the time adjustment, select **CANCEL** to go back to the "Adjust time zone offset" window.
   - To close the **Adjust time zone offset** action, select **CANCEL**.

Define a time zone

Use the "Define time zone" window to define a time zone and optionally, the automatic clock adjustment algorithms for Daylight Saving Time when the desired time zone is not available in the **Time zone** drop-down list.

Note: This help topic assumes that you have already:

- Selected one of the five user-defined time zones (UD1 to UD5) from the bottom of the **Time zone** field's drop-down list
- Selected the **Define** option on either the "Set time zone" or "Adjust time zone offset" windows. If you have not done so, return to “Step 8: Set Time Zone” on page 1053 or Step 1 of “Adjust time zone offset” on page 1016 and select a user-defined time zone and the **Define** option before continuing with these instructions.

To define a time zone, do the following.

1. Use the following fields of the "Define time zone" window to choose the time zone settings.

   Description
   Specifies a description of the algorithm (cannot exceed 80 characters).

   Standard time name
   Specifies an abbreviated description of the time zone while on standard time. This field can contain a maximum of four characters.

   Daylight saving time name
   Specifies an abbreviated description of the time zone while on Daylight Saving Time. This optional field can contain a maximum of four characters.

   UTC offset
   Specifies an offset range from -14 hours to +14 hours. This value is specified in plus or minus hours and minutes.

   Daylight saving time offset
   Displays the Daylight Saving Time offset of the selected time zone. If a time zone is not specified, or the selected time zone does not have Daylight Saving Time, the offset is 0 (zero).

   Define adjustment of clock for daylight saving time
   To request that the algorithms be defined for automatic clock adjustment, do the following.

   a. Select the **Define adjustment of clock for daylight saving time** option (a check mark is displayed). Otherwise, if this option is not selected (a check mark is not displayed) the **Daylight saving time start** and **Daylight saving time end** fields are unavailable, and you cannot specify the algorithms for automatic clock adjustment for Daylight Saving Time.

      If a Daylight Saving Time offset is specified, you must manually switch from standard to Daylight Saving Time. Conversely, if a Daylight Saving Time offset is not specified, you must manually switch from Daylight Saving Time to standard.

   b. Select one of the following **Daylight saving time start** algorithms. The algorithm is used for adjusting the clock to begin Daylight Saving Time.

      Schedule by day of week in month
      To set the clock adjustment for Daylight Saving Time to begin on a specific day in the month (such as the first Sunday in April at 7:00), select **Scheduled by day of week in month**. To see an example of this setting, hover over the question mark icon.

      Schedule by date
      To set the clock adjustment for Daylight Saving Time to begin on a specific day and time (such as March 31 at 22:00), select **Scheduled by date**. To see an example of this setting, hover over the question mark icon.

      Schedule by time of week after a specific date
      To set the clock adjustment for Daylight Saving Time to begin on a specific day of the week after a specific date (such as the first Friday after March 15 at 7:00), select **Scheduled by**

day of week after a specific date. To see an example of this setting, hover over the question mark icon.

Depending on the selection that you made, supply the necessary information in the appropriate date and time fields by using the down arrow to select a value.

c. Select one of the **Daylight saving time end** algorithms. The algorithm is used for adjusting the clock to end Daylight Saving Time.

Schedule by day of week in month
To set the clock adjustment for Daylight Saving Time to end on a specific day in the month (such as the last Sunday in October at 6:00), select **Schedule by day of week in month**. To see an example of this setting, hover over the question mark icon.

Schedule by date
To set the clock adjustment for Daylight Saving Time to end on a specific day and time (such as September 23 at 18:00), select **Schedule by date**. To see an example of this setting, hover over the question mark icon.

Schedule by day of week after a specific date
To set the clock adjustment for Daylight Saving Time to end on a specific day in the month (such as the last Sunday in October at 6:00), select **Schedule by day of week in month**. To see an example of this setting, hover over the question mark icon.

Depending on the selection that you made, supply the necessary information in the appropriate date and time fields by using the down arrow to select a value.

2. After you select the user-defined time zone settings, do one of the following.
   - To create the time zone, select **APPLY**. If the change is successful, the "User-defined time zone saved successfully" window is displayed. Click **CLOSE**.
   - To close the "Define time zone" window, select **CANCEL**.
3. Return to the task from which you accessed the **Define** option. Choose the appropriate link, as follows.
   - If you selected **Define** on the "Adjust time zone offset window", go to Step 2 in “Adjust time zone offset” on page 1016.
   - If you selected **Define** on the "Set time zone" window, go to Step 2 of “Step 8: Set Time Zone” on page 1053.

Adjust leap second offset

The **Adjust leap second offset** action guides you through the process of adjusting the leap second offset of the current Coordinated Server Time (CST) for the CTN.

Leap seconds adjust the accuracy of UTC time to account for irregularities in the rate of the Earth's rotation. A leap second is inserted between second 23:59:59 of one calendar date and second 00:00:00 of the following date. The International Earth Rotation and Reference Systems Service (IERS) determines when a leap second is required and issues Bulletin C to announce whether a leap second must be added. Since 1972, the IERS scheduled leap seconds for either June 30th or December 31st.

Note: It is possible that a leap second could also be removed, but this has never occurred. In that case, the time would be adjusted from 23:59:58 to 00:00:00.

Adjusting the leap second offset

Use the "Adjust leap second offset" window to adjust the leap second offset for a CTN.

1. Specify the leap second offset in the **Offset** field. The leap second offset value that is in effect for the CTN is initially displayed in this field.

   When the External Time Server (ETS) is an NTP server or PTP interface, the UTC time information that is obtained from public servers is automatically adjusted for added leap seconds. In this case, unless your company requires time stamps to meet a specific level of accuracy, you can set the offset value to 0.

You must specify an offset value if your company has legal or contractual requirements for time stamps to be accurate to a specific value. You must also specify an offset value if your company uses time stamps for time-dependent banking, scientific, or navigational purposes. The offset value must equal the total accumulated number of leap seconds that were announced by the IERS since January 1972. As of January 2017, the total number of leap seconds is 27.

To determine the correct offset value to enter, go to the IERS website and check Bulletin C for the months since January 2017. Add 1 for each leap second that was inserted since December 2016.

IMPORTANT: It is dangerous to add more than one leap second at a time while programs are running on the system. For example, if your system missed adding a leap second three times in a row, add one leap second. Allow the system to adjust itself, then add the second leap second, and so on.

Before starting work on the system, the leap second value can be jumped to the proper value.

2. Choose a scheduling option, as follows.

   Schedule offset change on
   Specifies a date on which the leap second offset takes effect. When this option is selected, the **Date** field becomes available. Select the calendar icon to choose the date. This option is selected by default.

   Schedule offset change on is the default option and is already selected when the window opens.

   Schedule offset change on June 30th
   Specifies that the leap second offset value takes effect on June 30th.

   Schedule offset change on December 31st
   Specifies that the leap second offset value takes effect on December 31st.

   Change offset immediately
   Specifies that the leap second offset takes effect immediately.

3. After you specify the leap second offset value and select a scheduling option, do one of the following.

   - To apply the changes, select **APPLY**. The "Leap second change confirmation" window displays the new leap second offset and scheduling values and prompts you to confirm that you want to make the changes. Do one of the following.
     - To confirm, select **CONTINUE**. The "Sending adjustment value to CTS" window is displayed, which indicates the progress of the change. If the change is successful, the "Leap second offset adjusted successfully" window is displayed. Click **CLOSE** to return to the "Adjust leap second offset" window.

       If you added more than one leap second in the "Adjust leap second offset" window, the "Leap second change is greater than 1" error window is displayed. Click **CLOSE** to return to the "Adjust leap second offset" window.
     - If you decide that you do not wish to continue with the leap second adjustment, select **CANCEL** to go back to the "Adjust leap second offset" window.
   - To close the **Adjust leap second offset** action, select **CANCEL**.

Get CTN configuration status

Use the **Status** field and icon on the topology toolbar to determine the overall health of the CTN 's configuration.

If the topology contains no errors, a green circle and check mark icon are displayed in the **Status** field. Click (select) this icon to display an information window that explains the status. To close the information window, click the green **Status** icon again.

When a server or system in the CTN has one or more errors, the following changes occur in the topology view.

- The **Status** icon on the topology toolbar changes to a red exclamation mark inside a red circle, and displays a number to indicate the number of errors.

- The outline of the server or system's rectangle in the topology view changes to red, and displays a red exclamation mark.

Getting information about all errors in the topology

To get information about all of the errors in the topology, click the **Status** icon (the red circled exclamation mark) on the topology toolbar, which opens the **Errors** window. The **Errors** window displays information about each of the errors in the topology, in drop-down list style.

The **Errors** window provides the following information for each error.

- Name of the system or server that contains the error
- Error name
- Error description
- Error message number
- Date and time at which the error message was sent.

When there are many errors, and the list is too long to fit vertically on the screen, the **Errors** window displays the errors on multiple pages. Use the right and left arrow icons at the bottom of the **Errors** window to move between pages.

To close the **Errors** window, click the red **Status** icon again.

Getting information about server or system-specific errors

To get information about one or more errors for a particular server or system, click its rectangle in the topology view. The STP Status window opens.

On the STP Status window, click **This system has x errors**. The **Errors** window opens and displays information about each error, for this server or system only, in drop-down list style.

The **Errors** window provides the following information for each error.

- Name of the system or server that contains the error
- Error name
- Error description
- Error message number
- Date and time at which the error message was sent.

You can also see a list of the errors for all servers and systems in the CTN by clicking the **See all** link on the **Errors** window. Clicking **See all** closes the STP status window and expands the content of the **Errors** window to include all errors in the CTN.

When there are many errors, and the list is too long to fit vertically on the screen, the **Errors** window displays the errors on multiple pages. Use the right and left arrow icons at the bottom of the **Errors** window to move between pages.

To close the **Errors** window, click the red **Status** icon on the **Topology toolbar**.

Global CTN details area

Use the **Global CTN details** area of the **Manage System Time** window to specify a CTN to work with, or to get details about the servers and systems in the topology. For more information about the **Global CTN details** area, use the following links.

Select a different CTN

To see the other CTNs that are available, click (select) the down arrow in the **CTN ID** field. A list opens that displays the available CTNs. Select a new CTN from the list.

Rename a CTN

To edit the name of the current CTN, do the following. This is a global change that is applied to the Current Time Server (CTS) as well as to all members of the CTN.

Note: An inactive CTN cannot be renamed.

1. In the **CTN ID** field, click (select) the edit (pencil) icon. The **CTN ID** field changes to allow text entry. **Save** and **Cancel** options are also displayed.
2. Type a new name into the **CTN ID** field. The CTN ID is case-sensitive and can contain one to eight characters. Valid characters are A-Z, a-z, 1-9, and _ (underscore).

   Note: The name that you specify must not be the same as an existing CTN ID.

   At this point, if you decide that you do not want to rename the CTN, click **Cancel**.
3. To apply the changes, click **Save** (or press the **Enter** key).
4. When the **Global Timing Network ID Change Confirmation** window opens, do one of the following:
   - Click **CONTINUE** to apply the name change and refresh the CTN's topology view. If the name change is successful, the "CTN renamed successfully" window is displayed. Click **CLOSE**.
   - Click **CANCEL** or **x** to cancel the name change and return to the topology view.

Determine the membership status for the current CTN

The global CTN details area includes the **Membership** field, which indicates whether membership in the current CTN is restricted or unrestricted. Possible values are **Restricted CTN** and **Unrestricted CTN**.

Determine the servers and systems, and the roles they play in the CTN

The **Global CTN details** area displays the stratums that make up the structure of the topology, and the servers and systems that are associated with them.

Stratums are used to identify the hierarchy of the servers and systems within the timing network. The stratum number indicates the position within the hierarchy. Level 1 is the highest stratum and level 4 is the lowest. Some systems have a maximum stratum level of 3.

Under each stratum is a list of the servers and systems that belong to it. If a server has one or more special roles, abbreviations for those roles are displayed beside the server name. Click (select) any of the systems to display the **STP Status** window, provides information about the following.

Server role
Specifies the role that the server plays in the topology. The roles are as follows.

- PTS: Preferred Time Server
- BTS: Backup Time Server
- ARB: Arbiter
- CTS: Current Time Server

For more information about server roles, see “Determine the servers that have roles in the CTN” on page 1006.

This field applies to systems with roles (servers) only. For systems that do not have roles, this field is empty.

Timing state
Indicates the timing state in which the server or system is operating. If it has a value of anything other than **Synchronized**, then the server or system is not actively participating in a CTN. The possible **Timing state** values are **Unsynchronized**, **Synchronized**, or **Stopped**.

Usable clock source
Indicates whether a usable STP clock source is available to synchronize the server time of day (TOD). This value can be either **Yes** or **No**.

Maximum timing stratum level
Specifies a number that indicates how far a server can be from the Current Time Server and still be in a synchronized state. If the maximum timing stratum level is 3 (three), a server can be two hops away.

Maximum STP version
Specifies a number that indicates the maximum level of STP facility code that is supported by this server.

See local uninitialized STP links

Number of local uninitialized STP links.

Click **See local uninitialized STP links** to display the **Local Uninitialized STP Links** window, which provides a table of information about the server or system's coupling links that can be used to exchange STP messages with other servers. If there are no uninitialized STP links, **There are no local uninitialized STP links** appears as a field name only (it is not an active link). The table shows the **Local STP Link ID** (PCHID address), the **STP Link Type**, and the reason why the link is uninitialized (**Reason code sent** and **Reason code received**). All links in the table are in an uninitialized state.

The possible reason codes are:

Allowable paths exceeded
Greater than 512 STP paths are being activated. Contact next level of support.

Busy
A busy condition or resource contention was detected. This should be a temporary condition. Contact next level of support if the condition persists.

CF response
The attached server does not support STP.

Communication error
A communication timeout is recognized for the attached server, which indicates that the attached server stopped sending STP timing information.

Configuration error
This server detected a different CTN ID on the attached server. The CTN ID must match the CTN ID of this server to be a member of the same STP-only CTN.

Disagree on CTN members allowed
This server disagrees with the attached server about which servers are allowed to participate in the STP-only CTN. One or both servers might have specified which servers are allowed to participate in the CTN.

Fenced
The link is operational, but it is in a fenced state and cannot be initialized for STP communication. Remove the link from the fenced state.

Initialization is not complete
The physical link is operational, but link initialization has not been attempted or is in progress. This might be a temporary condition.

Invalid operation parameters
An invalid STP command was sent. Contact next level of support.

Link failure
A link failure is detected on the physical link. Determine the reason for the failure or contact next level of support.

Network configuration error
This server and the attached server do not have the same network configuration. They might have the same servers configured, but disagree on who is the Current Time Server. Verify the configuration at each server to determine why they disagree. Contact next level of support if the condition persists.

Node descriptor error
The node descriptor on the physical link is not valid.

No response
An attempt was made to communicate with the attached server, but it did not respond within the allowed time. Verify the links. Contact next level of support if the condition persists.

Not allowed to join CTN
The attached server is not allowed to join the same STP-only CTN as this server. This server might have specified which servers are allowed to participate in the CTN.

Offline
The physical link is in the offline state on this server. Configure the link online.

Removed path
The attached server sent a command to remove the STP path. This might be a temporary condition. Contact next level of support if the condition persists.

Self-coupled server
The link is attached from this server to itself.

STP is not enabled
The attached server does not have the STP feature enabled. STP communication with the server is not possible.

Takeover active state
The Current Time Server is being reassigned. This might be the result of a recovery action. Verify the status of the Preferred Time Server and Backup Time Server. This condition should be temporary. Contact next level of support if the condition persists.

Unsupported version (min=x, max=y)
The attached server is running with an STP version that is incompatible with this server's STP version. The minimum and maximum STP version is identified.

ASSUME CTS
If a system that is not the Current Time Server (the PTS or the BTS) needs to take over as the Current Time Server (CTS), the **ASSUME CTS** option is displayed in the **STP Status** window.

Console-assisted recovery uses the HMC in an attempt to determine the status of the PTS (when initiated by the BTS) or the status of the BTS (when initiated by the PTS). Console-assisted recovery helps to determine whether the BTS can take over as CTS, or the PTS can take back its role as the CTS.

When STP configuration cannot be restored through console-assisted recovery from either the PTS or BTS, an outage for both servers can occur until link path connectivity is re-established between the two servers. In this situation, if the status of the servers can be determined manually, you can force one of the servers to assume the CTS role without permanently reconfiguring the CTN.

To force the specified server (PTS or BTS) to assume the CTS role, do the following.

1. Verify that there is no system functioning as the Current Time Server for the CTN.
2. Click **ASSUME CTS**.
3. In the "Assume Current Time Server confirmation" window, click **CONTINUE**.
4. Read the conditions and options that are presented to you in the "Assume Current Time Server confirmation" window carefully. If you are certain that you want this system to assume the role of CTS, click **YES**. Otherwise, click **NO**.

For more information about the server roles and the related abbreviations, see “Topology view” on page 1003.

Get help for using Manage System Time

To access help for using the functions and features of the Manage System Time task, click **Help**.

STP actions

The **STP Actions** area of the **Manage System Time** main window includes a number of actions that you can perform against a specified CTN. Hover over an action to see a short description. To see the diagnostic actions that are available, click (select) **Diagnostic actions** (or its down arrow).

Note: In some cases, one or more of the STP actions might not be available to certain users. In this situation, the actions that are unavailable are not displayed under **STP Actions**.

The **Export CTN data** STP action provides the ability to export information about the current CTN to a Microsoft Excel spreadsheet. The resulting .xsl file can be downloaded and used with a screen reader for enhanced accessibility. For information about exporting CTN data to a file, see the help topic "Export CTN data" on page 1040.

For more information about the STP actions, use the following links.

Add systems to CTN

The **Add systems to CTN** action guides you through the process of adding one or more systems to a CTN.

Note the following limitations for using the **Add systems to CTN** action.

- You cannot add servers when CTN membership restrictions are in effect. If you open the **Add systems to CTN** action while CTN membership is restricted, "The members of this CTN are restricted" window opens to warn you, and gives you the opportunity to remove the restrictions. For more information, see "The members of this CTN are restricted window" on page 1047.
- While two CTNs are in the process of merging (**Join existing CTN** action), you cannot add servers to either of those CTNs.

Note: You cannot add servers when CTN membership restrictions are in effect. If you open the **Add systems to CTN** action while CTN membership is restricted, "The members of this CTN are restricted" window opens to warn you, and gives you the opportunity to remove the restrictions. For more information, see "The members of this CTN are restricted window" on page 1047.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Step 1: Add CTN Members

Use the "Add systems to the Coordinated Timing Network (CTN)" window to select one or more systems to add to the CTN. You can select systems from CTNs that are not configured with a CTN ID or from inactive CTNs. (An inactive CTN is one or more systems for which a CTN ID was previously specified.)

The selectable systems are displayed with their related CTNs. Each system is represented in the topology by a rectangle and is labeled with its system name.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which you are adding systems.

To add members to a CTN, do the following.

1. Click (select) one or more systems, from any of the CTNs that are displayed in this window, to add them to the current CTN. When you click a system, it changes color (dark gray) to indicate that it is selected.
2. When you are finished selecting systems, do one of the following.
   - To go to the next step, click **NEXT**. If any of the systems you selected are not connected to any of the systems in the current CTN, the "Systems do not have connection to CTN" window opens and displays the unconnected systems. Do one of the following.
     - To add the selected systems to the CTN, and to go to the next step, click **CONTINUE**.
     - To go back to the "Add systems to the Coordinated Timing Network (CTN) window to select other systems, click **CLOSE**.
   - To close the **Add servers to CTN** action, click **CANCEL**.

Step 2: Confirm Changes

Use the "Confirm changes" window to confirm that you want to add the specified systems.

1. Review the new topology to ensure that the changes you made created the results that you expected, then do one of the following.
   - If the topology is correct, click (select) **APPLY** to apply the changes and proceed to the next step.
   - If the topology is not correct, click **BACK** to return to the "Add systems to the Coordinated Timing Network (CTN)" window. The systems that you chose in Step 1 are still selected.
2. The "**Local CTN ID change confirmation**" window is displayed after you select **APPLY** on the **Confirm Changes** window. It provides a table of information about the changes you are making. For each system that you selected, it displays the **System name**, the CTN that it is moving from (**Source CTN**) and the CTN that it is moving to (**Destination CTN**). If you selected more than four systems, use the scroll bar to view them.

   Review the information in the "Local CTN ID change confirmation" window, then do one of the following.
   - If the information in the table is correct, click **APPLY** to apply the changes.

     After you click **APPLY**, the "Adding systems to CTN" window opens, which indicates the progress of the configuration changes. If the systems are added successfully, the "Systems added to CTN successfully" window is displayed. Click **CLOSE**.

     Note: When a system is added to a CTN, the topology display in the main window is automatically refreshed.
   - If the information in the table is not correct, click **CANCEL**, to return to the "Confirm changes" window.

Configure External Time Source

The **Configure External Time Source** action guides you through the process of modifying and configuring the External Time Source for a server or system.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Step 1: Select System

Use the table in the "Select a system to modify its External Time Source" window to select the system that will have its ETS configured.

1. Use the **Select** column in the table to select a system (you can select one). The table provides the following information for each system.

   System name
   Name of the system. If the system has a role in the CTN, the abbreviation for that role is displayed beside the system name.

   ETS
   External Time Source of the system. Possible values are **NTP**, **NTP with PPS** (pulse per second), **PTP**, **PTP with PPS** (pulse per second), and **None**.

   Preferred
   The IP address of the preferred NTP server or the name of the preferred PTP interface. If a preferred NTP server or PTP interface is not defined for the system, this field is blank.

   Secondary
   The IP address of the secondary NTP server or the name of the secondary PTP interface. Defining two NTP servers or PTP interfaces for each system ensures redundancy. If a secondary NTP server or PTP interface is not defined for the system, this field is blank.
2. After selecting a system, do one of the following.
   - To go to the next step, click (select) **NEXT**.
   - To close the **Configure External Time Source** action, click **x**.

Step 2: Choose External Time Source

Use the **Choose External Time Source** window to select an External Time Source.

1. Select one of the following options from the **Choose External Time Source** window.

   Use NTP
   Specifies that an NTP server is the External Time Source. Up to two NTP servers can be configured for use.

   Use NTP with Pulse Per Second (PPS)
   Specifies that an NTP server with pulse per second (PPS) is the External Time Source. An NTP server with PPS provides enhanced time accuracy for the CTN. STP is designed to track to the PPS signal from the NTP server and maintain accuracy of 10 microseconds, as measured at the PPS input of the server.

   A highly stable and accurate pulse per second (PPS) output from the NTP server that precisely indicates the start of a second, must be attached to the PPS port of the server in the CTN. One NTP server with a pulse per second output can be configured to each PPS port. Also, at least one NTP server must be configured at the server that has the Current Time Server role.

   A number of variables such as accuracy of the NTP server to its time source (GPS radio signals, for example) and the cable that is used to connect the PPS signal determine the ultimate accuracy of STP relative to Coordinated Universal Time (UTC).

   Use PTP
   Specifies that a PTP interface is the External Time Source. Up to two PTP interfaces can be configured for use.

   Use PTP with Pulse Per Second (PPS)
   Specifies that a PTP interface with pulse per second (PPS) is the External Time Source. A PTP interface with PPS provides enhanced time accuracy for the CTN. STP is designed to track to the PPS signal from the PTP interface and maintain accuracy of 10 microseconds, as measured at the PPS input of the interface.

   A highly stable and accurate pulse per second (PPS) output from the PTP interface that precisely indicates the start of a second, must be attached to the PPS port of the server in the CTN. One PTP interface with a pulse per second output can be configured to each PPS port. Also, at least one PTP interface must be configured at the server that has the Current Time Server role.

   A number of variables such as accuracy of the PTP interface to its time source (GPS radio signals, for example) and the cable that is used to connect the PPS signal determine the ultimate accuracy of STP relative to Coordinated Universal Time (UTC).

   None
   Specifies that an External Time Source is not used.

2. After you select an External Time Source option, do one of the following:

   - If you chose **Use NTP**, **Use NTP with Pulse Per Second (PPS)**, **Use PTP**, or **Use PTP with Pulse Per Second (PPS)**, click (select) **NEXT** to go to the next step.

     If you chose the **None** option, the **No External Time Source Selected** message window is displayed. If you are sure that you want to proceed without selecting an External Time Source, click **CONTINUE** to go to “Step 5: Confirm Changes” on page 1038.

     If you do not want to continue without selecting an external time source, click **CANCEL** to return to the **Choose External Time Source** window.
   - To return to the "Select a server on which to modify the External Time Source" window, click **BACK**.

Step 3: Verify ETS Selections

The process of verifying External Time Source selections is different, depending on whether the ETS is an NTP server or PTP interface. Refer to the appropriate section in this help topic:

- If you specified **NTP** or **NTP with Pulse Per Second (PPS)** in “Step 2: Choose External Time Source” on page 1027, refer to “Verify ETS Selections (NTP only)” on page 1028.
- If you specified **PTP** or **PTP with Pulse Per Second (PPS)** in “Step 2: Choose External Time Source” on page 1027, refer to “Verify ETS Selections (PTP only)” on page 1034.

Verify ETS Selections (NTP only)

Use the "Verify Network Time Protocol servers" window to verify the NTP servers.

When the "Verify Network Time Protocol servers" window opens, an NTP connectivity test is run, which queries the status of enabled servers. The "Testing NTP connectivity" message window is displayed, which indicates the progress of the test. When the test completes, one of the following messages is displayed.

- If the test is successful, the "Connectivity test successful" message is displayed. Click **OK**.
- If the test is not successful, the "Connectivity test failed" message is displayed. Click **OK**.

1. Use the table and other options in the "Verify Network Time Protocol servers" window to verify the NTP servers. The table displays the following details for the configured NTP servers. A maximum of two servers are included in the table for each system. The *Preferred* NTP server is displayed in the first row and the *Secondary* NTP server (if applicable) is displayed in the second row.

   Enabled
   Displays a switch that indicates whether the NTP server is enabled or disabled. When the position of the switch is to the right, the server is enabled. When the position of the switch is to the left, the server is disabled. To disable or enable an NTP server, click (select) the switch until it is in the appropriate position.

   PPS port (applies to NTP with pulse per second only)
   Indicates the PPS port that is associated with the server.

   Note: This column is only displayed in the table if you selected **Use NTP with pulse per second (PPS)** as the External Time Source.

   The **PPS port status** area, which is displayed below the table in the "Verify Network Time Protocol servers" window, provides status for the PPS ports of the *Preferred* and *Secondary* NTP servers. If a system's ETS is configured for **NTP with pulse per second (PPS)**, and that system is the Arbiter, or has no role in the CTN, then the **PPS port status** area is not displayed.

   NTP server
   Displays the IP or web address of the servers that you specified in “Step 1: Select System” on page 1026. The IP or web address is displayed regardless of whether a server is enabled or disabled.

   If you wish to edit a server's address, click (select) the **Edit NTP address** (pencil) icon. Specify a new address, then, to save the changes, either click the check mark icon or press the **Enter** key on the keyboard. To delete the changes and exit edit mode, click the x icon.

   After you edit an NTP server address, the values for that server in the **Stratum**, **Source**, and **Connection status** columns are replaced by ellipses (**...**). To restore values to the **Stratum**, **Source**, and **Connection status** columns, click **TEST CONNECTIVITY**. After the test completes, the columns are automatically updated with the current values for that server.

   Stratum
   Indicates the accuracy of the time at the NTP server. A stratum level of 1 indicates that the NTP server obtains its time directly from a reference time source. A stratum level of *n* indicates that the NTP server is *n*-1 hops away from the time source.

   Source
   Displays a short description of the time source for the NTP server. If the NTP server has a **Stratum** of 1, the value displayed in the **Source** field is the time source from which the NTP server obtains the time. If the NTP server has a value that is greater than 1, the value that is displayed in the **Source** field is the address of the time source from which the NTP server obtains the time.

   Some of the possible source values and their descriptions include:

Local
Uncalibrated local clock

Cesium
Calibrated Cesium clock

Rubidium
Calibrated Rubidium clock

PPS
Calibrated quartz clock or other pulse-per-second source

IRIG
Inter-Range Instrumentation Group

ACTS
NIST telephone modem service

USNO
USNO telephone modem service

PTB
PTB (Germany) telephone modem service

TDF
Allouis (France) Radio 164 kHz

DCF
Mainflingen (Germany) Radio 77.5 kHz

MSF
Rugby (UK) Radio 60 kHz

WWV
Ft. Collins (US) Radio 2.5, 5, 10, 15, 20 MHz

WWVB
Boulder (US) Radio 60 kHz

WWVH
Kaui, Hawaii (US) Radio 2.5, 5, 10, 15 MHz

CHU
Ottawa (Canada) Radio 3330, 7335, 14760 kHz

LORAN-C
LORAN-C radio navigation system

OMEGA
OMEGA radio navigation system

GPS
Global Positioning Service

HBG
Prangins, HB 75 kHz

JJY
Fukushima, JP 40 kHz, Saga, JP 60 kHz

GOES
Geostationary Orbit Environment Satellite

INIT
Initializing

GNSS
Global Navigation Satellite System

Connection status
Indicates the current status of an NTP server, or the results of a query to the server. The status in this field can be either **Error** or **No errors**.

When the connection status is **Error**, you can get more detailed information by clicking the caret to the right. The table row for this server expands and displays the following information.

Possible status messages include:

Success

Message:
Success

Explanation:
Access to the NTP time server was successful.

Action:
None.

Success - initializing

Message:
Success - initializing

Explanation:
Access to the NTP time server was successful. The NTP time server is still initializing.

Action:
None.

Success - local source

Message:
Success - local source

Explanation:
Access to the NTP time server was successful, however, the local clock of the NTP time server is being used as the time source.

Action:
If the NTP time server was just configured for use, it might be using its local clock while synchronization to its real-time source is taking place. If the status persists for too long, consider assigning a different NTP time server to ensure an accurate time source for the STP-only CTN.

Incorrect IP address

Message:
Incorrect IP address

Explanation:
The NTP IP address is not in the proper format or the DNS failed to recognize the web address and could not convert it into an IP address.

Action:
Correct the IP address or the web address and select **TEST CONNECTIVITY**.

Socket failure

Message:
Socket failure

Explanation:
The support element is resource constrained and is unable to create a connection to the NTP time server.

Action:
Contact next level of support.

Communication failure

Message:
Communication failure

Explanation:

- An error occurred while reading from or writing to the NTP time server.
- IPv6 link-local address is specified that is not fully qualified.

Action:

- Verify the Ethernet connection between the NTP time server and the support element. select **TEST CONNECTIVITY** to test access to the NTP time server. If the problem persists, contact next level of support.
- IBM z10 accepts IPv6 addresses for target NTP time servers. Normal IPv6 addresses should resolve correctly to the target NTP server. Link-local addresses (FE80:*) are not routable addresses and are only for use on the same link (same subnet). These link-local addresses do not resolve correctly unless they are on the same subnet as an interface to the support element and are fully qualified with the zone identifier. Find the fully qualified setting for the link-local address.

Timeout failure

Message:
Timeout failure

Explanation:
A timeout occurred while waiting for the NTP time server to respond to a request.

Action:
Verify that the IP address or web address of the NTP time server, the status of the NTP time server, and the connections to the physical NTP time server to ensure that the request is reaching its destination. If a problem is found, select **TEST CONNECTIVITY** to test access to the NTP time server. If successful, select **Next**. If the NTP time server is fully operational, the connections are valid, and the problem still persists, contact next level of support.

Server access denied

Message:
Server access denied

Explanation:
The NTP time server denied access to the request.

Action:
Verify the IP address or web address is a valid NTP time server and select **TEST CONNECTIVITY**.

Server unsynchronized

Message:
Server unsynchronized

Explanation:
The NTP time server has not yet fully synchronized to its target time source.

Action:
The synchronization process takes time for the specified **NTP Server** to follow its time source. Wait a while (up to 20 minutes) to see if the synchronization completes and the problem gets resolved. If the specified **NTP Server** fails to yield success, configure a new **NTP Server** and select **TEST CONNECTIVITY** to test the server.

Server must resynchronize

Message:
Server must resynchronize

Explanation:
The **NTP Server** is in the process of resynchronizing to its target time source.

Action:
The resynchronization process takes time for the specified **NTP Server** to adjust to follow its time source. Wait a while (several hours) to see if the resynchronization completes and the problem gets resolved. If the specified **NTP Server** fails to yield success, configure a new **NTP Server** and select **TEST CONNECTIVITY** to test the server.

NTP server error

Message:
NTP server error

Explanation:
An undefined error was returned while accessing the NTP time server.

Action:
Verify that the IP address or web address is a valid NTP time server and select **TEST CONNECTIVITY**.

Unsupported NTP server version

Message:
Unsupported NTP server version

Explanation:
The NTP time server is using an NTP version that is not supported.

Action:
Configure an NTP time server that is using NTP V3 or higher and select **TEST CONNECTIVITY**.

NTP server stratum greater than 15

Message:
NTP server stratum greater than 15

Explanation:
The NTP time server returned a stratum greater than fifteen (15). Fifteen (15) is the maximum allowable NTP time server stratum.

Action:
Change the IP address or web address to a valid NTP timeserver and select **TEST CONNECTIVITY**.

NTP server packets are bad

Message:
NTP server packets bad

Explanation:
The NTP packets received were not in the proper format.

Action:
Change the IP address or web address to a valid NTP time server and select **TEST CONNECTIVITY**.

Invalid source ID

Message:
Invalid source ID

Explanation:
The source ID (NTP reference ID) returned from the stratum-1 NTP time server does not contain printable characters.

Action:
Change the IP address or web address to a valid NTP time server and select **TEST CONNECTIVITY**.

CPC/NTP time difference > 60 seconds

Message:
CPC/NTP time difference > 60 seconds

Explanation:
The timestamp returned in the NTP packet for this NTP time server differed from the CPC time by more than 60 seconds.

Action:
Verify the NTP time server is working properly and is attached to a valid time source. If the NTP time server is valid and this is a newly configured STP-only CTN, it is possible that the initial time was set incorrectly. If a disruptive action can be performed, the STP-only CTN can be deconfigured. After deconfiguring the CTN, setup a new CTN using the **Setup new CTN** action. On the **SET DATE AND TIME** step, select **Use the configured External Time Source** to set date and time to initialize the CPC clock with the time from the NTP time server. Otherwise, the time difference can be manually steered out using the **Adjust time** panel within **Current time details** by specifying the full +/- 60 second adjustment limit. When the adjustment amount is less than 60 seconds, the NTP time server status will be updated.

2. If applicable, use the following options of the "Verify Network Time Protocol servers" window for testing the connectivity of the NTP servers and setting (and resetting) NTP thresholds.

TEST CONNECTIVITY
Queries the status of enabled servers. Testing the connectivity of NTP servers is optional, but recommended.

To test the IP connectivity of enabled servers, click **TEST CONNECTIVITY**. When the test completes, the values in the **Stratum**, **Source**, and **Connection status** columns for those servers are updated with the results.

If a server is disabled, the values in the **Stratum**, **Source**, and **Connection status** columns are blank. If you re-enable the server (using the toggle in the **Enabled** column), the values in these columns remain blank. However, using the **TEST CONNECTIVITY** option to run the connectivity test restores the current values to these columns.

SET NTP THRESHOLDS (optional)
Specifies threshold settings for suppressing the generation of hardware and operating system messages that are related to changes in the NTP server stratum level or source ID. Operating system messages are only generated if the operating system supports posting of messages to notify customers of STP related hardware messages. Setting the NTP thresholds is optional.

To set the NTP threshold values for a server, click **SET NTP THRESHOLDS**. On the **Set NTP Thresholds** window, specify values for the following options.

Stratum level threshold
Indicates the NTP server stratum level that must be reached before a hardware and operating system message is generated.

Using the **Stratum level threshold** drop-down list, select the stratum level threshold value to indicate the NTP server stratum level that must be reached before a hardware and operating system message is generated. The threshold can be set as low as 2 and as high as 15.

If 2 is selected and the External Time Source (ETS) NTP stratum level changes from 1 to 2, hardware and operating system messages are generated.

If 7 is selected and the ETS NTP stratum level changes from 3 to 4, which is typical of a polling NTP server, no hardware or operating system messages are generated.

If 7 is selected and the ETS NTP stratum level changes from 3 to 11, which is typical of an NTP server losing its time source, hardware and operating system messages are generated.

Source ID time threshold
Indicates the amount of time that must pass before a change in the source ID generates a hardware and operating system message.

Using the **Source ID time threshold** drop-down list, select the source ID time threshold value to indicate the amount of time that must pass before a change in the source ID generates a hardware and operating system message. The messages are issued if the source ID does not return to the original value within the specified time period. If **0 hours 0 minutes** is selected, the messages occur immediately upon detecting a source ID change. The threshold can be set as low as **0 hours 0 minutes** and as high as **24 hours 0 minutes** hours, in increments of one half hour.

If 1 hour is selected, and the ETS stratum-1 source ID changes from GPS to FLY and then back to GPS within the hour time period, no hardware or operating system messages are generated.

If 1 hour is selected, and the ETS stratum-1 source ID changes from GPS to FLY and does not turn back to GPS within the hour time period, hardware and operating system messages are generated.

After selecting values for the **Stratum level threshold** and **Source ID time threshold** options, do one of the following.

- To apply the changes, click **APPLY**.
- To return to the "Verify Network Time Protocol servers" window, click **CANCEL**.
- To restore the values in the **Set NTP Thresholds** window to the defaults, click **RESET**.

RESET
Restores the values in the "Verify Network Time Protocol servers" window to the original values.

3. After verifying the NTP server, do one of the following.
   - To go to the next step, click **NEXT**.

     If the specified NTP servers have the same addresses, the "System duplicate ports" message window opens. Do one of the following.

     – Click **CONTINUE** to apply the changes and go to the next step.
     – Click **CANCEL** to return to the "Verify Network Time Protocol servers" window.
   - To return to the Choose External Time Source window, click **BACK**.

Verify ETS Selections (PTP only)

Use the **Verify Precision Time Protocol interface** window to verify the PTP interfaces.

ATTENTION:

With the added option of utilizing Precision Time Protocol (PTP) as an External Time Server for STP, the network administrator needs to understand the requirements for use of PTP within their IPV4 or IPv6 enterprise information system environment.

The IBM Z PTP implementation adheres to the *Enterprise Profile for the Precision Time Protocol With Mixed Multicast and Unicast Messages* as defined by the Internet Engineering Task Force.

This profile utilizes the End-to-end (E2E) delay measurement mechanism. With this configuration, the corresponding PTP grandmaster servers are expected to operate according to the Enterprise Profile requirements. The IBM Z implementation places an additional requirement that unicast Delay Request and Delay Response Messages, sometimes referred to as the hybrid E2E option, are enabled at the grandmaster.

Corresponding switches and routers in the pathways between the Support Element and the PTP grandmaster server(s) will need to be configured to permit multi-cast and unicast UDP ports 319 and 320, PTP Sync and PTP General message packets, respectively, to ensure proper transmission of PTP packets.

ATTENTION:

The Ethernet interfaces (adapters) that are used with PTP are **em3** and **em4**. If you are using both interfaces to access separate PTP networks, you might need to make changes to the Support Element (SE) routing table.

PTP grandmaster servers send multicast announce messages to potential PTP clients. After a potential PTP client receives an announce message, it sends a request back to the PTP grandmaster using unicast. When these unicast messages leave the SE, they must go over the appropriate Ethernet interfaces to establish the PTP message flow. In most cases, the SE management communications are routed through the **em3** interface, by default. As a result, if a PTP client expects to send unicast requests to the PTP grandmaster using the **em4** interface, you must update the SE routing table to direct those messages through the **em4** interface. Likewise, if the **em4** interface is used by default, and the PTP client expects to send unicast requests using the **em3** interface, you must update the routing table so that the **em3** interface is used.

Before you make the SE routing table changes, you need to know the addresses of all PTP grandmasters that will be the target of communication through the non-default interface. Also, you need to determine whether to target PTP grandmasters by their IP address and/or by the subnet mask in which they reside. If you need to specify several PTP grandmasters and/or subnets, you must add multiple route entries. This ensures that all PTP grandmasters that need to communicate over the non-default interface can do so. When specifying the route entries, you must also provide the gateway address that is accessible for the non-default interface.

To update the SE routing table, do the following:

1. Open the HMC **Customize Network Settings** task.
2. Select the **Routing** tab.
3. Under the Static Routes table, click **New**.
4. Provide information on the Route Entry display for the new entry. Do one of the following:
   - If the PTP grandmaster's IP address is being targeted, do the following:
     a. In the **Type** field, specify **Host**.
     b. In the **Destination** field, specify the PTP grandmaster address.
     c. In the **Adapter** field, specify the non-default adapter (interface).
   - If the PTP grandmaster's subnet is being targeted, do the following:
     a. In the **Type** field, specify **Net**.
     b. In the **Destination** field, enter the TCP/IP address of the PTP grandmaster subnet. Note that the value you specify here must complement the value specified in the **Subnet Mask** field.
     c. In the **Subnet Mask** field, enter the subnet mask of the PTP grandmaster subnet. Note that the value you specify here must complement the value specified in the **Destination** field.
     d. In the **Gateway** field, specify the non-default gateway address.
     e. In the **Adapter** field, specify the non-default adapter (interface).
5. Repeat the steps above to establish route entries for each PTP grandmaster and/or subnet.
6. After all route entries have been added, click **OK**. Accept the reboot prompt to activate the changes. After the SE returns from the reboot, the routing changes will be in place to allow for proper PTP synchronization.

When the **Verify Precision Time Protocol interface** window opens, a PTP connectivity test is run, which queries the status of enabled interfaces. The **Testing PTP connectivity** message window is displayed, which indicates the progress of the test. When the test completes, one of the following messages is displayed.

- If the test is successful, the "Connectivity test successful" message is displayed. Click **OK**.
- If the test is not successful, the "Connectivity test failed" message is displayed. Click **OK**.

1. Use the table and other options in the **Verify Precision Time Protocol interface** window to verify the PTP interfaces. The table displays the following details for the configured PTP interfaces. A maximum of two interfaces are included in the table for each system. The *Preferred* PTP interface is displayed in the first row and the *Secondary* PTP interface (if applicable) is displayed in the second row.

   Enabled
   Displays a switch that indicates whether the PTP interface is enabled or disabled. When the position of the switch is to the right, the interface is enabled. When the position of the switch is to the left, the interface is disabled. To disable or enable a PTP interface, click (select) the switch until it is in the appropriate position.

   Ethernet Interfaces
   Displays the names of the Ethernet interfaces of the systems that you specified in "Step 1: Select System" on page 1026. The name is displayed regardless of whether an interface is enabled or disabled.

   PPS Ports (is displayed for PTP with PPS only)
   Indicates the PPS port that is associated with the server.

   Note: This column is only displayed in the table if you selected **Use PTP with pulse per second (PPS)** as the External Time Source.

   PTP Grandmaster ID
   Indicates the identifier of the grandmaster, which is a derivative of the MAC address.

   Connection status
   Indicates the current status of the connection to the grandmaster clock. The status in this field can be either **Connected** or **Error**.

   Connected
   The timing sequence to the Grandmaster ID is connected.

   Error
   The timing sequence to the Grandmaster ID is paused or disconnected.

   When the connection status is **Error**, you can get more detailed information by clicking the caret to the right. The table row for this interface expands and displays the following information.

   Possible status messages include:

   Success

   Explanation:
   Access to the PTP network was successful.

   Action:
   None.

   PTP connection started

   Explanation:
   The PTP interface detected a grandmaster in the PTP network. The interface will take a few seconds to start following the time of the PTP network.

   Action:
   Click **TEST CONNECTIVITY** to re-query the connection. If the problem persists, contact the next level of support.

   PTP connection not complete

   Explanation:
   The PTP interface did not detect a PTP network.

   Action:
   Either there is an issue with the PTP connections to the interface or the interface needs time to connect to the network. Click **TEST CONNECTIVITY** to re-query the connection. If the problem persists, check the connections to make sure that they support PTP on the path to the potential grandmasters. When the issue is found and fixed, click **TEST CONNECTIVITY** to check the connection changes.

PTP connection not complete

Explanation:
The interface does not appear to be connected to a proper PTP network.

Action:
Verify that the connections to the interface all support PTP, and that the PTP server is connected directly or indirectly to the interface. If a problem is found, fix the issue and click **TEST CONNECTIVITY** to check the connection changes.

PTP connection not complete

Explanation:
The PTP interface is listening to the PTP network, or the interface does not appear to be connected to a proper PTP network.

Action:
Click **TEST CONNECTIVITY** to re-query the connection. If the problem persists, verify that the connections to the interface all support PTP and that the PTP server is connected directly or indirectly to the interface. If a problem is found, fix the issue and click **TEST CONNECTIVITY** to check the connection changes.

PTP connection not complete

Explanation:
The PTP interface is beginning to follow the PTP network.

Action:
Click **TEST CONNECTIVITY** to re-query the connection. If problem persists, contact next level of support.

PTP interface error

Explanation:
PTP interface fault detected.

Action:
The interface is not receiving PTP signals from the network. Either there is a switch that does not support PTP or there are no boundary clocks to be grandmaster. Examine your network to make sure that the network has switches that all support PTP and that the main timeserver is properly configured to be a PTP grandmaster. If the problem persists, contact the next level of support.

PTP interface not found

Explanation:
The PTP interface was not found.

Action:
Contact the next level of support.

PTP error

Explanation:
An undefined error was returned while accessing the PTP interface.

Action:
Click **TEST CONNECTIVITY** to re-query the connection. If the problem persists, contact the next level of support.

2. If applicable, click the **TEST CONNECTIVITY** option of the **Verify Precision Time Protocol interface** window to query the status of enabled PTP Ethernet interfaces. Using **TEST CONNECTIVITY** is optional, but recommended.

   After clicking **TEST CONNECTIVITY**, the "Testing NTP connectivity" message window is displayed, which indicates the progress of the test. When the test completes, the values in the table for the enabled PTP Ethernet interfaces are updated and one of the following messages is displayed.

   - If the test is successful, the "Connectivity test successful" message is displayed. Click **OK**.

- If the test is not successful, the "Connectivity test failed" message is displayed. Click **OK**.

3. After verifying the PTP interfaces, do one of the following.
   - To go to the next step, click **NEXT**.
   - To return to the **Choose External Time Source** window, click **BACK**.

Step 4: Choose Preferred ETS Selection

The process of verifying External Time Source selections is different, depending on whether the ETS is an NTP server or PTP interface. Refer to the appropriate section in this help topic:

- If you specified **NTP** or **NTP with Pulse Per Second (PPS)** in “Step 2: Choose External Time Source” on page 1027, refer to “Choose Preferred ETS Selection (NTP only)” on page 1038.
- If you specified **PTP** or **PTP with Pulse Per Second (PPS)** in “Step 2: Choose External Time Source” on page 1027, refer to “Choose Preferred ETS Selection (PTP only)” on page 1038.

Choose Preferred ETS Selection (NTP only)

Use the **Choose the preferred NTP server** window to select the preferred NTP server. The IP addresses of the servers that you configured in the previous step are displayed for selection.

To choose the preferred NTP server, do the following.

1. Select the IP address of the server that you would like to designate as the preferred server.
2. After selecting a server, do one of the following.
   - To go to the next step, click (select) **NEXT**.
   - To return to the "Verify Network Time Protocol servers" window, click **BACK**.

Choose Preferred ETS Selection (PTP only)

Use the **Choose the preferred PTP Ethernet interface** window to select the preferred PTP Ethernet interfaces. The names of the Ethernet interfaces that you configured in the previous step are displayed for selection.

To choose the preferred PTP Ethernet interface, do the following.

1. Select the PTP interface that you would like to designate as the preferred interface.
2. After selecting the interface, do one of the following.
   - To go to the next step, click (select) **NEXT**.
   - To return to the "Verify Network Time Protocol servers" window, click **BACK**.

Step 5: Confirm Changes

Use the "Confirm External Time Source configuration" window to confirm your External Time Source configuration changes.

1. Review the information on the "Confirm External Time Source configuration" window. If you chose **NTP**, **NTP with PPS**, or **None** as the External Time Source, this window provides information in the following areas:
   - **Selected system**
   - **External Time Source (ETS)**
   - **Verified ETS information**
   - **Preferred ETS server/interface**
   - **NTP thresholds**

   If you chose **PTP** or **PTP with PPS** (pulse per second) as the External Time Source, this window provides information in the following areas:

- **Selected system**
- **External Time Source (ETS)**
- **Verified ETS information**
- **Preferred ETS server/interface**

Each of these areas displays both **New** configuration details (the changes you just made) and the **Previous** configuration details (the configuration settings that existed before you started this action).

To change a **New** configuration setting, click (select) the **Edit** link within the appropriate area. This link returns you to the associated step and window, where you can make the necessary changes.

2. After reviewing the configuration information and, if needed, making changes, do one of the following.
   - To apply the External Time Source configuration changes, click **APPLY**. If the configuration changes are successful, the "The External Time Source (ETS) configuration was saved successfully" window is displayed. Click **CLOSE** or, to configure another External Time Source, click **CONFIGURE ANOTHER ETS**. If you choose to configure another ETS, you will return to the "Select a system to modify its External Time Source" window (“Step 1: Select System” on page 1026).
   - To return to the previous step, click **BACK**.

Deconfigure CTN

The **Deconfigure CTN** action guides you through the process of deconfiguring (removing the roles of) the Preferred Time Server (CPC), Backup Time Server (CPC), and Arbiter of a CTN.

Note the following limitations for using the **Remove systems from CTN** action.

- You cannot deconfigure a CTN when CTN membership restrictions are in effect. If you open the **Deconfigure CTN** action while CTN membership is restricted, the "The members of this CTN are restricted" window opens to warn you, and gives you the opportunity to remove the restrictions. For more information, see “The members of this CTN are restricted window” on page 1047.
- While two CTNs are in the process of merging (**Join existing CTN** action), you cannot deconfigure either of those CTNs.

Note: You cannot deconfigure a CTN when CTN membership restrictions are in effect. If you open the **Deconfigure CTN** action while CTN membership is restricted, the "The members of this CTN are restricted" window opens to warn you, and gives you the opportunity to remove the restrictions. For more information, see “The members of this CTN are restricted window” on page 1047.

IMPORTANT: The **Deconfigure CTN** action results in the loss of the clock source for all servers in the CTN, causing all servers to become unsynchronized. This action is disruptive to all z/OS images that need time synchronization. Therefore, the **Deconfigure CTN** action must be used with extreme caution, and only if absolutely required.

To reestablish a deconfigured CTN, use the **Setup new CTN** action to reassign the roles, verify or set the leap second and time zone data, and set the time on the CTS for the CTN.

After you select the **Deconfigure CTN** action, the **Disruptive Task Confirmation: Deconfigure** window opens.

The Disrupted Partitions table provides the following information about each of the partitions that will be disrupted when the CTN is deconfigured.

Name
Identifies the name of the partition.

System
Identifies the system that contains the partition.

Status
Identifies the current status of the partition.

OS Name
Identifies the operating system name that is associated with the partition.

To confirm that you understand that deconfiguring the CTN is disruptive to the active partitions (which are shown in the table), do the following. If you do not wish to provide confirmation for any of the partitions in the table, click (select) **CANCEL** to close the **Deconfigure CTN** action.

1. For a partition that you want to confirm, note the value that is displayed in the **Name** and **OS Name** columns. Type the exact value for either the **Name** or **OS Name** into the **Confirmation text** field (or use copy and paste). Do this for each partition that you want to confirm. The **Name** and **OS Name** values are case-sensitive. If an **OS Name** value does not exist, then use the **Name** value instead.
2. In the **Password** field, type the user password. The user password is determined in the **User Management** task.
3. After you provide the confirmation text and user password, do one of the following.
   a. To confirm that you want to deconfigure the specified partitions, click **APPLY** (or press the **Enter** key).

      After you click **APPLY**, the Deconfiguring CTN window opens, which indicates the progress of the change. When the change is complete, one of the following messages is displayed.

      - If the deconfigure action is successful, the "CTN deconfigured successfully" message window is displayed. Click **DONE**.
      - If the deconfigure action is not successful, the "Deconfiguring the CTN failed" message window is displayed. Click **DONE**.

   b. To close the **Deconfigure CTN** action without confirming any of the partitions, click **CANCEL**.

Export CTN data

The **Export CTN data** action guides you through the process of saving CTN data to a Microsoft Excel spreadsheet (.xls file).

Note: If you start the Manage System Time task from a local HMC, you do not have access to the HMC file system and are not able to retrieve the exported file. As a result, the **Export CTN data** action is not available from a local HMC. In this case, the "Export CTN data (.xls) is unavailable" window is displayed. Click **CLOSE**. To export the spreadsheet, create a remote connection to the HMC using a web browser, open the **Manage System Time** task, then select the **Export CTN data** STP action.

After you select the **Export CTN data** action, the "Exporting CTN data" window opens, which indicates the progress of the export operation.

When the export is complete, the "CTN data exported to .xls" window is displayed. Do one of the following.

- To retrieve the exported file, click **DOWNLOAD**. The file is stored in the folder that is specified in your web browser settings.
- To cancel the export, click **CANCEL**. The spreadsheet file is not retained.

The name of the exported file is in the following format.

```
<CTNID>_CTN_Export_yyyy-mmm-dd_hh-mm-<AM/PM>.xls
```

For example, an exported file might be named the following.

```
System01_CTN_Export_2016-Sep-20_02-23-PM.xls
```

The spreadsheet contains the following columns of information about the CTN.

CTN ID
Displays the name of the current CTN

Membership
Indicates whether membership in the current CTN is restricted (**Restricted CTN**) or unrestricted (**Unrestricted CTN**)

Time
Displays the time for the Current Time Server (CTS)

Date
Displays the date for the Current Time Server

Time Zone
Displays the time zone for the Current Time Server

Status
Indicates the overall health of the CTN 's configuration

Modify assigned server roles

The **Modify assigned server roles** action guides you through the process of reassigning the roles of the servers within a Coordinated Timing Network (CTN).

Note the following limitations for using the **Modify assigned server roles** action.

- You cannot modify assigned server roles when CTN membership restrictions are in effect. If you open the **Modify assigned server roles** action while CTN membership is restricted, the "The members of this CTN are restricted" window opens to warn you, and gives you the opportunity to open to remove the restrictions. For more information, see “The members of this CTN are restricted window” on page 1047.
- While two CTNs are in the process of merging (**Join existing CTN** action), you cannot modify assigned roles any of the servers within either of those CTNs .

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Note the following:

- At a minimum, the Preferred Time Server (PTS) and the Current Time Server (CTS) must be assigned. In most cases, the PTS is also the CTS.
- Assigning server roles is a global change to the CTN (the changes are propagated throughout the CTN).
- Any server that is assigned a role requires connectivity through coupling links, to all other servers with roles in the CTN.

Step 1: Choose PTS

Use the **Choose Preferred Time Server** window to select the system that will become the Preferred Time Server (PTS) for the CTN. The systems that are available for role assignment are displayed in the window. Each system is represented by a rectangle and is labeled with its system name.

Just above the display of systems is a list of the **Current role selections**. This list shows each role in the CTN and the system that is assigned to it. It also displays the date on which the role assignments for the CTN were last modified.

1. Click (select) the system that you want to assign as the PTS. When you click a system, it changes color to indicate that it is selected.
2. After selecting a system, do one of the following.
   - To go to the next step, click **NEXT**.

     In some cases, the following warning message is displayed.

     Selection exceeds the maximum stratum limit
     This occurs when the system you specified causes the CTN to have at least one system that is too far from the Current Time Server and, therefore, will not be in a synchronized state. Click **CLOSE** to return to the **Choose Preferred Time Server** window.
   - To close the **Modify assigned server role** action, click **CLOSE**.

Step 2: Choose BTS

Use the Choose Backup Time Server window to select the system that will become the Backup Time Server (BTS) for the CTN. The systems that are available for role assignment are displayed in the window.

Each system is represented by a rectangle and is labeled with its system name. Systems that are assigned to other roles are displayed as unavailable.

Just above the display of systems is a list of the **Current role selections**. This list shows each role in the CTN and the system that is assigned to it. It also displays the date on which the role assignments for the CTN were last modified.

Note: If the CTN has only one member, the **Choose BTS** and **Choose Arbiter** steps are skipped. Instead, you will proceed to the **Choose CTS** step.

The **Previous Selections** area, in the lower right corner of the window, displays the system name of the Preferred Time Server. After the BTS role is assigned, its system name is displayed here as well.

The Backup Time Server is a stratum 2 server. Its purpose is to take over as the stratum 1 server if the Preferred Time Server fails. Although assigning a BTS is optional, running without one is not advised because the Preferred Time Server becomes a single point of failure in your timing network.

1. Specify your Backup Time Server preference by doing one of the following.
   - If you want to specify a Backup Time Server, click a system to select it. When you click a system, it changes color (dark gray) to indicate that it is selected.
   - If you do not want to configure a Backup Time Server, select the **Do not configure a Backup Time Server** option.

     Note: If you choose not to configure a Backup Time Server, *Not Configured* appears in the **Previous Selections** area after this step is complete.
2. After specifying a Backup Time Server, or choosing not to, do one of the following.
   - To go to the next step, click **NEXT**.

     If you chose not to configure a Backup Time Server, or if the CTN has only two members (a PTS and a BTS), the next step in the **Modify assigned server roles** action, **Choose Arbiter**, is skipped. Instead you will proceed to the **Choose CTS** step.

     If you specified a Backup Time Server, in some cases the following warning messages are displayed.

     BTS is more than one stratum away
     This occurs when the specified BTS is more than one stratum away from the Preferred Time Server, which could affect time accuracy. Either click **CANCEL** to return to the **Choose Backup Time Server** window to select a different system, or click **CONTINUE** to go to the next step.

     Selection exceeds the maximum stratum limit
     This occurs when the system you specified causes the CTN to have at least one system that is too far from the Current Time Server and therefore, will not be in a synchronized state. Click **CANCEL** to return to the **Choose Backup Time Server** window.
   - To return to the **Choose Preferred Time Server** window, click **BACK**.

Step 3: Choose Arbiter

Use the **Choose Arbiter** window to select the system that will become the Arbiter for the CTN. The systems that are available for role assignment are displayed in the window. Each system is represented by a rectangle and is labeled with its system name. Systems that are assigned to other roles are displayed as unavailable.

Just above the display of systems is a list of the **Current role selections**. This list shows each role in the CTN and the system that is assigned to it. It also displays the date on which the role assignments for the CTN were last modified.

Note: If you chose not to configure a Backup Time Server, or if the CTN has only two members, the **Choose Arbiter** step is skipped.

The **Previous Selections** area, in the lower right corner of the window, displays the system names of the Preferred Time Server and Backup Time Server (if applicable). After the Arbiter role is assigned, its system name is displayed here as well.

The Arbiter is optional, but it is recommended if a CTN contains three or more servers and a Backup Time Server is assigned. The Arbiter is a stratum 2 server. Its purpose is to provide additional means for the Backup Time Server to determine whether it should take over as the Current Time Server when unplanned events affect the CTN.

1. Specify your Arbiter preference by doing one of the following.
   - If you wish to configure an Arbiter, click a system to select it. When you click a system, it changes color (dark gray) to indicate that it is selected.
   - If you do not wish to configure an Arbiter, select the **Do not configure an Arbiter** option.

     Note: If you choose not to configure an Arbiter, *Not Configured* appears in the **Previous Selections** area after this step is complete.
2. After specifying an Arbiter (or choosing not to), do one of the following.
   - To go to the next step, click **NEXT**.

     If you specified an Arbiter, in some cases the following warning message is displayed.

     Arbiter is more than one stratum away
     This occurs when the specified Arbiter is more than one stratum away from the Preferred Time Server, which could affect time accuracy. Either click **CANCEL** to return to the **Choose Arbiter** window to select a different system, or click **CONTINUE** to go to the next step.
   - To return to the **Choose Backup Time Server** window, click **BACK**.

Step 4: Choose CTS

Use the **Choose Current Time Server** window to specify the system that will become the Current Time Server (CTS).

The **Previous Selections** area, in the lower right corner of the window, displays the system names of the Preferred Time Server, Backup Time Server (if applicable), and Arbiter (if applicable).

Just above the list of options is a list of the **Current role selections**. This list shows each role in the CTN and the system that is assigned to it. It also displays the date on which the role assignments for the CTN were last modified.

The Current Time Server is the CTN's stratum 1 server. It provides time information to the entire STP-only CTN.

In most cases, the Preferred Time Server is designated as the Current Time Server in an STP-only CTN. However, the Backup Time Server can also be the Current Time Server.

1. Specify the Current Time Server by selecting either the **Preferred Time Server** or **Backup Time Server** option. If a Backup Time Server was not configured, the **Backup Time Server** option is displayed as unavailable.
2. After you select a Current Time Server option, do one of the following.
   - To go to the next step, click (select) **NEXT**.
   - To return to the **Choose Arbiter** window, click **BACK**.

Step 5: Confirm Changes

Use the "Confirm changes" window to view and confirm the server role assignment changes.

1. Review the topology to ensure that the changes you made to the server role assignments created the results that you expected.

   If the new topology contains an error, the system in error is outlined in red, and the **Status** icon on the **Topology toolbar** is displayed in red. For more information, see “Getting information about server or system-specific errors” on page 1021.
2. After reviewing the topology, do one of the following.

- If the topology is correct, click (select) **APPLY** to apply the changes. If the server roles are modified successfully, the "The server roles have been changed successfully" window is displayed. Click **CLOSE**.

  Note: After you click **APPLY**, the topology display is automatically refreshed.

  If you attempt to apply a configuration that is the same as the current configuration, the "There are no changes to be applied" window is displayed. Click **CLOSE** to return to the "Confirm changes" window.
- If the topology is not correct, click **BACK** to return to the **Choose Arbiter** window.

Remove systems from CTN

The **Remove systems from CTN** action guides you through the process of removing one or more systems from a CTN, and then placing the removed systems in a new CTN.

Note the following limitations for using the **Remove systems from CTN** action.

- You cannot remove systems when CTN membership restrictions are in effect. If you open the **Remove systems from CTN** action while CTN membership is restricted, the "The members of this CTN are restricted" window opens to warn you, and gives you the opportunity to remove the restrictions. For more information, see "The members of this CTN are restricted window" on page 1047.
- You cannot use the **Remove systems from CTN** action to remove systems with roles from a CTN. If you try to launch this action for a CTN that contains only systems with roles, the "Unable to remove systems from the CTN" error message is displayed. To remove a roled system, the message instructs you to first use the **Modify assigned server role** action to remove its role assignment.
- While two CTNs are in the process of merging (**Join existing CTN** action), you cannot remove systems from either of those CTNs.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Step 1: Remove Systems from CTN

Use the "Remove systems from Coordinated Timing Network (CTN)" window to select one or more systems to remove from a CTN. Each selectable system is represented in the window by a rectangle and is labeled with its system name.

The systems that are listed in this window do not have roles and are available for removal. Members of the CTN that have roles cannot be removed by using this action. To remove a system that has a role, click (select) **BACK** to exit the **Remove systems from CTN** task, and then open the **Modify assigned server roles** action to remove the role.

To remove one or more systems from a CTN, do the following.

1. Click one or more of the systems that are displayed in the "Remove systems from Coordinated Timing Network (CTN)" window to select them. When you click a system, it changes color to indicate that it is selected.
2. When you are finished selecting systems, do one of the following:
   - To go to the next step, click **NEXT**.

     You cannot remove a system if it will cause other systems to lose their connections to the CTN or exceed the maximum stratum level. In this situation, after you click **NEXT**, one of the following windows is displayed.

     – "Removing systems will cause other systems to lose their timing connection to the CTN"

     – "Removing systems will cause other systems to exceed the maximum stratum level"

     These windows display a warning and a list of the systems (one or more) that are causing the error. In this case, you cannot proceed any further with these systems selected. Click **CLOSE** to return to

the "Remove systems from the Coordinated Timing Network (CTN) window and deselect the systems that are causing the error.

- To close the **Remove systems from CTN** action, click **CANCEL**.

Step 2: Set the CTN ID

After one or more systems are removed from a CTN, the removed systems need a new CTN in which to reside. The purpose of this step is to designate a CTN for the newly removed systems by assigning its CTN ID.

Use the "Set the CTN ID for the systems that will be removed" window to choose a name for the new CTN, as follows.

1. Specify the CTN ID. You can either use the ID of an inactive CTN, or you can create a new CTN ID, as follows. (An inactive CTN is one or more systems for which a CTN ID was previously specified.)

   Note: During a join (merge) operation between two CTNs, you cannot move systems into either of the CTNs that are involved in the join. If a join is occurring when you arrive at this step, the merging CTNs are not available for selection from the **CTN ID** field drop-down list.

   - To set the CTN ID to the name of an inactive CTN, click (select) the **CTN ID** field drop-down list arrow and select an inactive CTN from the list. (All of the CTNs that are included in the drop-down list are inactive.)
   - To create a new CTN ID, do the following.
     a. Click the **CTN ID** field drop-down list arrow and select the **Create new CTN ID** option. After you select this option, the **CTN ID** field changes to allow text entry. **Save** and **Cancel** options are also displayed.
     b. In the **CTN ID** field, type the new name of the CTN. The CTN ID is case-sensitive and can contain one to eight characters. Valid characters are A-Z, a-z, 1-9, and _ (underscore).
     c. To confirm the CTN name change, click **Save** (or press the **Enter** key). Or, if you do not want to create the new CTN ID, click **Cancel**.
2. After you specify the CTN ID, do one of the following.
   - To apply your changes and go to the next step, click **NEXT**.

     If the CTN ID you specified matches the name of an existing active CTN, the "The CTN ID could not be set" window opens to warn you. Click **CANCEL** to return to the "Set the CTN ID for the systems that will be removed" window and set a different CTN ID.
   - To return to the "Remove systems from Coordinated Timing Network (CTN)" window, click **BACK**.

Step 3: Confirm Changes

Use the "Confirm changes" window to confirm that you want to remove the specified systems. The "Confirm changes" window displays the removed systems in their new CTN.

To confirm and apply the changes, do the following.

1. Review the CTN's topology to ensure that the changes you made created the results that you expected. After you review the topology, do one of the following.
   - If the topology is correct, click (select) **APPLY** to apply the changes and go to the next step.
   - If the topology is not correct, click **BACK** to return to the "Set the CTN ID for the systems that will be removed" window.
2. After clicking **APPLY**, the "Remove servers from CTN" disruptive action window is displayed, which warns you about the potential risks of removing systems and requires you to confirm that you want to do so. Go to “Remove servers from CTN disruptive window” on page 1046 for information on using this window to complete the **Confirm Changes** step.

Remove servers from CTN disruptive window

The "Remove servers from CTN" disruptive action window warns you about the potential risks of removing systems and requires you to confirm that you want to do so.

1. Use the following table to review the details about the partitions that will be disrupted when you remove systems.

   Name
   Identifies the name of a partition that will be disrupted when systems are removed.

   System
   Identifies the system that contains the partition that will be disrupted when systems are removed.

   Status
   Identifies the status of the partition that will be disrupted when systems are removed.

   OS Name
   Identifies the associated operating system name of the partition that will be disrupted when systems are removed.

   Note: If the partition is not operating, an **OS Name** is not displayed.
2. Confirm that you want to remove systems for one or more of the disrupted partitions, as follows. If you do not want to provide confirmation for any of the partitions in the table, click (select) **CANCEL** to return to the "Confirm changes" window.

   a. Some users are required to specify confirmation text for each server that is to be removed. In the **User Settings** task, if the system administrator indicated that, for your user ID, confirmation text is required for disruptive actions, the **Confirmation text** field is included in the row for each partition. (So, if the **Confirmation text** field is present, you are required to provide confirmation text, as follows.)

      In the **Confirmation text** field for a partition, type or copy and paste the exact text that is shown in either the **Name** or **OS Name** column. Do this for each partition that you want to confirm. The **Name** and **OS Name** values are case-sensitive. If an **OS Name** value does not exist, then use the **Name** value instead.

   b. Some users are required to specify a password before a server can be removed. In the **User Settings** task, if the system administrator specified that, for your user ID, a password is required for disruptive actions, the **Password** field is included below the table. (So, if the **Password** field is present, then you are required to provide a password, as follows.)

      In the **Password** field, type the user password. The user password is determined in the **User Management** task.
3. After providing the confirmation text and user password, if required, do one of the following.

   - To confirm that you want to apply the changes, click **APPLY** (or press the **Enter** key). If the systems are successfully removed, the "Systems removed from the CTN successfully" window is displayed. Click **CLOSE**.

     Note: When a system is removed from a CTN, the topology display in the main window is automatically refreshed.
   - If you do not want to apply the changes, click **CANCEL** to return to the "Confirm changes" window.

Set CTN member restriction

The **Set CTN member restriction** action guides you through the process of controlling the systems and servers that are allowed to join a CTN.

Restricting membership in a CTN helps you to prevent it from being deconfigured in the event of a power loss or a power-on reset (POR).

Note: CTN membership can be restricted only when the CTN contains a maximum of two servers, and one of those servers is assigned the PTS role, while the other is assigned the BTS role. If the specified CTN is currently unrestricted, and it contains more than two systems, or a system that does not have a role, the

"The CTN cannot be restricted" window is displayed immediately after you select the **Set CTN member restriction** action. For more information about how to use the "The CTN cannot be restricted" window to resolve the issue, see "The CTN cannot be restricted window" on page 1047.

Choose a CTN membership restriction option

To choose a CTN membership restriction option, do the following.

1. Select one of the following options from the "Coordinated Timing Network (CTN) member restriction preferences" window.

   Allow any server to be a member of the CTN
   Select the **Allow any server to be a member of the CTN** option to add servers to this CTN, or to modify its server roles. This is the default option.

   Only allow the servers that are specified below to be members of the CTN
   Selecting this option specifies that a maximum of two systems can be members of this CTN, and those systems must be the CTN's Preferred Time Server (PTS) and the Backup Time Server (BTS). This is also known as a *save configuration* or *bounded* system.

2. After you select a membership restriction option on the "Coordinated Timing Network (CTN) member restriction preferences" window, do one of the following.

   - To apply the changes, click (select) **APPLY**. If you chose **Allow any server to be a member of the CTN**, the "*CTN_name* is now unrestricted" message window is displayed. If you chose **Only allow the servers that are specified below to be members of the CTN**, the "*CTN_name* is now restricted" message window is displayed.
   - To close the **Coordinated Timing Network (CTN) member restriction preferences** window, click **BACK**.

The members of this CTN are restricted window

If you used the **Set CTN member restriction** action to restrict membership in a CTN, you cannot do any of the following:

- Add servers to the CTN
- Remove servers from the CTN
- Deconfigure the CTN
- Modify the roles of the CTN's servers.
- Join existing CTN
- Split to new CTN

If you try to add servers, remove servers, deconfigure a CTN, or modify server roles in a CTN that has restricted membership, the "The members of this CTN are restricted" window opens when you start any of these actions. In this situation, do one of the following.

- To go to the **Set CTN member restriction** action and remove the restriction (change your restriction preference to **Allow any server to be a member of the CTN**), click (select) **CONTINUE**.
- If you prefer not to remove the CTN membership restriction, click **CANCEL** to return to the **Manage System Time** main window.

The CTN cannot be restricted window

The "The CTN cannot be restricted" window is displayed immediately when you select the **Set CTN membership** STP action and the specified CTN's membership includes either of the following.

- More than two servers
- At least one system that has no role.

The "The CTN cannot be restricted" window explains the limitation and provides you with the opportunity to go to the related STP action to make the necessary changes.

If the specified CTN has more than two members, "The CTN cannot be restricted" window opens to warn you. It also provides a link to the **Remove systems from the CTN** action so that you can reduce the number of systems in the CTN to two before returning to the **Set CTN member restriction** action. In this case, do one of the following.

- To go to the **Remove systems from the CTN** action to reduce the number of systems in the CTN to two, click (select) **CONTINUE**.
- To close the **The CTN cannot be restricted** window, click **CANCEL**.

If the CTN includes systems that do not have assigned roles, "The CTN cannot be restricted" window opens to warn you. It also provides a link to the **Modify assigned server roles** action so that you can assign the missing PTS and BTS roles before returning to the **Set CTN member restriction** action. In this case, do one of the following.

- To go to the **Modify assigned server roles** action to assign the missing PTS and BTS roles, click **CONTINUE**.
- To close the **The CTN cannot be restricted** window, click **CANCEL**.

Setup new CTN

The **Setup New CTN** action guides you through the process of configuring one or more STP-enabled servers into an STP-only Coordinated Timing Network (CTN). This process consists of the following basic steps.

- Setting the CTN ID
- Specifying CTN members
- Assigning server roles
- Initializing the time (leap seconds, time zone, date, and time)

When the **Manage System Time** task is started, and there is no active CTN, the "The timing network has not been configured" message is displayed. Click (select) **SETUP TIMING NETWORK** to open the **Setup new CTN** STP action.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Step 1: Set the CTN ID

Use the "Set the Coordinated Timing Network (CTN) ID" window to specify the CTN ID.

All STP-configured systems in a CTN must have the same *CTN ID*. The CTN ID is the identifier name that is used to indicate whether the system is configured to be part of a CTN and, if so, identifies that CTN.

To set the CTN ID, do the following.

1. Provide a name for the CTN. You can either select the name of an existing, but inactive CTN, or you can specify a new name. (An inactive CTN is one or more systems for which a CTN ID was previously specified.)
   - To use the name of an existing CTN, do the following.
     a. Click (select) the down arrow in the **CTN ID** field. A list opens that displays the available CTNs and the **Create new CTN ID** option.
     b. Select a CTN from the list. After a CTN is selected, its name is displayed in the **CTN ID** field.
   - To specify a new name for the CTN, do the following.
     a. Click the down arrow in the **CTN ID** field. A list opens that displays the available CTNs and the **Create new CTN ID** option.
     b. Select the **Create new CTN ID** option. After you select this option, the **CTN ID** field changes to allow text entry. **Save** and **Cancel** options are also displayed.

c. Type a new name into the **CTN ID** field. The CTN ID is case-sensitive and can contain one to eight characters. Valid characters are A-Z, a-z, 1-9, and _ (underscore).

Note: The name that you specify must not be the same as an existing CTN ID.

At this point, if you decide that you do not want to specify a new name for the CTN, click **Cancel**.

d. To apply the changes, click **Save** (or press the **Enter** key).

2. After you specify the name of the CTN, do one of the following.

- To go to the next step, click **NEXT**.

  In some cases, the following warning message is displayed.

  The CTN ID could not be set
  This error occurs when an active CTN that uses the name you specified, already exists. You cannot go to the next step without correcting this error. Click CANCEL to return to the "Set the Coordinated Timing Network (CTN)" window and specify a different name.

- To close the **Setup new CTN** action, click **CLOSE**.

Step 2: Specify CTN Members

Use the "Specify Coordinated Timing Network (CTN) members" window to select one or more systems to add to the CTN. You can select systems that are not configured in a CTN, or systems that are from inactive CTNs. (An inactive CTN is one or more systems for which a CTN ID was previously specified.)

The selectable systems are displayed with their related CTNs. The first group (labeled *Not configured*) includes only systems that are not currently members of a CTN. Each system is represented by a rectangle and is labeled with its system name.

Note: If the CTN ID that you specified in the previous step is the CTN ID of an existing but inactive CTN, the systems that belong to that inactive CTN are automatically selected in the "Specify Coordinated Timing Network (CTN) members" window.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which you are adding systems. As you add systems with roles to the CTN, they are displayed here also. This includes the Preferred Time Server (PTS), the Backup Time Server (BTS), and the Arbiter.

To specify the members of the CTN, do the following.

1. Click (select) one or more systems from any of the CTNs that are displayed in this window, to add them to the new CTN. When you click a system, it changes color (dark gray) to indicate that it is selected.

   If you chose an existing but inactive CTN ID in “Step 1: Set the CTN ID” on page 1048, any systems that belong to that CTN are automatically selected in the "Specify Coordinated Timing Network (CTN) members" window. These systems cannot be removed at this time. If you attempt to deselect any of the preselected systems, a warning message is displayed. You must complete the CTN setup first. Then, to remove a system, use the “Remove systems from CTN” on page 1044 STP action.

2. When you have finished selecting systems, do one of the following.

- To go to the next step, click **NEXT**. If any of the systems you selected are not connected to any of the systems in the current CTN, the "Unable to add systems to CTN configuration" window opens and displays the names of systems that are unconnected to the CTN. To return to the "Specify Coordinated Timing Network (CTN) members" window, click **CANCEL**.
- To return to the "Set the Coordinated Timing Network (CTN) ID" window, click **BACK**.

Step 3: Choose PTS

Use the **Choose Preferred Time Server** window to select the system that will become the Preferred Time Server (PTS) for the CTN. The systems that are available for role assignment are displayed in the window. Each system is represented by a rectangle and is labeled with its system name.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which the Preferred Time Server is being assigned. After the PTS role is assigned, its system name appears here as well.

The PTS is responsible for time synchronization among the servers and systems of the CTN. The PTS is usually the Current Time Server in an STP-only CTN, and automatically becomes the preferred stratum 1 server. The PTS must have connectivity to the Backup Time Server (BTS) and the Arbiter, and to all servers that are planned to be stratum 2 servers.

To choose a Preferred Time Server, do the following.

1. Click (select) a system to designate it as the Preferred Time Server. When you click a system, it changes color (dark gray) to indicate that it is selected.
2. After you select a system, do one of the following.
   - To go to the next step, click **NEXT**.

     In some cases, the following warning message is displayed.

     Selection exceeds the maximum stratum limit
     This occurs when the system you specified causes the CTN to have at least one system that is too far from the Current Time Server and therefore, will not be in a synchronized state. Click **CANCEL** to return to the **Choose Preferred Time Server** window.
   - To return to the **Choose Preferred Time Server** window, click **BACK**.

Step 4: Choose BTS

Use the **Choose Backup Time Server** window to select the system that will become the Backup Time Server (BTS) for the CTN. The systems that are available for role assignment are displayed in the window. Each system is represented by a rectangle and is labeled with its system name. Systems that are assigned to other roles are displayed as unavailable.

Note: If the CTN has only one member, the **Choose BTS** and **Choose Arbiter** steps are skipped. Instead, you will proceed to the **Choose CTS** step.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which the BTS is being assigned. The system name of the Preferred Time Server is also displayed. After the BTS role is assigned, its system name is displayed here as well.

The Backup Time Server is a stratum 2 server. Its purpose is to take over as the stratum 1 server if the Preferred Time Server fails. Although assigning a BTS is optional, running without one is not advised because the Preferred Time Server becomes a single point of failure in your timing network.

The Backup Time Server must have connectivity to the Preferred Time Server and the Arbiter, and to all other stratum 2 servers that are connected to the Preferred Time Server.

To choose a Backup Time Server, do the following.

1. Specify your Backup Time Server preference by doing one of the following.
   - If you want to specify a Backup Time Server, click a system to select it. When you click a system, it changes color to indicate that it is selected.
   - If you do not want to configure a Backup Time Server, select the **Do not configure a Backup Time Server** option.

     Note: If you choose not to configure a Backup Time Server, *Not Configured* appears in the **Previous Selections** area after this step is complete.
2. After you specify a Backup Time Server, or choose not to, do one of the following.
   - To go to the next step, click **NEXT**.

     If you chose not to configure a Backup Time Server, the next step in the **Setup a CTN** action, **Choose Arbiter**, is skipped. Instead you will proceed to the **Choose CTS** step.

     If you specified a Backup Time Server, note that in some cases the following warning messages are displayed.

BTS is more than one stratum away
This occurs when the specified BTS is more than one stratum away from the Preferred Time Server, which could affect time accuracy. Either click **CONTINUE** to go to the next step, or click **CANCEL** to return to the **Choose Backup Time Server** window to select a different system.

Selection exceeds the maximum stratum limit
This occurs when the system you specified causes the CTN to have at least one system that is too far from the Current Time Server and, therefore, will not be in a synchronized state. Click **CANCEL** to return to the **Choose Backup Time Server** window.

- To return to the **Choose Preferred Time Server** window, click **BACK**.

Step 5: Choose Arbiter

Use the **Choose Arbiter** window to select the system that will become the Arbiter for the CTN.

Note: If you chose not to configure a Backup Time Server, or if the CTN has only two members, the **Choose Arbiter** step is skipped.

The systems that are available for role assignment are displayed in the window. Each system is represented by a rectangle and is labeled with its system name. Systems that are assigned to other roles are displayed as unavailable.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which the Arbiter is being assigned. It also displays the system names of the Preferred Time Server and Backup Time Server. After the Arbiter role is assigned, its system name is displayed here as well.

The Arbiter is a stratum 2 server, whose role is to assist the Backup Time Server in determining whether it should take over as the Current Time Server if unplanned events affect the CTN. Configuring an Arbiter is optional, but it is recommended in order to enhance the failure detection and recovery capabilities of the CTN.

An Arbiter can be configured only if a minimum of three systems are included in the CTN, and only if a Backup Time Server is configured.

The Arbiter must have connectivity to the Preferred Time Server and the Backup Time Server, and to all other stratum 2 servers that are connected to the Preferred Time Server.

To choose an Arbiter, do the following.

1. Specify your Arbiter preference by doing one of the following.
   - If you wish to configure an Arbiter, click a system to select it. When you click a system, it changes color (dark gray) to indicate that it is selected.
   - If you do not wish to configure an Arbiter, select the **Do not configure an Arbiter** option.

     Note: If you choose not to configure an Arbiter, *Not Configured* appears in the **Previous Selections** area after this step is complete.
2. After you specify an Arbiter (or choose not to), do one of the following.
   - To go to the next step, click **NEXT**.

     In some cases, the following warning message is displayed.

     Arbiter is more than one stratum away
     This occurs when the specified Arbiter is more than one stratum away from the Preferred Time Server, which could affect time accuracy. Either click **CONTINUE** to go to the next step, or click **CANCEL** to return to the **Choose Arbiter** window to select a different system.
   - To return to the **Choose Backup Time Server** window, click **BACK**.

Step 6: Choose CTS

Use the **Choose Current Time Server** window to specify the system that will become the Current Time Server (CTS).

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which the Current Time Server is being assigned. It also displays the system names of the Preferred Time Server (PTS), Backup Time Server (BTS) (if configured) and Arbiter (if configured).

The Current Time Server is the CTN's stratum 1 server. It provides time information to the entire CTN. The Current Time Server adjusts the Coordinated Server Time (CST) by steering it to the time that is obtained from an external time source.

Only one stratum 1 server can be assigned to a CTN, and it must be either the Preferred Time Server or the Backup Time Server. In most cases, the Preferred Time Server is designated as the Current Time Server in an STP-only CTN.

It is recommended that the Preferred Time Server be designated as the Current Time Server when the configuration is being initialized. Later, if there is a need to reassign the roles, the Current Time Server can be concurrently assigned to the Backup Time Server. This action can be part of a planned reconfiguration of the Preferred Time Server as long as the planned action is not disruptive.

To choose a Current Time Server, do the following.

1. On the **Choose Current Time Server** window, specify whether the Preferred Time Server or the Backup Time Server will also be the Curent Time Server. **Preferred Time Server** is selected by default. If a Backup Time Server is not configured, or if the Preferred Time Server is the only member of the CTN, the **Backup Time Server** option on this panel is displayed as unavailable.
2. After you select a server, do one of the following.
   - To go to the next step, click (select) **NEXT**.
   - To return to the **Choose Arbiter** window, click **BACK**.

Step 7: Set Leap Seconds

Use the "Set leap seconds" window to specify the leap seconds for the CTN.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which the leap second offset is being assigned. It also displays the system names of the Preferred Time Server (PTS), Backup Time Server (BTS) (if configured) and Arbiter (if configured).

Leap seconds adjust the accuracy of UTC time to account for irregularities in the rate of the Earth's rotation. A leap second is inserted between second 23:59:59 of one calendar date and second 00:00:00 of the following date. The International Earth Rotation and Reference Systems Service (IERS) determines when a leap second is required and issues Bulletin C to announce whether a leap second must be added. Since 1972, the IERS scheduled leap seconds for either June 30th or December 31st.

To set the leap seconds for the CTN, do the following.

1. Specify the leap second offset in the **Offset** field in the "Specify leap seconds" window. The current leap second offset value for the NTP server/PTP interface or 0 (zero) is initially displayed in this field.

   When the External Time Server (ETS) is an NTP server or PTP interface, the UTC time information that is obtained from public servers is automatically adjusted for added leap seconds. In this case, unless your company requires time stamps to meet a specific level of accuracy, you can set the offset value to 0.

   You must specify an offset value if your company has legal or contractual requirements for time stamps to be accurate to a specific value, or uses time stamps for time-dependent banking, scientific, or navigational purposes. The offset value must equal the total accumulated number of leap seconds that were announced by the IERS since January 1972. As of January 2017, the total number of leap seconds is 27.

   To determine the correct offset value to enter, go to the IERS website and check Bulletin C for the months since January 2017, and add 1 for each leap second that was inserted since December 2016.
2. After you specify a leap second offset value, do one of the following.
   - To go to the next step, click (select) **NEXT**.
   - To return to the **Choose Current Time Server** window, click **BACK**.

Step 8: Set Time Zone

Use the "Set time zone" window to specify the time zone, daylight saving time offset, scheduled time zone adjustment, and scheduled daylight saving time adjustment for the CTN.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which the time zone is being assigned. It also displays the system names of the Preferred Time Server (PTS), Backup Time Server (BTS) (if configured) and Arbiter (if configured).

To set the time zone, do the following.

1. Use one of the following options to either select or define a time zone.

   Time Zone
   To select a time zone, use the **Time Zone** field. This is a read-only field but it displays a list of supported, selectable time zones. The initial value in this field is either *<Not initialized>* or a previously specified time zone. Click (select) the drop-down list arrow to view them. Each of the supported time zone entries includes a defined offset from UTC and the daylight saving time offset for that entry, if applicable.

   If the time zone you need does not appear in the list, select one of the five user-defined time zones (UD1 to UD5) at the bottom of the list and then click the **Define** option to create the time zone.

   Define
   Use this option to define a time zone and optionally, the automatic clock adjustment algorithms for daylight saving time when the time zone you need is not available in the **Time Zone** drop-down list.

   To create a user-defined time zone, do the following.

   a. Select one of the five user-defined time zones (UD1 to UD5) at the bottom of the **Time Zone** field's drop-down list. After you select a user-defined time zone, the **Define** option becomes available.
   b. Click **Define** to create the time zone. The "Define time zone" window is displayed, which you can use to define the settings for the new time zone.
   c. Go to “Define a time zone” on page 1018, complete the steps there for defining a time zone, then return here (a link is provided).

2. In the "Set time zone" window, use the following options in the "Clock Adjustment for Daylight Saving Time" area to adjust the clock for daylight saving time.

   Daylight saving time offset (hours : minutes)
   Displays the daylight saving time offset of the selected time zone. If a time zone is not specified, or the selected time zone does not have daylight saving time, the offset is 0 (zero).

   Automatically adjust
   To support automatic adjustment of daylight saving time, select **Automatically adjust**.

   If the specified time zone indicates that it supports automatic adjustment of daylight saving time, then this option is selected by default. If a time zone is not specified, or the time zone does not support automatic adjustment of daylight saving time, this option is disabled. If this option is enabled but not selected, you can select **Automatically adjust** to turn on the automatic adjustment of daylight saving time for the CTN.

   Set standard time
   To change to standard time, select **Set standard time**. If the specified time zone does not support automatic adjustment of daylight saving time, then this option is selected by default.

   Set daylight saving time
   To change to daylight saving time, select **Set daylight saving time**.

3. After you set a time zone, do one of the following.

   - To go to the next step, click **NEXT**.
   - To return to the "Set leap seconds" window, click **BACK**.

Define a time zone

Use the "Define time zone" window to define a time zone and optionally, the automatic clock adjustment algorithms for Daylight Saving Time when the desired time zone is not available in the **Time zone** drop-down list.

Note: This help topic assumes that you have already:

- Selected one of the five user-defined time zones (UD1 to UD5) from the bottom of the **Time zone** field's drop-down list
- Selected the **Define** option on either the "Set time zone" or "Adjust time zone offset" windows. If you have not done so, return to “Step 8: Set Time Zone” on page 1053 or Step 1 of “Adjust time zone offset” on page 1016 and select a user-defined time zone and the **Define** option before continuing with these instructions.

To define a time zone, do the following.

1. Use the following fields of the "Define time zone" window to choose the time zone settings.

   Description
   Specifies a description of the algorithm (cannot exceed 80 characters).

   Standard time name
   Specifies an abbreviated description of the time zone while on standard time. This field can contain a maximum of four characters.

   Daylight saving time name
   Specifies an abbreviated description of the time zone while on Daylight Saving Time. This optional field can contain a maximum of four characters.

   UTC offset
   Specifies an offset range from -14 hours to +14 hours. This value is specified in plus or minus hours and minutes.

   Daylight saving time offset
   Displays the Daylight Saving Time offset of the selected time zone. If a time zone is not specified, or the selected time zone does not have Daylight Saving Time, the offset is 0 (zero).

   Define adjustment of clock for daylight saving time
   To request that the algorithms be defined for automatic clock adjustment, do the following.

   a. Select the **Define adjustment of clock for daylight saving time** option (a check mark is displayed). Otherwise, if this option is not selected (a check mark is not displayed) the **Daylight saving time start** and **Daylight saving time end** fields are unavailable, and you cannot specify the algorithms for automatic clock adjustment for Daylight Saving Time.

      If a Daylight Saving Time offset is specified, you must manually switch from standard to Daylight Saving Time. Conversely, if a Daylight Saving Time offset is not specified, you must manually switch from Daylight Saving Time to standard.

   b. Select one of the following **Daylight saving time start** algorithms. The algorithm is used for adjusting the clock to begin Daylight Saving Time.

      Schedule by day of week in month
      To set the clock adjustment for Daylight Saving Time to begin on a specific day in the month (such as the first Sunday in April at 7:00), select **Scheduled by day of week in month**. To see an example of this setting, hover over the question mark icon.

      Schedule by date
      To set the clock adjustment for Daylight Saving Time to begin on a specific day and time (such as March 31 at 22:00), select **Scheduled by date**. To see an example of this setting, hover over the question mark icon.

      Schedule by time of week after a specific date
      To set the clock adjustment for Daylight Saving Time to begin on a specific day of the week after a specific date (such as the first Friday after March 15 at 7:00), select **Scheduled by**

day of week after a specific date. To see an example of this setting, hover over the question mark icon.

Depending on the selection that you made, supply the necessary information in the appropriate date and time fields by using the down arrow to select a value.

c. Select one of the **Daylight saving time end** algorithms. The algorithm is used for adjusting the clock to end Daylight Saving Time.

Schedule by day of week in month
To set the clock adjustment for Daylight Saving Time to end on a specific day in the month (such as the last Sunday in October at 6:00), select **Schedule by day of week in month**. To see an example of this setting, hover over the question mark icon.

Schedule by date
To set the clock adjustment for Daylight Saving Time to end on a specific day and time (such as September 23 at 18:00), select **Schedule by date**. To see an example of this setting, hover over the question mark icon.

Schedule by day of week after a specific date
To set the clock adjustment for Daylight Saving Time to end on a specific day in the month (such as the last Sunday in October at 6:00), select **Schedule by day of week in month**. To see an example of this setting, hover over the question mark icon.

Depending on the selection that you made, supply the necessary information in the appropriate date and time fields by using the down arrow to select a value.

2. After you select the user-defined time zone settings, do one of the following.
   - To create the time zone, select **APPLY**. If the change is successful, the "User-defined time zone saved successfully" window is displayed. Click **CLOSE**.
   - To close the "Define time zone" window, select **CANCEL**.
3. Return to the task from which you accessed the **Define** option. Choose the appropriate link, as follows.
   - If you selected **Define** on the "Adjust time zone offset window", go to Step 2 in “Adjust time zone offset” on page 1016.
   - If you selected **Define** on the "Set time zone" window, go to Step 2 of “Step 8: Set Time Zone” on page 1053.

Step 9: Set Date and Time

Use the "Set date and time" window to initialize the local date and time (TOD) for the CTN.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which the time zone is being assigned. It also displays the system names of the Preferred Time Server (PTS), Backup Time Server (BTS) (if configured) and Arbiter (if configured).

To set the date and time, do the following.

1. Select one of the following methods for setting the date and time.

Use the configured External Time Source to set date and time: *ETS_type*
To access the specified External Time Source (if one is configured), select **Use the configured External Time Source to set the date and time**. This option is selected by default and is the preferred option. Using this option ensures that the Coordinated Server Time matches the time source.

The type of External Time Source that is configured is displayed to the right of this option. An ETS can be configured as **NTP**, **NTP with Pulse Per Second**, **PTP**, **PTP with Pulse Per Second**, or **None**.

If an External Time Source is not currently configured, you can do so by clicking (selecting) **Configure External Time Source**. Clicking this link opens the **Configure External Time Source** action, which guides you through the process of configuring an ETS. As long as the **Configure External Time Source** action is open, the **Setup new CTN** action is in standby mode (you cannot interact with or exit the action). A message window is displayed that explains this and the "Set date

and time" window becomes obscured. Until the **Configure External Time Source** action closes, you cannot continue with the CTN setup. After the **Configure External Time Source** action closes, the "Set date and time" window is refreshed to reflect the new ETS configuration.

Set date and time
To manually set the date and time to specific values, do the following.

a. Select **Set date and time**.

b. Specify the date and time in the **Date** and **Time** fields. The initial value in the **Time** field is from the Support Element (SE) of the server on which the CTN setup is being performed. Use the calendar icon to select the date instead of typing it in the **Date** field.

Modify time by delta to set date and time
To specify a delta value for setting the time, do the following.

a. Select **Modify time by delta to set date and time**.

b. Specify an amount of time by which to change the clock in the **Delta** field. The default value is +00:00:00.000.

The format is plus or minus hours:minutes:seconds.fractions of a second (+/- hh:mm:ss.mmm). A positive number does not require the plus sign (+). You do not need to specify 0 (zero) for the units that you do not need.

For example, to change the clock by -10 seconds, specify -10. To change the clock by 5 minutes and 23 seconds, specify 5:23.

2. After choosing an option for setting the date and time, do one of the following.

- To go to the next step, click **NEXT**.

If you selected the **Use the configured External Time Source to set the date and time** option, but an External Time Source is not configured, the following message is displayed.

There is no External Time Source configured
Do one of the following.

– To configure an External Time Source, click **CONTINUE**. Clicking this link opens the **Configure External Time Source** action, which guides you through the process of configuring an ETS. As long as the **Configure External Time Source** action is open, the **Setup new CTN** action is in standby mode (you cannot interact with or exit the action). A message window is displayed that explains this and the "Set date and time" window becomes obscured. Until the **Configure External Time Source** action closes, you cannot continue with the CTN setup. After the **Configure External Time Source** action closes, the "Set date and time" window is refreshed to reflect the new ETS configuration. .

– To return to the "Set date and time" window, click **CANCEL**.

- To return to the "Set time zone" window, click **BACK**.

Step 10: Confirm Changes

Use the "Confirm changes" window to confirm the topology of the new CTN.

1. Review the new topology to ensure that the choices you made created the results that you expected, then do one of the following.

- If the topology is correct, click (select) **APPLY** to apply the changes. The "Creating CTN" window is displayed, which indicates the progress of the change. If you decide that you do not want to continue creating the CTN, click **CANCEL** to go back to the "Set time and date" window.

If the CTN is set up successfully, the "Coordinated Timing Network setup successfully" window is displayed. Click **CLOSE**.

- If the topology is not correct, click **BACK** to return to the "Set date and time" window.

Note: To deconfigure a CTN, use the **Deconfigure CTN** STP action.

View External Time Source

The **View External Time Source** action guides you through the process of viewing the configuration information of an External Time Source (ETS).

Note: Because you have view only permission, the **Manage System Time** task automatically displays the view only version of the **Configure External Time Source** action. Note the banner at the top of the window, which indicates that you are in view only mode. In view only mode, you are able to view configuration data, but you cannot make any changes.

A **progress bar** is displayed on each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Step 1: Select System

Use the "Select a system to view its External Time Source" window to select the system that is associated with the External Time Source you want to view.

To select a system, do the following.

1. Use the **Select** column in the table to select a system (you can select one). The table provides the following information for each system.

   System name
   Name of the system. If the system has a role in the CTN, the abbreviation for that role is displayed beside the system name.

   ETS
   External Time Source of the system. Possible values are **NTP**, **NTP with PPS** (pulse per second), **PTP**, **PTP with PPS** (pulse per second) and **None**.

   Preferred
   The IP address of the preferred NTP server or PTP interface. If a preferred NTP server or PTP interface is not defined for the system, this field is blank.

   Secondary
   The IP address of the secondary NTP server or PTP interface. Defining two NTP servers or PTP interfaces for each system ensures redundancy. If a secondary NTP server or PTP interface is not defined for the system, this field is blank.
2. After you select a system, do one of the following.
   - To go to the next step, click **NEXT**.
   - To close the **View External Time Source** action, click **CANCEL**.

Step 2: View Configuration

The "View External Time Source configuration" window displays details about the configuration.

1. Review the configuration details for the following areas:

   External Time Source (ETS)

   Displays the External Time Source. The possible values are as follows.

   Network Time Protocol (NTP)
   Specifies that an NTP server is the External Time Source. Up to two NTP servers can be configured for use.

   NTP with Pulse Per Second (PPS)
   Specifies that an NTP server with pulse per second (PPS) is the External Time Source. An NTP server with PPS provides enhanced time accuracy for the CTN. A highly stable and accurate pulse per second (PPS) output from the NTP server, that precisely indicates the start of a second, must be attached to the PPS port of the server in the CTN. One NTP server can be configured to each PPS port.

Precision Time Protocol (PTP)
Specifies that a PTP interface is the External Time Source. Up to two PTP interfaces can be configured for use.

PTP with Pulse Per Second (PPS)
Specifies that a PTP interface with pulse per second (PPS) is the External Time Source. A PTP interface with PPS provides enhanced time accuracy for the CTN. A highly stable and accurate pulse per second (PPS) output from the PTP interface, that precisely indicates the start of a second, must be attached to the PPS port of the server in the CTN. One PTP interface with a pulse per second output can be configured to each PPS port.

None
Specifies that an External Time Source is not used.

Selected system
Displays the system ETS that is being viewed.

Verified ETS information

For NTP or NTP with PPS, the possible values are as follows:

Enabled
Specifies whether the NTP server is enabled or disabled. The possible values are **Enabled** or **Disabled**.

NTP server
Displays the IP or web address of an NTP server. The IP or web address is displayed regardless of whether a server is enabled or disabled.

Stratum
Indicates the accuracy of the time at the NTP time server. A stratum level of 1 indicates that the NTP time server obtains its time directly from a reference time source. A stratum level of *n* indicates that the NTP time server is *n*-1 hops away from the time source.

Source
Displays a short description of the time source for the NTP server. If the NTP server has a **Stratum** of 1, the value that is displayed in the **Source** field is the time source from which the NTP server obtains the time. If the NTP server has a value that is greater than 1, the value that is displayed in the **Source** field is the address of the time source from which the NTP server obtains the time.

Some of the possible source values and their descriptions include:

Local
Uncalibrated local clock

Cesium
Calibrated Cesium clock

Rubidium
Calibrated Rubidium clock

PPS
Calibrated quartz clock or other pulse-per-second source

IRIG
Inter-Range Instrumentation Group

ACTS
NIST telephone modem service

USNO
USNO telephone modem service

PTB
PTB (Germany) telephone modem service

TDF
Allouis (France) Radio 164 kHz

DCF
Mainflingen (Germany) Radio 77.5 kHz

MSF
Rugby (UK) Radio 60 kHz

WWV
Ft. Collins (US) Radio 2.5, 5, 10, 15, 20 MHz

WWVB
Boulder (US) Radio 60 kHz

WWVH
Kaui, Hawaii (US) Radio 2.5, 5, 10, 15 MHz

CHU
Ottawa (Canada) Radio 3330, 7335, 14760 kHz

LORAN-C
LORAN-C radio navigation system

OMEGA
OMEGA radio navigation system

GPS
Global Positioning Service

HBG
Prangins, HB 75 kHz

JJY
Fukushima, JP 40 kHz, Saga, JP 60 kHz

GOES
Geostationary Orbit Environment Satellite

INIT
Initializing

GNSS
Global Navigation Satellite System

Status
Indicates the current status of an NTP time server, or the results of a query to the server. The status in this field can be either **Errors** or **No errors**.

For PTP or PTP with PPS (pulse per second), the possible values are as follows:

Enabled
Specifies whether the PTP Ethernet interface is enabled or disabled. The possible values are **Enabled** or **Disabled**.

Ethernet interface
Preferred Ethernet interface that was chosen when PTP was configured. Possible values are **em3** or **em4**.

PTP Grandmaster ID
Identifier of the grandmaster, which is a derivative of the MAC address.

Status
Indicates the current status of a PTP Ethernet interface, or the results of a query to the interface. The status in this field can be either **Errors** or **No errors**.

Preferred ETS server/interface

Displays either the IP address of the preferred NTP server or the name of the preferred PTP Ethernet interface.

NTP thresholds

Specifies threshold settings for suppressing the generation of hardware and operating system messages that are related to changes in the NTP server stratum level or source ID. Operating

system messages are only generated if the operating system supports posting of messages to notify customers of STP-related hardware messages. Setting the NTP thresholds is optional.

The following fields are included with **NTP thresholds**.

Stratum level threshold
Indicates the NTP server stratum level that must be reached before a hardware and operating system message are generated. The threshold can be set as low as 2 and as high as 15.

If 2 is specified and the External Time Source (ETS) NTP stratum level changes from 1 to 2, hardware and operating system messages are generated.

If 7 is specified and the ETS NTP stratum level changes from 3 to 4, which is typical of a polling NTP server, no hardware or operating system messages are generated.

If 7 is specified and the ETS NTP stratum level changes from 3 to 11, which is typical of an NTP server losing its time source, hardware and operating system messages are generated.

Source ID time threshold
Indicates the amount of time that must pass before a change in the source ID generates a hardware and operating system message.

The messages are issued if the source ID does not return to the original value within the specified time period. If **0 hours 0 minutes** is specified, the messages occur immediately upon detecting a source ID change. The threshold can be set as low as **0 hours 0 minutes** and as high as **24 hours 0 minutes**, in increments of one half hour.

If 1 hour is specified, and the ETS stratum-1 source ID changes from GPS to FLY and then back to GPS within the hour time period, no hardware or operating system messages are generated.

If 1 hour is specified, and the ETS stratum-1 source ID changes from GPS to FLY and does not turn back to GPS within the hour time period, hardware and operating system messages are generated.

2. After reviewing the configuration information, do one of the following.
   - To close the **View External Time Source** action, click **DONE**.
   - To return to the previous step, click **BACK**.

Advanced actions

The following STP actions are available for diagnostics and advanced tasks.

Control Pulse Per Second signal

The **Control Pulse Per Second signal** action guides you through the process of testing a system's PPS signal or diagnosing problems with a pulse per second (PPS) port.

Note: This action can be used only by support system personnel.

Note: If no ports have been configured for any of the servers in the CTN, the **Control Pulse Per Second signal** action is not available from the list of STP actions on the Manage System Time main window.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Step 1: Select Server

Use the "Select the server to test its Pulse Per Second (PPS) signal" window to select a system. (You can select only one system). The table displays the following details for each system in the CTN.

System Name
Identifies the name of the system.

PPS Port 0
If Port 0 is a PPS port, identifies the IP address of the NTP server or the name of the PTP interface.

PPS Port 1
If Port 1 is a PPS port, identifies the IP address of the NTP server or the name of the PTP interface.

After selecting a system, do one of the following.

- To go to the next step, click (select) **NEXT**.
- If you do not want to continue, click **CANCEL** to close the **Control Pulse Per Second signal** action.

Step 2: Control PPS Signal

Use the "Control Pulse Per Second (PPS) signal" window to set the following options for the ports in the selected NTP server or PTP interface. This window displays whether PPS signals are detected at a PPS port, allows internal diagnostics to be run on each port, shows when a port has been fenced by Licensed Internal Code, and allows a port to be reset.

1. Select one of the following options for Port 0, Port 1, or both.

   Allow PPS port to receive PPS signals from ETS (default)
   When selected, specifies that the port is allowed to receive PPS signals from the External Time Source (ETS). This option is the default.

   The possible values for **PPS pulse status** are shown below. When the **Allow PPS port to receive PPS signals from ETS (default)** option is selected, the **PPS pulse status** can be either **Detected** or **Not Detected**.

   Detected
   Pulse per second signals are being detected on the port from an External Time Source.

   Not Detected
   Pulse per second signals are not being detected on the port from an External Time Source.

   Not Applicable
   The status of the pulse per second signals cannot be shown at this time. The PPS port is fenced or set to perform an internal diagnostic test on the port.

   Note: The port cannot receive PPS signals from the External Time Source when the **Fenced by Licensed Internal Code** option is selected.

   Perform internal diagnostic test on PPS port
   When selected, specifies that you want to test the PPS port. To test the PPS port, do the following.

   a. Select the **Perform internal diagnostic test on PPS port** option.
   b. Click (select) **INTERNAL TEST** to run an internal diagnostic test on the port, which determines whether the PPS hardware is functioning properly.

   Fenced by Licensed Internal Code
   Specifies whether or not the port is fenced by Licensed Internal Code. The **Fenced by Licensed Internal Code** option is available only in PEMODE (pedebug).

   When the port is fenced, it cannot receive PPS signals from the External Time Source (and the port's status is **Not Applicable**). In this case, if you want the port to be able to receive PPS signals from the External Time Source, you must unfence it by deselecting the **Fenced by Licensed Internal Code** option.

2. After selecting an option for one or both ports, do one of the following.
   - To apply the changes, click **APPLY**.
   - To return to the previous step, click **BACK**
3. If you clicked **APPLY**, do one of the following.
   - If you selected the **Allow PPS port to receive PPS signals from ETS** option, the "Updating port status" window is displayed, which indicates the progress of the change. When the update is complete, one of the following message windows is displayed.
     – If the change was successful, the "Port configured successfully" window opens. Click **CLOSE** to return to the "Control Pulse Per Second (PPS) signal" window.

  - If the change was not successful, the "Port configuration changes failed" window opens. Click **CLOSE** to return to the "Control Pulse Per Second (PPS) signal" window.
- If you selected the **Perform internal diagnostic test on PPS port** and **INTERNAL TEST**, the "Internal diagnostic test" confirmation window is displayed. As the "Internal diagnostic test" message instructs you, remove the cable from the PPS input coaxial connector on the appropriate FSP/STP card to enable a proper test. After removing the cable, do one of the following.
  - To confirm that you want to continue with the diagnostic test, click **CONTINUE**.
  - If you do not want to continue with the test, click **CANCEL**.

  If you clicked **CONTINUE** on the "Internal diagnostic test" message window, the following occurs.
  - The port's state changes to **Test** and the **PPS pulse status** changes to **Not Applicable**.
  - The "Running internal diagnostic test" window opens, which indicates the progress of the test.

  When the test is complete, one of the following message windows is displayed.
  - If the test is successful, a "Success" window opens. Click **CLOSE** to return to the "Control Pulse Per Second (PPS) signal" window.
  - If the frequency of the signals that is detected on the port is incorrect, the "Failed - bad frequency" window is displayed. Verify that a cable is not connected to the PPS input coaxial connector on the FSP/STP card. If a cable is connected, remove it and perform the test again. Click **CLOSE** to return to the Control Pulse Per Second (PPS) signal window.

  After running the internal diagnostic test, do the following.

  a. The port's status remains **Test** and the **PPS pulse status** remains **Not Applicable**. To return to the default state and receive PPS signals from the External Time Source, return to the "Control Pulse Per Second (PPS) signal" window, select the **Allow PPS port to receive PPS signals from ETS**, then click **APPLY**.

  b. Reconnect the PPS source cable from the External Time Source to the PPS input coaxial connector on the FSP/STP card.

Join existing CTN

The **Join existing CTN** action guides you through the process of merging the systems of one CTN into another CTN.

Note the following limitations for using the **Join existing CTN** action.

- The current CTN must be active in order to join it with another CTN.
- A coupling link must exist between the CTS of the selected CTN and the CTS of the current CTN.
- While two CTNs are in the process of merging, they cannot join with other CTNs.
- You cannot merge CTNs when membership restrictions for the current CTN are in effect. If you open the **Join existing CTN** action while the current CTN membership is restricted, "The members of this CTN are restricted" window opens to warn you, and gives you the opportunity to remove the restrictions. For more information, see “The members of this CTN are restricted window” on page 1047.
- The clocks of both CTNs must be within one second of each other. However, this should not be an issue with systems that are controlled by an accurate External Time Source.

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Note: After selecting the **Join existing CTN** action, if there are no other CTNs available to join, a message is displayed to warn you. Click **CLOSE** to exit the **Join existing CTN** action and return to the **Topology view**.

Step 1: Select existing CTN

Use the "Select an existing CTN to join" window to select a CTN with which to join (merge). You can select only one CTN.

Before continuing, it is recommended that you review the list of limitations for the **Join existing CTN** action in “Join existing CTN” on page 1062.

Each of the selectable CTNs is displayed with its CTN name and related CTS. Only active CTNs are displayed.

Note: If the **Join existing CTN** action is launched from a different CTN while the two CTNs are merging, the merging CTNs are not available for selection from the "Select an existing CTN to join" window.

To select a CTN, do the following.

1. Click (select) any one of the CTNs that are displayed in this window to identify it as the CTN into which you want to merge the current CTN. When you click a CTN, it changes color (dark gray) to indicate that it is selected.
2. After selecting a CTN, do one of the following.
   - To go to the next step, click **NEXT**.

     If there is no coupling link between the CTS of the selected CTN and the CTS of the current CTN, the "The CTNs cannot be joined" message window is displayed. Click **CLOSE** to return to the "Select an existing CTN to join" window.

Step 2: Confirm changes

Use the "**Confirm changes**" window to confirm that you want to merge the specified CTNs.

1. Review the new topology to ensure that the changes you made created the results that you expected. Above the topology, a line of text is displayed that provides the new CTN's ID.
2. After reviewing the topology, do one of the following.
   - If the topology is not correct, click **BACK** to return to the "**Select an existing CTN to join**" window. The CTN that you chose in Step 1 is no longer selected.
   - If the topology is correct, click (select) **APPLY** to apply the changes. The **Joining CTN** progress message is displayed.

     While the CTNs are merging, they exist in a transitional state until the **Join** operation is complete (until the joining CTN finishes synchronizing its time with the target CTN).

     During this transitional state, the following limitations apply.

     – You cannot make modifications to either CTN.

     – The other STP actions are not available for the merging CTNs, except for **Save STP debug data** and **View Pulse Per Second signal**, and only for users with specific privileges.

     In the **Topology view**, while the two CTNs continue to merge, a banner is displayed at the top of the window for both the current CTN and the CTN to which it is being joined. The banner warns you that the **Join** operation is in progress and includes the following information.

     Estimated time remaining
     Displays the amount of time that remains before the join is complete. Refreshing the topology view updates the displayed time.

     Cancel Join
     Cancels the join operation. The success of the cancel operation depends on how much of the **Join** has already occurred. If you cancel early enough, the **Cancel** is successful and the "Join canceled successfully" message is displayed. However, if you cancel too late in the **Join** operation, the **Cancel** is unsuccessful and the "Join cannot be canceled" message is displayed.

     When the **Join** operation has successfully completed, the message "Join successful" is displayed. Note that after the two CTNs merge, all role assignments of the systems in the new CTN are preserved, while the role assignments of the systems in the current CTN are removed.

Save STP debug data

The **Save STP debug data** action guides you through the process of collecting STP data. When you use this task, a *call-home* is automatically generated in which the debug data is transferred to the support system.

Use the "Save STP debug data" window to collect STP data. This data is collected concurrently. A log is recorded, which causes the STP debug data file to be automatically sent back to the support system.

To save STP debug data, do the following.

1. Specify the scope of STP debugging by selecting one of the following options.

   All systems in the CTN. Select a target system below.
   Select this option to collect STP data from all of the systems in the CTN. Use the drop-down list to select a target system. Although this option is for collecting data from all systems in the CTN, you must still specify a target system. In the drop-down list, a check mark is displayed beside the system that is currently selected.

   Note: The **All systems in the CTN** option can be used only if a CTN includes systems (specifically, the target system) that are capable of a CTN-wide save (HMC/SE Version 2.13.1 or later). Otherwise, the **All systems in the CTN** option is not available.

   Select a single target system in the CTN
   Select this option to collect STP data from a specified target system only. Use the drop-down list to select a target system. In the drop-down list, a check mark is displayed beside the system that is currently selected.
2. After you select a target system, do one of the following.
   - To save the debug data, click (select) **CONTINUE**. The "Saving STP debug data" message is displayed while the data is being saved. If the data is saved successfully, the "STP debug data for *CTN_name* saved successfully" window is displayed. Click **CLOSE**.
   - To close the **Save STP debug data** action, click **CANCEL**.
3. When the "Save STP debug data" window returns, click **DONE**.

Split to new CTN

The **Split to new CTN** action guides you through the process of moving a portion of systems out of a CTN and into a new CTN.

Note the following limitations for using the **Split to new CTN** action.

- You cannot use the **Split to new CTN** action to split systems with roles from a CTN. To split a system with a role from a CTN, click **BACK** to exit the **Split to new CTN** action and then open the **Modify assigned server roles** action to remove its role assignment.
- You cannot split systems to a new CTN when membership restrictions for the current CTN are in effect. If you open the **Split to new CTN** action while the current CTN membership is restricted, "The members of this CTN are restricted" window opens to warn you, and gives you the opportunity to remove the restrictions. For more information, see “The members of this CTN are restricted window” on page 1047.
- While two CTNs are in the process of merging (**Join existing CTN** action), you cannot split systems out of either of those CTNs.
- You cannot split systems from the current CTN to an inactive CTN. (An inactive CTN is one or more systems for which a CTN ID was previously specified.)

A **progress bar** is displayed at the top of each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Step 1: Set CTN ID

Use the "Set the new Coordinated Timing Network's (CTN) ID" window to specify an ID for the new CTN.

Before continuing, it is recommended that you review the list of limitations for the **Split to new CTN** action in “Split to new CTN” on page 1064.

Note: As you begin the **Split to new CTN** action, a dialog window is displayed that tells you to verify that your workloads are balanced appropriately. The reason for this warning is that improperly split workloads might result in divided sysplexes. After verifying that your workloads are balanced properly, click **CONTINUE** to continue with the **Split to new CTN** action.

Before you can split systems out of an existing CTN, you must first create a CTN to receive them. The "Set the new Coordinated Timing Network's (CTN) ID" window allows you to specify the name of that CTN.

Choose a name for the new CTN, as follows.

1. In the **CTN ID** field, type the name of the new CTN. The CTN ID is case-sensitive and can contain one to eight characters. Valid characters are A-Z, a-z, 1-9, and _ (underscore).
2. To apply your changes and go to the next step, click **NEXT**.

Step 2: Specify CTN Members

Use the "Specify CTN members for split" window to select one or more systems to split from the current CTN.

Members of the current CTN that have roles cannot be split to a new CTN by using this action. The systems that are listed in this window do not have roles and are available for splitting. To split a system that has a role from this CTN, click (select) **BACK** to exit the **Split to new CTN** action, and then open the **Modify assigned server roles** action to remove the role.

The current CTN's name is displayed in the **CTN ID** field of the "Select CTN members for split" window. Each of the CTN's selectable systems is represented by a rectangle and is labeled with its system name.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the new CTN (which you specified in the previous step).

To split systems from the current CTN to a new CTN, do the following.

1. Click (select) one or more systems that are displayed in this window to split them to the new CTN. When you click a system, it changes color (dark gray) to indicate that it is selected.
2. When you are finished selecting systems, click **NEXT** to go to the next step.

   If you selected a system that will result in divided sysplexes, the "Identical sysplex names exist" message window is displayed and warns you that the system you selected already has LPARs with the same name. The message window also provides the following information.

   - Above the table, the CTN ID of the current CTN is displayed on the left and the CTN ID of the new CTN (to which the systems will be split) is displayed on the right. When you click either of these CTN names, the table below refreshes to display the information for the selected CTN.
   - The table displays the systems that have duplicate sysplex names and their corresponding LPAR names.

     Note: A system appears in multiple rows in the table if it has more than one sysplex with duplicate LPARs.

   If the "Identical sysplex names exist" message is displayed, do the following.

   a. Click the drop-down icon for each system (or hover over its row in the table) to see more information about the duplicate LPARs.
   b. Verify that your workloads are divided appropriately. Determine whether a sysplex is actually being divided, or if there are merely two sysplexes with the same name.
   c. When you are ready to proceed, click **CONTINUE** to go to the next step.

Step 3: Choose Preferred Time Server (PTS) for the split CTN

Use the "**Choose Preferred Time Server (PTS) for the split CTN**" window to select the system that will become the Preferred Time Server (PTS) for the CTN. The systems that are available for role assignment

are displayed in the window. Each system is represented by a rectangle and is labeled with its system name.

The **Previous Selections** area, in the lower right corner of the window, displays the CTN ID of the CTN to which the Preferred Time Server is being assigned.

Because the PTS is the only role specified, the Current Time Server (CTS) is responsible for time synchronization among the systems in the CTN.

To choose a Preferred Time Server, do the following.

1. Click (select) a system to designate it as the Preferred Time Server (you can choose only one). When you click a system, it changes color (dark gray) to indicate that it is selected.
2. After you select a system, click **NEXT** to go to the next step.

Step 4: Confirm Changes

Use the Confirm Changes window to confirm the topology of the new CTN.

The Confirm Changes window contains the new topology for both CTNs. Immediately above the **Topology view**, two links provide a toggle between the topology of the newly-created CTN and the current CTN. The link on the left is the name of the newly-created CTN and the link on the right is the name of the current CTN. Use these links to preview both views.

1. Review the new topology to ensure that the choices you made created the results that you expected, then do one of the following.
   - If the topology is not correct, click **BACK** to return to the "**Choose Preferred Time Server (PTS) for the split CTN**" window.
   - If the topology is correct, click (select) **APPLY** to apply the changes. The "Creating CTN" window is displayed, which indicates the progress of the change. If you decide that you do not want to continue creating the CTN, click **CANCEL** to go back to the "**Choose Preferred Time Server (PTS) for the split CTN**" window.

     If the CTN is split successfully, the "The CTN split task completed successfully" window is displayed. Click **CLOSE**.

View Pulse Per Second signal

The **View Pulse Per Second signal** action guides you through the process of viewing details about a CTN's Pulse Per Second (PPS) signal.

In general, this action is available only in PEMODE (pedebug) or to a service representative.

A **progress bar** is displayed on each of the windows for this action. As you advance through the steps, the progress bar indicates the name of the step that you are currently performing. You can go back to a previous step by clicking (selecting) its step name on the progress bar. The steps in this help topic reflect the steps that are displayed on the progress bar.

Step 1: Select System

Use the table in the "Select a system to view its Pulse Per Second (PPS) signal" window to select a system. The table contains only systems that are members of the current Coordinated Timing Network (CTN).

To select a system, do the following.

1. Use the **Select** column in the table to select a system (you can select one). The table provides the following information for each system.

   System name
   Identifies the name of the system.

   PPS Port 0
   If Port 0 is a PPS port, identifies either the address of its server (for NTP) or the Ethernet interface name of its server (for PTP). If an NTP or PTP server is not defined for Port 0, this field is blank.

PPS Port 1
If Port 1 is a PPS port, identifies either the address of its server (for NTP) or the Ethernet interface name of its server (for PTP). If an NTP or PTP server is not defined for Port 1, this field is blank.

2. After selecting a system, do one of the following.
   - To go to the next step, click (select) **NEXT**.
   - To close the **View Pulse Per Second signal** action, click **CANCEL**.

Step 2: View PPS Signal

The "Control Pulse Per Second (PPS) signal" window displays details about the PPS signal for the specified system.

1. Review the PPS signal details for the PPS ports of the specified server. This window displays the options that were selected for both Port 0 and Port 1. The options are defined as follows:

   Allow PPS port to receive PPS signals from ETS (default)
   When selected, specifies that the port is allowed to receive PPS signals from the External Time Source (ETS). This option is the default.

   The **Allow PPS port to receive PPS signals from ETS** option is disabled in view-only mode.

   When this option is selected, the **PPS pulse status** is either **Detected** or **Not Detected**.

   Note: The port cannot receive PPS signals from the External Time Source when the **Fenced by Licensed Internal Code** option is selected.

   Perform internal diagnostic test on PPS port
   When selected, specifies that you want to test the PPS port. The **Perform internal diagnostic test on PPS port** option is disabled in view-only mode.

   The **Internal Test** option is used for running an internal diagnostic test on the port to determine whether or not the PPS hardware is functioning properly. The **Internal Test** option is disabled in view-only mode.

   Fenced by licensed internal code
   When selected, specifies that the port is fenced by Licensed Internal Code. The **Fenced by licensed internal code** option is disabled in view-only mode.

   The **Fenced by Licensed Internal Code** option is available only when using the **pedbg** command to collect HMC diagnostic data.

   When this option is selected (the port is fenced), the port cannot receive PPS signals from the External Time Source. In this case, if you want the port to be able to receive PPS signals from the External Time Source, the port must be unfenced (see the **Control Pulse Per Second signal** STP action).

2. After reviewing the Pulse Per Second signal information, do one of the following.
   - To close the **View Pulse Per Second** signal action, click (select) **DONE**.
   - To return to the previous step, click **BACK**.

Manage Web Services API Logs

Accessing the Manage Web Services API Logs task

To view or save the web services API log file:

1. Open the **Manage Web Service API Logs** task. The Manage Web Services API Logs window is displayed.
2. You can make one of the following selections:

- **View Web Services Log**, then click **OK**. The View Web Services Log window is displayed. When you are done viewing the log and ready to exit the task, click **Cancel**.
- **Save Web Services Log**, then click **OK**. The Save File window is displayed. Select the link to save the file to your workstation, then click **OK** to proceed. The windows that follow allow you to indicate where you want to save the log file.

Manage Web Services API Logs

This task allows you to view or download data regarding the API requests that have been made using your Hardware Management Console user ID. This information may be helpful in resolving problems encountered when developing or running Web Services API client applications.

View Web Services Log
To view the Web Services API log, click **View Web Services Log**. The **View Web Services Log** window is displayed. It provides the most recent 1000 lines of log data for requests that have been made using your Hardware Management Console user ID. To return to the previous window, click **Cancel**.

Save Web Services Log
To save, in a separate file, all the available Web Services API log data for requests that have been made using your Hardware Management Console user ID, click **Save Web Services Log**. The **Save File** window is displayed. Select a link if you want to save the log file to your workstation. To continue with the process of saving the file to your workstation, click **OK** and continue with the save procedure.

To return to the previous window without saving the file, click **Cancel**.

OK
To proceed with viewing or saving the Web Services API log, click **OK**.

Cancel
To close this window without viewing or saving the Web Services API logs and to exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Monitor System Events

Accessing the Monitor System Events task for objects the HMC manages

Notes:

- For this task, an SMTP email server must be accessible from the Hardware Management Console. This is because all notifications from this task use email. The SMTP server that is specified cannot be configured to require authentication in order for the Hardware Management Console to connect to it to send the SMTP email.

  The email that is sent comes from the console name and domain name that is identified in the **Customize Network Settings** task. The general format of the "FROM" statement of the email is *console name*_EventMonitor@*console name*.*domain name*. For example, if the *console name* is **HMC1** and the *domain name* is **ibm.com**, then the email is sent from **HMC1_EventMonitor@HMC1.ibm.com**.

  In addition, you might need to update the DNS server that is used by your SMTP server in order for your SMTP server to be able to recognize the Hardware Management Console's email request as being from a valid source. You can refer to documentation related to your DNS server if you need to update your DNS server.

This task allows you to create and manage event monitors. Event monitors listen for events from objects the Hardware Management Console manages. The types of events include:

- State Changes
- Hardware Messages
- Operating System Messages
- Security Log

- Partition[1]
- Processor (CPU)[1]
- Network[1]
- Storage[1]
- Crypto[1]
- Accelerator[1]

Note: [1] These events appear for systems that are DPM enabled.

When an event is received, the monitor tests it with user-defined criteria. If the event passes the tests, the monitor sends email to interested users. The **Monitor System Events** task lets you enable or disable monitors, display or change information about settings such as the SMTP port.

An example of an event monitor you can create is one that listens for hardware messages. You also use the **Monitor System Events** task for pager notification. (Paging services typically support email forwarding to pagers, so no special support for paging is provided.)

An event monitor has the following characteristics:

- Unique name on the Hardware Management Console
- Persistent
- Enabled or disabled without changing its other characteristics
- Listens to one or more managed objects
- Notifies users by email if an event is received from a managed object and it passes through all of the event monitor's filters
- Defines event criteria that the event must match for the monitor to notify users.
- May be limited by time filters, such as the following:
  - A set of days, for example, Monday through Friday
  - A range of times during the day, for example 8 AM through 4 PM
  - A range of dates, for example, 2/14/2005 to 2/16/2005.

To create or change an event monitor:

1. Open the **Monitor System Events** task. The Event Monitor Summary window is displayed.
2. From this window you can:
   - View or change **Settings** information:
     - SMTP server
     - SMTP port
     - Notification delay (seconds).
   - Enable or disable **Monitors** information:
     - Name
     - Description
     - Enabled status.
   - To add, edit, or delete an event monitor, select it in the **Monitors** table and click **Add...**, **Edit...**, or **Delete**, respectively.
   - To test an event monitor for the specified SMTP server, click **Test...**.
3. Click **OK** to exit the task or click **Cancel** to close the task without making changes.

Event Monitor Summary

The **Monitor System Events** task allows you to create and manage event monitors. An *event monitor* listens for events from managed objects. When an event is received, the monitor tests it with user-defined criteria. If the event passes the tests, the monitor enables an email to be sent to interested users.

This window displays the overall configuration of the task and the currently defined event monitors.

SMTP Server
Specify the host name or IPv4 or IPv6 address of a Simple Mail Transfer Protocol (SMTP) server. The SMTP server must be accessible from the Hardware Management Console.

The IPv4 address is written as four decimal numbers, representing the four bytes of the IP address, which is separated by periods (for example, `9.60.12.123`). The IPv6 address can be written as eight groups of four hexadecimal digits, which are separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

Note: For IPv6 simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or you can use a double colon in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

SMTP Port
Specify the SMTP port, the default is 25.

Notification delay (seconds)
Specify a value that is the shortest time in seconds between successive email notifications to any particular email address. You cannot specify shorter than 60 seconds. The default value is 300 seconds.

Monitors list
Following are the types of event monitors:

- State Changes
- Hardware Messages
- Operating System Messages
- Security Log
- Partition[1]
- Processor (CPU)[1]
- Network[1]
- Storage[1]
- Crypto[1]
- Accelerator[1]

Note: [1] These events appear for systems that are DPM enabled.

This table lists the event monitors including a description for each. You can select any event monitor to edit or delete the current information. You can also choose to enable or disable the event monitors.

Additional functions on this window include:

Add...
To create a new event monitor, click **Add...**.

Edit...
To make changes to an existing event monitor, select the event monitor, then click **Edit...**.

Delete
To delete an existing event monitor, select the event monitor, then click **Delete**. After confirmation, this immediately removes the monitor from the listing. It is removed from the system and it is also removed as a listener from any managed objects.

OK
To validate the SMTP settings and to exit this task with the current settings, click **OK**.

Cancel
To exit this task without making any changes, click **Cancel**.

Test...
To test the selected monitor, click **Test...**, where you need to specify the type of event, the object that should generate the event, the event text, and the event time and date.

Note: For DPM monitors, click **Test...**. A message displays, indicating that the email was sent.

Help
To display help for the current window, click **Help**.

Event Monitor Editor

This window allows you to create new monitors and change existing monitors.

Name
Specify an event monitor name if you are creating a new entry, otherwise, this name specifies the event monitor you are currently editing.

Description
Specify a description if you are creating a new entry, otherwise, this description specifies the event monitor you are currently editing. This field is optional and can be left blank.

Type
Select one of the following support event types from the drop-down list:

- State Changes
- Hardware Messages
- Operating System Messages
- Security Log
- Partition[1]
- Processor (CPU)[1]
- Network[1]
- Storage[1]
- Crypto[1]
- Accelerator[1]

Note: [1] These events appear for systems that are DPM enabled.

If any event types do not have corresponding objects to select, those events will be disabled in this window and, therefore, cannot be selected.

Metric
Select the metric items depending on the event type from the drop-down list.

Event targets
Select one or more objects to monitor. The objects in the list will be appropriate for the event types selected in the previous step (3).

For event types that you can select for a DPM-enabled system, additional fields and explanatory text are displayed after the list of event targets.

- For event types with utilization metrics, the additional fields include a utilization threshold and duration that you can specify to trigger the event email. For example, suppose you select the Processor Utilization metric for the Partition event type, then select several partitions in the event targets table, and enter a utilization threshold of 50% for a duration of 5 minutes. The event is triggered when the processor utilization for any selected partition exceeds 50% for at least 5 consecutive minutes.
- For Network event types, the additional fields also include a duration, along with one or more thresholds that are specific to the selected metric. These thresholds specify either transmission rates or the number of dropped or discarded packets. For example:

- Suppose you select the Port Rx/Tx Rate metric, then select several adapters in the event targets table, and enter a rate threshold of 50 MBps, and a duration of 5 minutes. In this example, the event is triggered when, for any selected adapter port, either the receive rate or transmit rate exceeds 50 megabytes per second for 5 consecutive minutes.
- Suppose you select the Port Dropped Packets metric, then select several adapters in the event targets table, and enter a receive threshold of 50 dropped packets, a transmit threshold of 30 dropped packets, and a duration of 5 minutes. In this example, the event is triggered when, for any selected adapter port, either the number of dropped received packets exceeds 50, or the number of dropped transmitted packets exceeds 30, within 5 consecutive minutes.

Event ID range

Enter a message number range pattern that matches with the event message identifiers (for example; 89-93,235,451). Use the monitor value drop-down list for existing number range pattern identifiers. This field displays only for the security log event type selection and is only required if the event text pattern is not defined.

Note: This is not applicable for DPM monitors.

Event text pattern

Select or specify the event text that should cause a notification.

Note: This is not applicable for DPM monitors.

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the drop-down list.

A regular expression is required only if an event ID range is not specified. Comments are allowed and when specified whitespace (blank character) is ignored. For more details see the pound sign (#) special character explanation below.

This field is initially supplied with a set of examples you can choose from and the text filters from each of the currently defined monitors.

The event text may contain special characters which have specific meanings when the regular expression is evaluated. Some of the special characters and examples of each include:

.*

A period followed by an asterisk indicates any number of characters.

For example, **dog.*** would be evaluated as *dog*, *doghouse*, or *dogwood*.

^

A caret as the first character implies that the text that follows must be at the beginning of the line to match.

For example, **^house** would not match *The house on the hill* since *house* is not at the beginning of the phrase.

-->

Two dashes followed by the greater than sign are used to separate the before and after states when used with **State Changes** events. The before state is defined on the left side of the dashes and the after state is defined on the right side of the greater than sign.

For example, **Operating-->Exceptions** would match when the state changed from *Operating* to *Exceptions*.

[*text*]

Text enclosed in brackets implies matching on any of those characters.

For example, **[Ee]xception** matches on *Exception* or *exception*.

\s

A backslash followed by an s indicates a single whitespace character.

For example, **house\scat** is needed to match **house cat** since there is a blank between the two words.

If you specify a comment at the end of the text, then blanks are handled automatically for you. For more details see the pound sign (#) special character explanation below.

#

A pound sign indicates the start of a comment. If the event text contains a pound sign, then when the expression is evaluated the pound sign and all the text that follows is ignored, any leading or trailing blanks around the rest of the expression are removed, and any embedded blanks in the expression are changed to *\s* so the event text will match as desired.

For example, if the event text is **Not Operating-->Operating # From Not Operating state to Operating State**, then the regular expression is evaluated as **Not\sOperating-->Operating**. The comment is ignored and the embedded blanks are respected.

If you need to specify your own entry for the event text and you do not want any of the above processing to occur, then leave out the pound sign and your expression is evaluated as you specified it.

For more detailed information on regular expressions, refer to the documentation on java.util.regex.Pattern class.

Note: If a hardware event was created by problem analysis, the problem description text in the event text will be evaluated. To know whether or not this text will be evaluated you can look at the problem details by opening the **Hardware Messages** task. If the problem details includes a section titled **Problem Description** then that problem description text will be available to be evaluated.

Schedule

Optionally, specify the time, day of the week, and date range the event monitor should be in effect. You can choose to:

- **Limit to times** by specifying or clicking the clock icons to identify the start and end times to take effect
- **Limit to days** by selecting one of more days of the week to take effect
- **Limit to dates** by specifying or clicking the calendar icons to identify the start and end dates to take effect.

Note: The event must satisfy each of the 'limit to' properties to generate notifications. If these properties are not selected the event time is not considered.

Notification list

Select or specify the email addresses that should be notified.

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the drop-down list.

You can specify more than one email address by separating them with a space or comma.

If you are editing an event monitor this field will be supplied with email addresses you had previously specified. You can add to or delete from this list.

The email list optionally ends with a comment defined by all text after the first "#" sign.

Additional functions on this window include:

OK

To continue with the changes you made to an existing event monitor or after creating a new event monitor, click **OK**.

Cancel

To go back to the previous window without making any changes, click **Cancel**.

Help

To display help for the current window, click **Help**.

Test Event Generator

This window enables you to create test events to verify that your monitors are working as expected. The fields are initialized with the information you provided for the selected monitor.

Note: This is not applicable for DPM monitors.

1. What type of event should be generated?

Select the event type that should be generated:

- State Changes
- Hardware Messages
- Operating System Messages
- Security Log

If you initially selected an event type from the previous window this will be the type that will be preselected for you.

If any event types do not have corresponding objects to select, those events will be disabled in this window and, therefore, cannot be selected.

2. What object should generate the event?

Select the single object to be the source of the test event.

If you initially selected an object from the previous window this will be the object that will be preselected for you.

3. What should the event text be?

Specify the text for the test event or choose from a variety of sample messages.

4. What date and time should the event present?

Specify or select, using the icons, the time and date of the test event.

Additional functions on this window include:

Run Test...
To simulate a test event using the current settings of all the enabled monitors and SMTP server, click **Run Test...**.

Cancel
To return to the previous window without testing the enabled monitors and SMTP server, click **Cancel**.

Help
To display help for the current window, click **Help**.

Event Monitor Test Results

This window displays the results of the test events in log format.

Note: This is not applicable for DPM monitors.

The test event is passed to all of the monitors at the Hardware Management Console. If a given monitor has the same type of event as the test event and has as one of its event targets the same object as was selected for the test event, then that monitor is listed in the test results.

If a monitor is enabled, and the event passes all of the monitor's filters, an email is sent. The email includes:

- Indication that this was a test
- Parameters of the test event

- Information about the monitor or monitors that produced a test event.

Note: This window displays the details of the test results regardless of whether any monitor produces a test event.

Additional functions on this window include:

OK
To exit from this window, click **OK**.

Help
To display help for the current window, click **Help**.

Monitors Dashboard

Accessing the Monitors Dashboard task

Use this task to monitor system activity and display activity details for this system(s).

Note: To monitor Dynamic Partition Manager (DPM) enabled systems, select the DPM-enabled system from the navigation pane and select the **Monitor** tab from the workpane table. For more information on using the **Monitor** tab, go to the **Help Table of Contents** > **Tree Style User Interface** > **DPM System Monitoring**.

To monitor system activity for your system:

1. Select one or more systems.
2. Open the **Monitors Dashboard** task. The Monitors Dashboard window is displayed. The overview table includes information on machine type and model, processor and I/O usage, power consumption, and ambient air temperature. Expand the Details section to view activity details for the systems. You can also click on the Details Settings icon for a list of details that are defined for the system to display summaries of processing and channel activity for the this system, expand the Details section for the system you want to monitor.
3. For machines earlier than IBM z13 (z13), select the **Activity**

   icon to display summaries of processor and channel activity for this system and activity details specified in the system activity profiles that are active for the this system. Select the **Customize Activity Profiles**

   icon to work with system activity profiles. The currently active profile defines the activity summaries and details that the **Activity** task displays. In addition, the active profile calculates the Processor Usage and Channel Usage displayed on the **Monitors Dashboard Overview** table.
4. To monitor workload resource groups and policies, select **Open Workloads Report** located above the Overview table.
5. To monitor network metrics and display statistics for the networking resources associated with the IEDN, select **Open Network Monitors Dashboard** located above the Overview table.
6. When you have finished viewing this information, click **Close**.

Monitors Dashboard

Use this window to monitor system activity and display activity details for this system. The activity data is automatically refreshed every 15 seconds. A blank in any table cell means that the data is not supported or not available. This is not considered an error. The local time (last refresh time and time zone) is displayed at the top window.

Note: To monitor Dynamic Partition Manager (DPM) enabled systems, select the DPM-enabled system from the navigation pane and select the **Monitor** tab from the workpane table. For more information on using the **Monitor** tab, go to the **Help Table of Contents** > **Tree Style User Interface** > **DPM System Monitoring**.

Select **Pause Refresh/Resume Refresh** to suspend or resume the automatic refresh of activitydata that is displayed on the current window.

Additional functions on this window include:

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Overview Table

The **Overview** table displays system activity data for this system. The **Overview** table displays the following information:

Name
Displays the names of the CPC.

Status

Displays the current status of the objects. Click the Hardware Messages or Acceptable Status icons in the Status column to display Hardware Message details or Acceptable Status.

Type
Displays the system type.

Machine Type - Model
Displays the machine type - model of the system.

Processor Usage
For systems later than IBM z13 (z13), displays a value that is the simple average of the percentages of processing capacity for ALL the physical processor lines. For systems earlier than z13, displays a value that is a simple average of the percentages of processing capacity for the physical processor lines in the active system activity profile. The processor usage is based on the system activity profile that is active for HWMCA.

Note: For systems earlier than z13, the number and type of physical processor activity lines in the active system activity profile of the CPC determine how meaningful the processing activity summary is. The number and type of channel activity lines in the active system activity profile of the CPC determine how meaningful the processing activity summary is.

I/O Usage
Displays a simple average of the percentages of I/O capacity for ALL the channel lines and adapters in the system.

Note: The value displayed is a simple average of the percentages of I/O capacity for the channel lines in the active system activity profile. The I/O usage is based on the system activity profile that is active for HWMCA.

Power Consumption
Represents the average power consumption of the total system over the last sampled period. The power consumption is displayed in both kilowatts (kW) and Btu per hour (Btu/hr).

Ambient Temperature
Represents the average measured temperature of the air entering the system over the last sampled period. The ambient temperature is displayed in both degrees Celsius (ºC) and degrees Fahrenheit (ºF).

The toolbar at the top of the **Overview** table contains icons to select, filter, and sort the Overview table. If you place your cursor over an icon, the icon description is displayed.

The icons perform the following functions:

Select All
Selects all the systems in the **Overview** table.

Deselect All
Deselects all the systems in the **Overview** table.

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this CSV file into most spreadsheet applications.

Note: This function is available only when you are accessing the Hardware Management Console or Support Element remotely.

Show Filter Row
Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters
Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Edit Sort
Performs multicolumn sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single-column sorting by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
The **Clear All Sorts** icon allows you to return to the default ordering.

Quick Filter
Use the quick filter function to enter a filter string in the Filter input field, and then press Enter to apply the filter. By default all the columns are filtered, showing only rows containing a cell whose value includes the filter text. Clicking the arrow displays a menu that restricts the columns to which the filter is applied.

In addition, the **Select Action** list contains actions that you can perform on the systems in the **Overview** table:

- Select **Set Thresholds** to set system activity thresholds for this system. All systems are used if there is no selection made.
- Select **Start History** to display a histogram view of system activity in various intervals and durations. A histogram is displayed for each system. All systems are used if there is no selection made.
- Select **Export Data** to download the **Overview** table data in a Comma Separated Values (CSV) file. This downloaded CSV file can be imported into most spreadsheet applications.

  Note: This function is available only when you are accessing the Hardware Management Console or Support Element remotely.

Physical processor activity lines (systems earlier than z13)

The number and type of physical processor activity lines in the default system activity profile determine how meaningful the processing activity summary is.

Physical processor activity lines include:

- A physical processor line customized to monitor the average activity of all processors.
- A physical processor line customized to monitor the exact activity of a specific processor.
- A physical processor list customized to monitor the exact activity of one or more of the most active processors.
- A physical processor list customized to monitor the exact activity of one or more of the least active processors.

A processing activity summary bar represents the simple average of all physical processor activity lines in the default system activity profile of the CPC being monitored. A summary bar best represents the average processing activity of the CPC when its default profile includes only a physical processor line customized to monitor the average activity of all processors.

Other types and combinations of physical processor activity lines are permitted in the default profile, but the average activity calculated from those lines may not represent the average activity of all processors in the CPC.

For example, let the default profile include only:

- A physical processor line customized to monitor the exact activity of processor 0 specifically
- Another physical processor line customized to monitor the exact activity of processor 2 specifically

The summary bar for this profile would represent the average processing activity of processors 0 and 2 only.

For another example, let the default profile include only a physical processor list customized to monitor the exact activity of the three most active processors. The summary bar for this profile would represent the average processing activity of the three most active processors only.

Note: If the default profile for a CPC does not include any physical processor activity lines, then the average processing activity is always zero, so the processing activity summary bar never displays.

To display the default profile of a CPC, double-click on or above the CPC activity summary bar to open the window that displays the detailed activity for the CPC.

Channel activity lines (systems earlier than z13)

The number and type of channel activity lines in the default system activity profile determine how meaningful the channel activity summary is.

Channel activity lines include:

- A line customized to monitor the exact activity on a specific ESA/390 channel.
- A channel list customized to monitor the exact activity of one or more of the most active channels.
- A channel list customized to monitor the exact activity of one or more of the least active channels.
- A channel list customized to monitor the exact activity of one or more of the most active channels used by a specific logical partition.
- A channel list customized to monitor the exact activity of one or more of the least active channels used by a specific logical partition.
- A channel list customized to monitor the exact activity of the seven most active channels, **and**
- A channel list customized to monitor the exact activity of the seven least active channels.

Other types and combinations of channel activity lines are permitted in the default profile, but the average activity calculated from those lines may not represent the average activity of all channels used by the CPC.

For example, let the default profile include only:

- An ESA/390 channel line customized to monitor the exact activity of channel path identifier (CHPID) 29 specifically.
- Another ESA/390 channel line customized to monitor the exact activity of channel path identifier (CHPID) 2A specifically.

The summary bar for this profile would represent the average channel activity of CHPIDs 29 and 2A only.

For another example, let the default profile include only a channel list customized to monitor the exact activity of the sixteen most active channels. The summary bar for this profile would represent the average channel activity of the sixteen most active channels only.

Note: If the default profile for a CPC does not include any channel activity lines, then the average channel activity is always zero, so the channel activity summary bar never displays.

To display the default profile of a CPC, double-click on or above the channel activity summary bar to open the window that displays the detailed activity for the CPC.

Details

The Details section is an expandable section that displays activity details for the system. Systems prior to System z9® do not support details. System z9 and System z10 support Power Consumption and Environmental details only.

Starting with the zEnterprise 196, the following Details are supported:

- Power Consumption
- Environmentals
- Aggregated Processors
- Processors
- System Assist Processors
- Logical Partitions
- Channels
- Adapters

You can use the **Details** icon to select Details Settings and open the **Customize Activity Profiles** task and **Activity** task for system earlier than z13:

- Select the **Details** icon to configure the tables for the Monitors Dashboard Details area for this system. All systems are used if there is no selection made.
- Select the **Activity** task icon to open the **Activity** task for systems earlier than z13. This task displays summaries of processor and channel activity for the selected system and activity details specified in the system activity profiles that are active for the system.
- Select the **Customize Activity Profiles** task icon to open the **Customize Activity Profiles** task for systems earlier than z13. Use this task to work with systems activity profiles. The currently active profile defines the activity summaries and details that the **Activity** task displays. In addition, the active profile calculates the Processor Usage and Channel Usage displayed on the Monitors Dashboard Overview table.

You can work with the **Details** tables by using the **Select Action** list from the table tool bar.

Select **Start History** to display a view of system activity in various intervals and durations. A histogram is displayed for each selection made on the **Details** table.

Select **Processor Usage by Key** from the Processors list to display additional processor supervisor and problem states. (Available on systems starting on **z13**)

The following Table Actions are available:

Select All
Selects all objects in the **Details** table.

Deselect All
Deselects all selected objects in the **Details** table.

Export Data
Downloads table data in a Comma Separated Values (CSV) file. This downloaded CSV file can then be imported into most spreadsheet applications.

Show Filter Row
Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters
Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, you can perform single-column sorting by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
Returns to the default ordering.

Quick Filter
Specifies a filter string to apply. Enter string in the **Filter input** field, and then press **Enter** to apply the filter. By default all the columns are filtered, showing only rows containing a cell whose value includes the filter text. Clicking the arrow displays a menu that restricts the columns to which the filter is applied.

Power Consumption

Displays the average power consumption over the last sampled period for the system. The power consumption is displayed in both kilowatts (kW) and Btu per hour (Btu/hr).

Power consumption also displays the line currents for the power cord data in service representative mode.

Power consumption also displays the line currents for the power cord data in service representative mode.

Environmentals

Displays the average ambient temperature humidity, and dew point for the system. The ambient temperature represents the average measured temperature of the air entering the system over the last sampled period. The ambient temperature is displayed in both degrees Celsius (ºC) and degrees Fahrenheit (ºF).

The humidity specifies the amount of water vapor in the air as measured by the system. The humidity sensor gives a reading of the relative humidity of the air entering the system. The recommended long-term relative humidity for a system with an altitude from sea level to 900 meters (2953 feet) is 60%. The range of acceptable relative humidity is 8% - 80%.

The dew point specifies the air temperature in degrees Celsius (ºC) and degrees Fahrenheit (ºF) at which water vapor will condense into water. This is a calculated value based on the current temperature and relative humidity. Cooling the system to the dew point can result in condensation on critical internal parts, leading to equipment failure, unless the computer room environment is adequately maintained to prevent it.

Environmental also displays the air pressure in hectopascal (hPa) in service representative mode.

Aggregated Processors

Displays the aggregated processor usage for each type of physical processor on the system. For each type of processor the table displays the aggregated processor usage for all processors and all shared processors.

Some systems have only general purpose processors, but some systems can have special processors, which can include any combination of the following:

- Integrated Coupling Facility (ICF) processors
- Integrated Facility for Linux (IFL) processors
- zEnterprise Application Assist Processors (zAAPs) (Available only on machines prior to IBM z13 (z13).)
- z Integrated Information Processors (zIIPs)

Processors

Displays the processor usage for each physical processor on the system.

Starting on IBM z13 (z13) simultaneous multithreading (SMT) usage and thread usage displays showing percentage usage of each thread when the processor is running in SMT mode.

Select **Processor Usage by Key** from the Processors list to display the Processor Usage by Key window with additional processor supervisor and problem states. (Available on machines starting on z13)

Processor Usage by Key

This window displays additional data for processor's activity.

Key
Specifies the list of Program Status Word (PSW) keys for the processor. The hexadecimal list is X'0' to X'F'.

Total Usage (%)
Displays the total percentage usage for the processor's activity.

Supervisor State Usage (%)
Displays the supervisor state usage for the processor's activity.

Problem State Usage (%)
Displays the problem state usage for the processor's activity.

Additional functions on this window include:

OK
To close the current window after viewing the information, click **OK**.

Help
To display help for the current window, click **Help**.

System Assist Processors

Displays the processor usage for each System Assist Processor (SAP) on the system.

Logical Partitions

Displays the processor usage for each active logical partition on the system.

Starting on IBM z13 (z13) , the processor usage by processor type displays. Some systems have only general purpose processors, but some systems can have special processors, which can include any combination of the following:

- Integrated Coupling Facility (ICF) processors
- Integrated Facility for Linux (IFL) processors
- z Integrated Information Processors (zIIPs)
- Recovery Boost

Also, displays the z/VM Paging Rate for logical partitions running z/VM V6.1 or later. (Available on machines earlier than z13)

If a logical partition's processing weight is not capped, its processing weight is the *minimum* share of non-dedicated processing resources guaranteed to the logical partition when all non-dedicated processing resources are in use. But when non-dedicated processing resources are available, the logical partition can borrow them, if necessary, in excess of the share ordinarily provided by its processing weight.

The Processor Usage bar range for displaying activity graphically is 0% to 100%. Actual amounts of normalized processing activity that exceed 100% are not displayed on the Processor Usage bar, but the actual processor usage value is displayed and can be greater than 100%.

Channels

Displays the name of the owning logical partition or

```
Shared
```

if the channel is shared across partitions and the channel usage for each channel on the system.

Adapters

Displays the channel assignment, adapter type, and usage for each Crypto , Flash, and RoCE adapter on the system.

Details Settings

Use this window to configure the tables for the **Monitors Dashboard** Details area for this system. Select the tables you want to display and clear the tables you want to hide. The Details Settings are saved for the user ID.

When you start the **Details Settings** task for a single system, the current Details Settings, if any were previously saved, are displayed. Otherwise, all details tables are displayed. When you start the **Details Settings** task for more than one system, then all details tables are displayed and any changes saved are for this system. When you start the **Details Settings** task with no selected system, then all details tables are displayed and any changes saved are for all systems.

Note: The default is to display all details tables.

Power Consumption

Specifies displaying or hiding the **Power Consumption** details.

Environmentals

Specifies displaying or hiding the **Environmentals** details table.

Aggregated Processors

Specifies displaying or hiding the **Aggregated Processors** details table.

Processors

Specifies displaying or hiding the **Processors** details table, which displays the processor usage and simultaneous multithreading (SMT) usage and thread usage (starting on IBM z13 (z13) for each physical processor on the system.

System Assist Processors

Specifies displaying or hiding the **System Assist Processors** details table, which displays the processor usage for each System Assist Processor (SAP) on the system.

Logical Partitions

Starting on z13, specifies displaying or hiding the **Logical Partitions** details table, which displays the processor usage and processor type for each active logical partition on the system. For systems earlier than z13, the table also displays the z/VM Paging Rate for logical partitions running z/VM V6.1 or later.

Channels

Specifies displaying or hiding the **Channels** details table, which displays the name of the owning logical partition or

```
Shared
```

if the channel is shared across partitions and the channel usage for each channel on the system.

Adapters

Specifies displaying or hiding the **Adapters** details table, which displays the channel assignment, adapter type, and usage for each Crypto and Flash adapter on the system.

Additional functions on this window include:

OK
To activate and save the current thresholds, click **OK**.

Reset
To reset the thresholds to the previously saved values, click **Reset**.

Cancel
To close the window without saving changes to thresholds, click **Cancel**.

Help
To display help for the current window, click **Help**.

Dashboard Histogram Display

Use this window to display this system activity data in histogram form. The system activity can be displayed in various intervals and durations dynamically. The usage(%), power (kW or Btu/hr), storage (kBytes/second), or temperature (°C or °F) display on the left side of the histogram and the time intervals display on the bottom of the histogram.

Additional functions on this window include:

Clear
To clear the current histogram displayed and restart data collection, click **Clear**.

Pause
To pause the updating of the current histogram, click **Pause**.

Resume
To resume the updating of the current histogram, click **Resume**.

Export
To download the dashboard histogram data in a Comma Separated Values (CSV) file, click **Export**. This downloaded CSV file can then be imported into most spreadsheet applications.

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Frequency and Duration

Select the time frequency and duration for the system activity data to be displayed by using the down arrow on the entry field. The frequency and duration values are:

- 15 seconds for 1 hour
- 1 minute for 4 hours
- 5 minutes for 12 hours
- 10 minutes for 1 day
- 15 minutes for 2 days
- 1 hour for 10 days

Display Type

Select the type of system activity data to be displayed by using the down arrow on the entry field and selecting the desired data type. Depending on the targeted system details, the system activity display types can be one of the following:

System

- Processor Usage
- I/O Usage
- Power Consumption (kW)
- Power Consumption (Btu/hr)
- Ambient Temperature (°C)
- Ambient Temperature (°F)

Power Consumption

- Power Consumption (kW)
- Power Consumption (Btu/hr)
- Average Voltage
- Line current A
- Line Current B
- Line Current C

Input Air Temperature

- Input Air Temperature (ºC)
- Input Air Temperature (ºF)

Aggregated Processors

- All Processor Usage
- Shared Processor Usage

Processors

- Processor Usage
- Processor Usage by Key

System Assist Processors

- Processor Usage

Logical Partitions

- All Processor Usage
- CP Processor Usage
- IFL Processor Usage
- ICF Processor Usage
- zIIP Processor Usage

Channels

- Total Channel Usage

Adapters

- Total Adapters Usage

Set Thresholds

Use this window to set system activity thresholds for this system. A threshold value of 0 indicates no threshold is set. Depending on the type of threshold set, a warning indicator is displayed when the threshold value is reached. For processor and channel usage, the warning indicator is that the activity bar turns red. For power consumption and ambient temperature, the warning indicator is that the text turns red.

Thresholds are saved for the user ID. When you start the **Thresholds** task for a single system, the current thresholds, if any were previously saved, are displayed. Otherwise, no thresholds are displayed. When you start the **Thresholds** task for more than one system, then no thresholds are displayed and any changes saved are for this system. When you start the **Thresholds** task with no selected system, then no thresholds are displayed and any changes saved are for all systems.

Note: The default is no thresholds are set.

You can set threshold values for the following:

- Processor Usage (0 to 100%)

- Channel Usage (0 to 100%)
- Power Consumption (kW)
- Ambient Temperature (ºC)

Processors Usage
Specifies the threshold value, a percentage of 0-100 %, for the processor usage. After you specify the value, select the threshold type. An **Above** threshold displays a warning indicator when the processor usage value is above the threshold value. A **Below** threshold displays a warning indicator when the processor usage value is below the threshold value.

Channel Usage
Specifies the threshold value, a percentage of 0-100 %, for the processor usage. After you specify the value, select the threshold type. An **Above** threshold displays a warning indicator when the processor usage value is above the threshold value. A **Below** threshold displays a warning indicator when the processor usage value is below the threshold value.

Power Consumption
Specifies the threshold value, in kilowatts, for the power consumption. After you specify the value, select the threshold type. An **Above** threshold displays a warning indicator when the power consumption value is above the threshold value. A **Below** threshold displays a warning indicator when the power consumption value is below the threshold value.

Ambient Temperature
Specifies the threshold value, in degrees Celsius, for the ambient temperature. After you specify the value, select the threshold type. An **Above** threshold displays a warning indicator when the ambient temperature value is above the threshold value. A **Below** threshold displays a warning indicator when the ambient temperature value is below the threshold value.

Additional functions on this window include:

OK
To activate and save the current thresholds, click **OK**.

Reset
To reset the thresholds to the previously saved values, click **Reset**.

Cancel
To close the window without saving changes to thresholds, click **Cancel**.

Help
To display help for the current window, click **Help**.

Network Diagnostic Information

Accessing the Network Diagnostic Information task

This task displays network diagnostic information for the console's TCP/IP connection and allows you to send an echo request (ping) to a remote host.

To view information concerning the networking configuration on this Hardware Management Console:

1. Open the **Network Diagnostic Information** task. The Network Diagnostic Information window is displayed.
2. Use the following tabs to view the network information:
   - Ping
   - Interfaces
   - Ethernet Settings
   - Address
   - Routes
   - Address Resolution Protocol (ARP)

- Sockets
- Transmission Control Protocol (TCP)
- Internet Protocol (IP) Tables
- User Datagram Protocol (UDP)
- DNS
- Native Connections
- Test Support Element Communications (This tab is available only for user IDs with service or access administrator roles.)

3. Click **Cancel** when you are done viewing the information.

Network Diagnostic Information

You can use the console workplace to obtain network diagnostic information about the Hardware Management Console's network protocols. Use this window to access any one of the following *Network Diagnostic Information* tabs:

- Ping
- Interfaces
- Ethernet Settings
- Address
- Routes
- ARP (Address Resolution Protocol)
- Sockets
- TCP (Transmission Control Protocol)
- IP (Internet Protocol) Tables
- UDP (User Datagram Protocol)
- DNS
- Native Connections
- Test Support Element Communications

Cancel
To close this window and cancel the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Ping

Use this page to send an echo request (ping) to a remote host to see if the host is accessible and to receive information about that TCP/IP address or name.

TCP/IP Address or Name to Ping
Specify any TCP/IP address or host name in this field, then click **Ping**. The results for that TCP/IP address or host name are displayed in the page.

Ping
To send a ping command for the TCP/IP address or host name you specified in the field, click **Ping**.

Interfaces

Use this page to display the statistics for the network interfaces currently configured. To update the information that is currently displayed with the most recent information, click **Refresh**.

Ethernet Settings

Use this page to display the settings for the ethernet cards currently configured. To update the information that is currently displayed with the most recent information, click **Refresh**.

Address

Use this page to display TCP/IP addresses for the configured network interfaces. To update the information that is currently displayed with the most recent information, click **Refresh**.

Routes

Use this page to display the Kernel IP and IPv6 routing tables and corresponding network interfaces. To update the information that is currently displayed with the most recent information, click **Refresh**.

ARP

Use this page to display the contents of the Address Resolution Protocol (ARP) connections. To update the information that is currently displayed with the most recent information, click **Refresh**.

Sockets

Use this page to display information about TCP/IP sockets. To update the information that is currently displayed with the most recent information, click **Refresh**.

TCP

Use this page to display information about Transmission Control Protocol (TCP) connections. To update the information that is currently displayed with the most recent information, click **Refresh**.

IP Tables

Use this page to display information (in table format) about the Internet Protocol (IP) packet filter rules. To update the information that is currently displayed with the most recent information, click **Refresh**.

UDP

Use this page to display information about User Datagram Protocol (UDP) statistics. To update the information that is currently displayed with the most recent information, click **Refresh**.

DNS

Use this page to verify a Domain Name Services (DNS) server.

TCP/IP Address to Resolve
Specify a TCP/IP address in this input field, then click **DNS**.

DNS
To provide detailed information for the specified TCP/IP address to resolve, click **DNS**.

Native Connections

Use this page to display all of the native TCP/IP base communication service connections. To update the information that is currently displayed with the most recent information, click **Refresh**.

Test Support Element Communications

Use this page to test Support Element communications from the Hardware Management Console to the Support Element and from the Support Element back to the Hardware Management Console.

If the test is successful a message is displayed indicating a successful completion.

If the test fails a message is displayed indicating which step failed. Possible reasons for the failure include:

- The Support Element is older than Version 2.10.1
- A firewall is preventing data from being received by the Support Element

- A firewall is preventing data from being transmitted back to the Hardware Management Console from the Support Element

Note: This tab is only available for SERVICE or ACSADMIN user IDs or user IDs with service or access administrator roles.

TCP/IP Address of the Support Element
Specify a TCP/IP address of the support element in this field, then click **Test Communications**. The test results for the specified support element appears in this window.

Test Communications
To test communications between the Hardware Management Console and the specified support element, click **Test Communications**. The test results for the specified support element appears in this window.

Network Traffic Analyzer Authorization

Accessing the Network Traffic Analyzer Authorization task

Use this task for the selected OSA-Express or HiperSockets channel to customize or check the current authorization to trace network traffic. This task allows you to select:

- Customize network traffic analyzer settings
- Check current network traffic analyzer authorization.

To customize or check the network traffic analyzer settings:

1. Locate the **CPC** to work with.
2. Locate the OSA-Express or HiperSockets **Channel** you want to work with.
3. Open the **Network Traffic Analyzer Authorization** task.
   - For OSA-Express, the Network Traffic Analyzer Controls window displays.
   - For HiperSockets, the HiperSockets Network Traffic Analyzer Authorization window displays.
4. Depending on the channel type you have selected:
   - For OSA-Express, select the appropriate control task to:
     - *Customize Network Traffic Analyzer Settings...* to set up NTA authorization to allow or disallow the OSA channels from tracing outside of their own partition.
     - *Check current Network Traffic Analyzer authorization...* to allow the Support Element to scan all the OSA channels and report back which OSA channels are authorized for NTA to trace outside its own partition.
   - For HiperSockets, select the network traffic analyzer logical partition and eligible logical partitions that will be authorized to set up, trace, and capture the HiperSockets network traffic.
     - All IQD channels are not authorized to enable HiperSockets NTA
     - This IQD channel is not authorized to enable HiperSockets NTA
     - This IQD channel is authorized to enable, control and capture network traffic from all logical partitions that contain the IQD CHPID that maps to this IQD channel (Caution: This setting will result in tracing all traffic flowing between all the logical partitions using this IQD CHPID. This can result in performance degradation)
     - Customized HiperSockets NTA logical partition authorization list for this IQD channel.
5. Click **OK** to perform the selected operation.

Network Traffic Analyzer Controls

Use this window to select a Network Traffic Analyzer (NTA) control to enable or check the current authorization to trace network traffic. The following selections are available:

- Customize Network Traffic Analyzer Settings...

- Check current Network Traffic Analyzer Authorization...

OK
To continue with the operation, click **OK**.

Cancel
To close the window without saving changes you made, click **Cancel**.

Help
To display help for the current window, click **Help**.

Current Network Traffic Analyzer Authorization

This window displays the current channels that are authorized for the Network Traffic Analyzer to trace outside their own logical partitions.

OK
To close the window and return to the previous window, click **OK**.

Disable the Host Network Traffic Analyzer from tracing outside of the channel's own partition
To disable a channel authorized from the Network Traffic Analyzer tracing outside of the logical partition, select the channel from the above list then select **Disable the Host Network Traffic Analyzer from tracing outside of the channel's own partition**.

Help
To display help for the current window, click **Help**.

OSA-Express Host Network Traffic Analyzer Authorization

Use this window to select the level of authorization for the OSA-Express host network traffic analyzer. The Channel ID, type, and card description are displayed.

Status
You can use the Status table to check or change the single or multi-port network traffic analyzer authorization definitions for the selected channel. Select from the following choices the level of authorization you want for the OSA-Express Host Network Traffic Analyzer.

- Logical Partition - tracing allowed for resources define within the tracing host logical partition (this is the default)
- CHPID - Displays for a single port that allows tracing for all resources defined to this CHPID for all logical partitions sharing this CHPID
- Port - Displays for a multi-port that allows tracing for all resources defined to this port and for all logical partitions sharing this port
- Disabled - All tracing by the Host Network Traffic Analyzer is disallowed.

OK
To apply the changes you made, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize a HiperSockets NTA logical partition authorization List

Use this window to select the NTA logical partitions and eligible logical partitions that will be authorized to setup, trace, and capture the HiperSockets network traffic. To define NTA rules for each logical partition perform the following:

To authorize an NTA logical partition:

1. Click the NTA logical partition that will be authorized to set up, trace, and capture the HiperSockets network traffic.

2. Select the eligible logical partitions to be traced; you are required to select at least one eligible logical partition for authorization.

Only traffic flowing between the selected eligible logical partition or logical partitions is traced.

To remove authorization from a logical partition:

1. Click the NTA logical partition that is currently authorized.
2. Clear all eligible logical partitions.

Repeat the appropriate series of steps for all logical partitions for which the NTA rules need updating. Click **OK** to accept the changes.

OK
To apply the changes you made, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

HiperSockets Network Traffic Analyzer Authorization

Use this window to select the level of authorization for the HiperSockets NTA Logical Partition. The Channel ID, type, and card description are displayed. Select from the following choices the level of authorization you want for the HiperSockets NTA logical partition:

- All IQD channels are not authorized to enable HiperSockets NTA
- This IQD channel is not authorized to enable HiperSockets NTA
- This IQD channel is authorized to enable, control and capture network traffic from all logical partitions that contain the IQD CHPID that maps to this IQD channel
- Customized HiperSockets NTA logical partition authorization list for this IQD channel.

Submit
To apply modified NTA rules for the selected HiperSocket channel, select **Submit**.

Change Customized Settings...
To customize what partitions will be NTA authorized to trace and what partitions are eligible to be traced, select **Change Customized Settings...**.

Save Current Settings
To save and backup the current NTA authorization rules for all the HiperSocket channels, select **Save Current Settings**. Use this to save your current rules while you make a temporary change, then you can restore them later.

Restore Saved Settings
To restore the previous saved NTA authorization rules for all the HiperSocket channels, select **Restore Saved Settings**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

New Partition

Accessing the New Partition task

The **New Partition** task guides you through the process of creating a new partition on a Dynamic Partition Manager (DPM)-enabled system.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

You can access this task from the main HMC page by selecting the Systems Management node, by selecting a specific DPM-enabled system, or by selecting the task in the Tasks index. You can use either the default SYSPROG user ID or a user ID that a system administrator authorized to this task through customization controls in the **User Management** task.

To create a new partition:

1. Select a DPM-enabled system.
2. From the **Configuration** task group, open the **New Partition** task. This action opens the **New Partition** window.
3. Complete the required fields on the **Name**, **Processors**, **Memory**, **Network**, **Storage**, **Accelerators**, **Cryptos**, and **Boot** pages. To advance from one page to the next, click **Next**.
4. From the **Summary** page, review the information and then click **Finish** to complete the task. A progress indicator is displayed until DPM finishes creating the partition.

When it finishes creating the partition definition, DPM opens the Validation window, which displays a message indicating that your partition has been created, and lists additional tasks that you can use to work with the new partition. To work with the partition, click any of the links on the Validation window to open a related task in a separate window. When you are finished reviewing the information on the Validation window or using the provided links to related tasks, click **Close** to close the Validation window.

New Partition

The **New Partition** task guides you through the process of creating a new partition on a Dynamic Partition Manager (DPM)-enabled system. This process includes:

- Naming and describing the partition
- Assigning processors and memory
- Providing access to I/O, including networks, storage, accelerators, and cryptos
- Configuring the boot device and parameters for loading a hypervisor or operating system on the partition.

The **New Partition** task offers two modes through which you can create a partition: basic and advanced. This online documentation describes the basic mode of the **New Partition** task. For a comparison of the two modes and the implications of switching between them, see “New Partition task modes” on page 1092.

Regardless of the task mode that you use, note that you are only creating a partition, not starting it. After you have finished creating the partition by defining its properties through either task mode, you can start it by using the **Start** task.

The basic mode of the **New Partition** task is organized into the following pages, each of which are listed in the navigation pane.

As you advance through the pages by clicking **Next**, the current page is highlighted in the navigation pane. If you have not provided required information on a specific page, a warning icon is displayed next to the page link in the navigation pane.

The navigation pane also includes the following links to related tasks.

Monitor System
Switches the foreground window to the **Monitor** tab for the selected DPM system node.

You can find more detailed help on the following elements of this window:

Advanced
To switch to the advanced mode of the **New Partition** task, click **Advanced**. Clicking **Advanced** opens a confirmation dialog through which you can set the advanced mode as the default mode whenever you launch the **New Partition** task. The confirmation window contains the following controls.

Always use Advanced
Sets the advanced mode as the default mode whenever you open the **New Partition** task. By default, this check box is unchecked.

Switch
Changes the mode of the task to the advanced mode. If you click **Switch** to change to the advanced mode, any changes that you made in the basic mode are automatically carried over into the advanced mode.

Cancel
Returns to the basic mode of the **New Partition** task.

For the implications of switching between task modes, see "New Partition task modes" on page 1092.

Back
To navigate to the previous page in the task, click **Back**. This option is disabled on the **Welcome** page.

Next
To navigate to the next page in the task, click **Next**. This option is disabled on the **Summary** page.

Finish
This option is available only on the **Summary** page. To create a new partition, click **Finish**. A progress indicator is displayed until DPM finishes creating the partition.

When it finishes creating the partition definition, DPM opens the Validation window, which displays a message indicating that your partition has been created, and lists additional tasks that you can use to work with the new partition. To work with the partition, click any of the links on the Validation window to open a related task in a separate window. When you are finished reviewing the information on the Validation window or using the provided links to related tasks, click **Close** to close the Validation window.

Cancel
To exit the task without creating a new partition, click **Cancel**.

Help
To display help for the current window, click **Help**.

New Partition task modes

The **New Partition** task offers two modes through which you can create a partition: basic and advanced. Basic is the default mode, but you have the option of setting advanced as the default mode.

Basic
The basic task, which is presented the first time that you open the **New Partition** task, provides a quick, guided method of creating a partition; DPM either provides default values or automatically generates many of the values for partition properties that are required to successfully start a partition. Some of these properties are not displayed or editable in the basic task mode. To navigate through the task, use the **Next** and **Back** buttons. When you have finished entering values in the required fields, click **Finish** to create the partition definition.

Advanced
The advanced task, which you can launch from the basic task, enables experienced users to view all partition properties and to change any default values. To access each section in the advanced task, click the appropriate link in the navigation pane, or scroll down the main page and expand or collapse each section as necessary. When you have finished entering values in the required fields, click **OK** to create the partition definition.

To use the **New Partition** task in either mode, you need to use either the default SYSPROG user ID or a user ID that a system administrator authorized to this task through customization controls in the **User Management** task.

Comparing the task modes

Table 15 on page 1093 lists key partition properties, and indicates whether you can edit those properties using the **New Partition** task in either basic or advanced mode.

- A dash (—) indicates a property that you cannot edit in the basic task mode. DPM either provides default values or automatically generates values for these properties.
- A check mark (✔) indicates a property that you can edit.

*Table 15. Comparison of editable partition properties in the basic and advanced **New Partition** task modes*

Partition property	Basic mode	Advanced mode
Partition name	✔	✔
Partition short name and ID	—	✔
Partition type	✔	✔
Reserved resources	—	✔
Acceptable partition status values	—	✔
Controls: • **Partition access** • **Counter facility authorization** • **Sampling facility authorization**	—	✔ (editing requires SYSPROG or SERVICE user ID)
Shared processors	✔	✔
Dedicated processors	—	✔
Processing weights and capping	—	✔
Memory (initial allocation)	✔	✔
Maximum memory (dynamic allocation)	✔	✔
Network interface cards (NICs)	✔	✔
VLAN ID and MAC address for NICs	—	✔

*Table 15. Comparison of editable partition properties in the basic and advanced **New Partition** task modes (continued)*

Partition property	Basic mode	Advanced mode
Storage (storage groups, tape links, or HBAs)	✓	✓ (ability to edit device numbers for FCP storage groups and tape links, and to change adapters for FCP storage groups in this mode only)
Accelerators (virtual functions)	✓ (if supported by the system and installed)	✓ (if supported by the system and installed)
Cryptos (security)	✓ (if installed on system)	✓ (if installed on system) Permitting AES, DES, or ECC protected key import is available in this mode only.
Boot options, including Secure Boot for Linux	✓	✓

Switching between task modes

You have the option of switching between the basic and advanced task modes, and the option of setting the advanced mode as the default mode whenever you subsequently launch the **New Partition** task. To switch from the basic mode to the advanced mode, click **Advanced**, which is located in the lower left corner of the **New Partition** window. Clicking **Advanced** opens a confirmation dialog through which you can set the advanced mode as the default mode whenever you launch the **New Partition** task.

If you start in basic mode and switch to advanced mode

- If you edited any fields in the basic mode and then switch to the advanced mode, your changes are automatically carried over into the advanced mode. For example, if you entered a name for your new partition on the **Name** page of the basic task, that name is displayed on the **General** page of the advanced task.
- To switch back to the basic task mode, click **Basic**, which is located in the lower left corner of the **New Partition** window.
  - Clicking **Basic** opens a confirmation dialog through which you can set the basic mode as the default mode whenever you launch the **New Partition** task.
  - If you edited **any** fields in the advanced mode, those changes are not preserved when you switch back to the basic mode. However, any edits that you originally made in the basic mode are preserved. In other words, switching from advanced mode to basic mode wipes out all changes that you made in advanced mode, and restores the changes that you made in basic mode.

If you start in advanced mode and switch to basic mode

If you edited any fields in the advanced mode and then switch to the basic mode, your changes are discarded, even if the partition property is available for editing in the basic mode.

Welcome

When you first use the **New Partition** task, the **New Partition** window opens, with an overlay that highlights key task controls on the window.

- Click the **Okay, got it** button to remove the page overlay. The Welcome page is displayed; it provides a summary of the steps that you complete to create a new partition.
- On the Welcome page, you can use two controls to modify the page display.

  - Click the **Show this welcome page next time** check box if you want to see the Welcome page the next time that you open this task. By default, the check box is not selected.
  - Click the icon at the end of the check box label if you want to restore the page overlay.
- When you have finished, click **Next** to navigate to the next page in the task.

Name

Use the Name page to provide a name for and description of the new partition.

On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Specify the name of the new partition, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. A partition name must uniquely identify the partition from all other partitions defined on the same system.

Description
Optionally, specify a description for the partition. The description can be up to 1024 characters in length.

Partition type
Specify one of the following values that identifies the type of partition that you are creating.

Linux
In this type of partition, you can install and run a Linux on Z distribution as a single operating system, or as a hypervisor for multiple guests.

z/VM
In this type of partition, you can install and run z/VM as a hypervisor for multiple Linux guests.

Secure Service Container
This type of partition is a Secure Service Container, in which you can run only specific software appliances that the Secure Service Container supports.

When the selected partition type is **Secure Service Container**, the page display includes the following additional fields.

Master User ID
Enter the user ID to be used as the default master user ID for the Secure Service Container partition. This user ID has authority to perform any task that is available through the Secure Service Container graphical user interface (GUI).

A master user ID can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

Master Password
Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis (), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

Confirm Master Password
Reenter the password exactly as you typed it for the Master Password field.

To navigate to the next page in the task, click **Next**.

Processors

Partitions on a DPM-enabled system can have only one defined processor type: either Central Processor (CP) or Integrated Facility for Linux (IFL), depending on the processor types that are installed on the system. Use the Processors page to define the type and number of shared virtual processors for the

partition, and to view various charts that are based on your selections. The virtual processors are allocated from physical processors of the selected type.

To work with the information on the Processors page, complete the following steps.

1. If the Processors type field is displayed, select a value. If you want to enable simultaneous multithreading for this partition, you must select the IFL processor type.
2. Review the Processors bar chart to determine how many processors are available on this system, and how many are already in use or reserved for other partitions.
3. Select the number of processors that you want to assign to your new partition. If you are creating a partition only to familiarize yourself with the process, you can accept the default value. Otherwise, base your selection on your knowledge of the processing requirements of the operating system and applications that you plan to run in this new partition.
4. Review the Processors bar chart and pie chart to understand how your selection affects the availability of processing resources on the system. Although you can select a number of processors greater than the number that is currently available, your new partition will not start unless currently active, unreserved partitions are stopped or more processors are added to the system.
5. When you have finished, click **Next** to navigate to the next page in the task.

The following list provides a description of each element on the Processors page. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Processor type
If this field is displayed in the Processors section, select either the **Central Processor (CP)** or **Integrated Facility for Linux (IFL)** processor type. If you want to enable simultaneous multithreading for this partition, you must select the IFL processor type.

If only one type of processor is installed on the system, this field is not displayed.

Processors
Select the number of shared processors for the new partition. You can use one of the following controls to modify the value.

Slider
The minimum value is 1 and the maximum value is the number of entitled processors on the system. The slider not only shows the total range of values that you can select, but also uses color to indicate the current state of processor resources on the system.

- Green indicates the range of available processor resources. If you select a value in this range, you can successfully start the partition.
- Yellow indicates the range of processor values that prevent the new partition from starting. This range is the number of dedicated processors that are assigned to active and reserved partitions. If you select a number in this range, you receive an inline warning message indicating that the processor value you selected is greater than the number of shared physical processors. In this case, the partition cannot be started unless the number of shared physical processors on the system is increased.

Text entry box and number spinner
Using the text box, enter a valid integer within the limits of the slider range. When you enter a value, the slider changes to reflect the value entered in the text box. Alternatively, use the number spinner to increment or decrement the value in the text entry box and slider. Each click increments or decrements the value by one, within the limits of the slider range.

Processors bar chart
Indicates the number of shared and dedicated physical processors on the system. The bar chart scale ranges from 0 to the system design limit. To show the actual number of processors that each bar segment represents, hover your cursor over the colored segment. A dotted line indicates the total number of entitled processors on the system. Entitled processors are processors that are licensed for use on the system; the number of entitled processors might be less than the total number of physical processors that are installed on the system.

To the right of the bar chart, a color legend identifies each segment of the bar chart:

- The number of shared processors that you have currently specified for the new partition. This value varies when you change the Processors setting through the slider, text box, or number spinner.
- The number of shared processors, if any, that are available for use by partitions on the system.
- The number of dedicated physical processors that are assigned to active partitions and reserved partitions, if any exist. This number does not reflect any dedicated processors that are assigned to stopped or unreserved partitions.
- The total number of entitled processors on the system. If you have specified a number in the second range (yellow) for the new partition, the total number of processors for all partitions might exceed the number of entitled processors.

Shared Processors pie chart

Indicates the relative distribution of virtual processors for this new partition and all active partitions on the system that are using shared physical processors.

To the right of the pie chart, a color legend identifies each of the partitions by name. To view details for a specific partition in the pie chart, hover your cursor over the pie wedge with the same color as shown in the legend, next to the partition name. The pie wedge is slightly enlarged and a tooltip displays details for the partition. The tooltip displays the partition name, the number of processors for that partition, and its relative percentage of the total shared partitions, rounded to two decimal places.

At most, the pie chart consists of 12 wedges, one of which is reserved for this new partition. If the system has more than 11 active partitions, the pie chart is divided as follows:

- One wedge for the new partition that you are defining. The wedge size and number of processors vary when you change the Processors setting through the slider, text box, or number spinner.
- One wedge for each of the 10 active partitions with the highest number of processors.
- One wedge that represents all remaining active partitions on the system and the total number of processors shared by this group. In the legend, this group wedge is labeled Others, with the total number of partitions in parentheses.

Memory

Each partition on a DPM-enabled system has exclusive use of a user-defined portion of the total amount of entitled memory that is installed on the system. Use the Memory page to define the initial and maximum amounts of memory to be assigned to the new partition. The partition receives its initial amount when it is started.

When you define the amount of memory to be assigned, or allocated, to a specific partition, you specify an initial amount of memory, and a maximum amount that must be equal to or greater than the initial amount. If the maximum amount of memory is greater than the initial amount, you can add memory up to this maximum to the active partition, without stopping and restarting it.

To work with the information on the Memory page, complete the following steps.

1. Review the Installed Memory bar chart to determine how much memory is available on this system, and how much is already in use or reserved for other partitions.
2. Select the amounts of initial and maximum memory that you want to assign to your new partition. If you are creating a partition only to familiarize yourself with the process, you can accept the default values for both the Memory and Maximum Memory fields. Otherwise, base your selection on your knowledge of the memory requirements of the operating system and applications that you plan to run in this new partition.
3. To understand how your selection affects the availability of memory resources on the system, review the updated Installed Memory bar chart.
4. When you have finished, review another section or click **OK** to save the partition definition.

The following list provides a description of each element on the Memory page. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional. You can set the memory amounts in different units: megabytes (MB), gigabytes (GB), or terabytes (TB). The default unit is GB. To change the unit, hover your cursor over the unit in a field label, and select another unit from the popup

display. When you change the unit for one field, the same unit change is replicated to the other display elements on the page.

Memory

Define the amount of memory to be assigned to the partition. This value represents the initial amount of memory that the partition receives when it is started. If you set this initial amount to a value greater than the value currently displayed for the Maximum Memory field, the maximum memory is automatically set to the same value. You can use one of the following controls to modify the value. If you are creating a Secure Service Container partition, you must specify an initial amount of at least 4096 MB (4 GB).

Slider

The minimum value that is displayed depends on the unit that you have selected (MB, GB, or TB); for example, the minimum value for the default unit (GB) is 0.5. The maximum value is the amount of entitled memory on the system; this maximum varies by system. The slider not only shows the total range of values that you can select, but also uses color to indicate the current state of memory resources on the system.

- Green indicates the range of available memory values that you can select and successfully assign to the partition.
- Yellow indicates the range of memory values that might prevent the partition from starting. This range is the amount of memory that is assigned to active and reserved partitions. If you select a number in this range, you receive an inline warning message indicating that the new partition might fail to start unless the amount of available memory on the system is increased.

Text entry box and number spinner

Using the text box, enter a valid integer within the limits of the slider range. When you enter a value, the slider changes to reflect the value entered in the text box. Alternatively, use the number spinner to increment or decrement the value in the text entry box and slider. Each click increments or decrements the value by 0.5, within the limits of the slider range.

Maximum Memory

Define the amount of maximum memory assigned to the partition. The selected value must be equal to or greater than the value specified in the Memory field. If you want this new partition to have access to additional memory resources without having to stop and restart it, specify a value that is greater than the value specified in the Memory field.

The controls (slider, text box and number spinner) are the same as those for the Memory field. The slider ranges and colors also have the same significance as those for the Memory field.

Installed Memory bar chart

Indicates the distribution and amounts of system memory, including the memory assigned to this partition. The bar chart scale ranges from 0 to the total amount of memory that is installed on the system. To show the actual amount of memory that each bar segment represents, hover your cursor over the colored segment.

To the right of the bar chart, a color legend identifies each segment of the bar chart:

- The amount of memory that you have currently specified for this partition. This value varies when you change the Memory setting through the slider, text box, or number spinner.
- The maximum amount of memory that you have currently specified for this partition. This value is represented as a dotted line in the bar chart, and its position moves when you change the Maximum Memory setting through the slider, text box, or number spinner.
- The total amount of allocated memory, which is the total memory assigned to all active and reserved partitions on this system.
- The amount of entitled memory for this system. Entitled memory is the amount of memory that is licensed for use, which might be less than the total amount of memory that is installed on the system. This value is represented as a dotted line in the bar chart.

Network

Network interface cards (NICs) provide a partition with access to internal or external networks that are part of or connected to a system. Each NIC represents a unique connection between the partition and a specific network adapter that is defined or installed on the system.

Use the Network page to create NICs that enable the partition to access the networks connected to the DPM-enabled system. When you create a NIC, you can select the adapter that you want to use from a list of all of the network adapters that are currently configured on the system.

- For availability, select at least two network adapters of the same type, and create a NIC for each one.
- If you are creating a Secure Service Container partition, you must specify at least one NIC for communication with the Secure Service Container web interface.

To work with the information on the Network page, complete the following steps.

1. When you first use the **New Partition** task, the Network display contains an empty NICs table. If you are creating a Secure Service Container partition, the display includes additional information that you need to provide after you successfully define a NIC.

   From the Actions list in the NICs table, select **New** to open the **New Network Interface Card** window.
2. On the **New Network Interface Card** window, define a NIC for each network connection that is required for the operating system or hypervisor that runs on this partition, or for the applications that the operating system or hypervisor supports. For each NIC that you define, complete the following steps. For more detailed descriptions of the **New Network Interface Card** window elements, see "New Network Interface Card" on page 1102.
   a. Enter a unique, meaningful name and, optionally, a description of the new NIC.
   b. If you are creating a Secure Service Container partition, the display includes additional information about the network connection that is required to access the Secure Service Container web interface. This information includes an optional, virtual local area network (VLAN) identifier, the required IP address and type, and a mask / prefix.

      If you need more detailed descriptions as you provide these configuration values, see "New Network Interface Card" on page 1102.
   c. Review the entries in the Adapter Ports and Switches table to determine which network adapters are configured on the system.
      1) Check the percentages listed in the Uplink Utilization and Adapter NIC Allocation columns. If the percentage in either column is high (for example, 90%) for a specific port or switch, consider selecting a different port or switch on the same network.
      2) Look for a warning icon next to the name in the Adapter Name column; if the warning icon is displayed for a specific port or switch, select a different one on the same network.
      3) Select one port or switch by clicking the radio button in the Select column. Note that, if you select an OSA-Express adapter port other than port 0, you need to manually specify the relative port number through a Linux `qeth` device driver command, before entering the Linux command to bring the device online.
   d. Click **OK** to create the new NIC and close the **New Network Interface Card** window.
   e. Check the entry for the new NIC that is displayed in the NICs table on the Network page. Change the device number if your company uses a specific numbering convention for its networks.
   f. If the new NIC provides access to the Secure Service Container web interface, provide the required network settings that are displayed after the NICs table. If you need more detailed descriptions as you provide these configuration values, see "Secure Service Container Web Interface Communication" on page 1102.
3. Repeat the preceding steps, as necessary, to create a new NIC for each network connection that your new partition requires. If you define multiple NICs for a Secure Service Container partition, use the "Use to access the web interface" switch to identify whether the NIC provides access to the web interface.

4. When you have finished, click **Next** to navigate to the next page in the task.

The following topics describe the NICs table actions and elements, and the elements in the "Secure Service Container Web Interface Communication" section.

- “The NICs table toolbar” on page 1100
- “Columns in the NICs table” on page 1100
- “Standard table functions” on page 1102
- “Secure Service Container Web Interface Communication” on page 1102

The NICs table toolbar

The NICs table contains an entry for each network interface card, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Network Interface Card** window, through which you can create a new network interface card. For more information, see “New Network Interface Card” on page 1102.

Details
Opens the **NIC Details** window. This action is enabled when only one NIC is selected in the table. The **NIC Details** window fields and controls are the same as those for the **New Network Interface Card** window, with the following exceptions:

- The name, description (if any), device number, and adapter port or switch selection are displayed for the selected NIC.
- The Device number field is marked as a required field. The device number is a unique hexadecimal value that the system automatically generated when this NIC was created. If you want to edit this value, make sure that you enter a valid hexadecimal number.
- If the NIC is the only NIC that provides access to the Secure Service Container web interface, the "Use to access the web interface" switch is set on and cannot be set off.
- The Adapter Ports and Switches table contains entries for only those configured ports and switches that have the same card type as the selected NIC, because you cannot change the type of network interface card.

Delete
Opens the **Delete NIC** confirmation window through which you can delete one or more NICs. This action is enabled when one or more NICs are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected NICs. The confirmation window closes, and the resulting NICs table display does not contain any entries for the deleted NICs.
- Click **Cancel** to close the confirmation window and return to the Network section, without deleting any NICs.

Adapter Details
Opens the **Adapter Details** task in a separate window. This action is enabled when one or more NICs are selected in the table.

Columns in the NICs table

The NICs table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a virtual network interface card (NIC). The name is a hyperlink through which you can open the **NIC Details** window. To edit the name, double-click in the table cell and type the new name.

If this NIC represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

IP Address
Displays one of the following values:

- For a NIC that provides access to the Secure Service Container web interface, the value is either a specific IPv4 or IPv6 address or, for IP address types of DHCP and Link Local, the word Automatic.
- For all other NICs, the value displayed is a dash (-).

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the NIC. The operating system to be installed on the partition will use this device number to access the NIC. When creating a new NIC for an OSA card or HiperSockets switch, DPM generates three consecutive device numbers for the operating system to use for unit addresses, and displays only the first number in this field.

Change the device number if your company uses a specific numbering convention for its networks. To edit the device number, double-click in the table cell and type a new hexadecimal value. When you edit the device number for an OSA card or HiperSockets switch, DPM uses this new value as the first device number, and generates two consecutive device numbers based on the new value.

Notes:

- You cannot use a device number of 0000 for a PCI adapter, such as a RoCE adapter.
- The z/VM hypervisor does not support a device number of 0000 for an OSA card or HiperSockets switch.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port
Displays the adapter port value in decimal.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

VLAN ID
Displays the identifier of the virtual local area network (VLAN) through which the network adapter sends and receives network traffic. A VLAN ID value applies only for a NIC that is configured for the Secure Service Container web interface.

Description
Displays the user-provided description, if any, of the network interface card. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Secure Service Container Web Interface Communication

The "Secure Service Container Web Interface Communication" section displays network settings that you need to define for the Secure Service Container partition. Some of the values that you supply depend on the IP address type of the NIC that you created to access the web interface. An asterisk (*) preceding the label indicates that a value is required.

Host Name
Enter the Linux host name of the appliance to run in the Secure Service Container partition. To access the Secure Service Container web interface, users need to specify a URL that contains either a host name or an IP address for the Secure Service Container partition. A host name can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (any case), and the following special characters: period (.), colon (:), and hyphen (-).

Default IPv4 Gateway
Enter an IPv4 address for the default gateway. A default IPv4 gateway is required if you specified a Static IPv4 IP address type for the NIC.

Default IPv6 Gateway
Enter an IPv6 address for the default gateway. A default IPv6 gateway is required if you specified a Static IPv6 IP address type for the NIC.

DNS Server 1
Enter an IPv4 or IPv6 address for the primary domain name system (DNS) server. A DNS server definition is required if you specified a Dynamic Host Configuration Protocol (DHCP) IP address for the NIC.

DNS Server 2
Enter an IPv4 or IPv6 address for a secondary DNS server.

New Network Interface Card

Use the **New Network Interface Card** window to create a network interface card. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Initially displays a system-generated name for the new NIC, which you can edit by double-clicking in the name field and typing a new name. The NIC name must be different from the name of any other NIC that you define for this new partition.

Description
Optionally, provide a description for this new NIC. The description can be up to 1024 characters in length.

Use to access the web interface
Only when the partition type of this partition is **Secure Service Container**, the display includes a switch to indicate whether you can configure this NIC to access the Secure Service Container web interface. When the switch is set to **YES**, the display includes the following configuration settings, which Secure Service Container partitions require for access to the web interface. For a Secure Service Container partition, you can select only an OSA or HiperSockets adapter.

VLAN ID
Specify the virtual local area network (VLAN) if the link you are using is defined in TRUNK mode. The valid range of VLAN IDs is 1 - 4094. Note that DPM does not provide VLAN enforcement for Secure Service Container partitions.

IP Address Type
Select one of the following types:

- **DHCP** (Dynamic Host Configuration Protocol)
- **Link Local**
- **Static IPv4 Address**
- **Static IPv6 Address**

The selected type determines which of the remaining fields require values. An asterisk (*) preceding the label indicates that a value is required.

IP Address
Enter the IP address of the network adapter. This field is required only for IP addresses of type **Static IPv4 Address** and **Static IPv6 Address**.

Mask/Prefix
For an IPv4 address type, enter the mask/prefix in either bit notation (for example, `/24`) or mask notation (for example, `255.255.255.0`). For an IPv6 address type, enter the mask/prefix in bit notation only.

Adapter Ports and Switches table
Lists all of the configured ports or switches for all of the configured network adapters on this system. To successfully define a new NIC, you must select only one table entry.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. Select only one adapter port or switch for the new NIC.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port
Displays the adapter port value in decimal.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

Uplink Utilization
Indicates the average uplink utilization for the port or switch over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different port or switch on the same network. The utilization is shown in both a graphic progress bar and in numeric percentage. For

OSA and RoCE adapters, the physical port utilization is displayed; for HiperSockets, the switch utilization is displayed.

Adapter NIC Allocation
Indicates the percentage of NICs that are currently allocated to the adapter for this port or switch. If the percentage is high (for example, 90%), consider selecting a different port or switch on the same network. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes NICs only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

If you select a port or switch on an adapter that does not have sufficient allocation space for this new NIC, a warning message is displayed above the table. The message indicates that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the port or adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new NIC, click **OK** to create the NIC definition and close the **New Network Interface Card** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Storage

Use the Storage page to attach storage groups and tape links, or to create host bus adapters (HBAs) that enable the partition to access storage networks and hardware that is connected to the DPM-enabled system.

Depending on the version of DPM that is applied on the system, the Storage section contains a Storage Groups table, a Tape Links table, or an HBAs table with controls that you can use to attach storage groups and tape links, or to create HBAs. Follow the instructions that correspond to the type of table displayed on the page.

- "Attaching storage groups and tape links (DPM R3.1 or later)" on page 1104
- "Accessing FCP storage through HBAs (DPM R3.0 or earlier)" on page 1107

Attaching storage groups and tape links (DPM R3.1 or later)

System administrators create storage groups and tape links to enable partitions (and the operating systems and applications that they host) to use physical storage hardware that is connected to the system. A *storage group* is a logical group of storage volumes that share certain attributes. A *tape link* defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN.

DPM supports the following types of storage groups and tape links.

- FICON storage groups, which consist of volumes that reside on external Fibre Connection (FICON) extended count key data (ECKD) direct-access storage devices (DASD). This type of storage group is available starting with DPM R3.1.
- FCP storage groups, which consist of volumes that reside on external Fibre Channel Protocol (FCP) Small Computer System Interface (SCSI) disk storage devices. This type of storage group is available starting with DPM R3.1.

- Non-Volatile Memory Express (NVMe) storage groups, which consist of solid state drives (SSDs) that are installed in carrier cards in the system I/O drawers. NVMe storage is available only when the system has one or more IBM Adapter for NVMe1.1 features. This type of storage group is available starting with DPM R4.2.
- FCP tape links, each of which defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN. These connection attributes include storage resources such as system adapters, world wide port names (WWPNs), and the number of partitions that can share the connection. Support for FCP tape links is available starting with DPM R4.3.

FICON and FCP storage groups can be shared by multiple partitions, and multiple storage groups can be attached to one partition. FCP tape links also can be shared by multiple partitions, and multiple tape links can be attached to one partition. In contrast, only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared. However, a partition that has attached NVMe storage groups can also have attached FICON and FCP storage groups, and FCP tape links.

To attach one or more storage groups to the partition, complete the following steps.

1. When you first use the **New Partition** task, the Storage display contains an empty Storage Groups table and Tape Links table. Select the plus icon in the table toolbar to open the **Attach Storage Groups** or **Attach Tape Links** window.
   - On the **Attach Storage Groups** window, select one or more storage groups listed in the Storage Groups table to attach to this partition.
     - The suggested practice is to select storage groups that are in the Complete fulfillment state, but you can select any storage group except for those with a fulfillment state of Incomplete, or those that are already attached to the maximum number of partitions. If you do select groups in states other than Complete, some storage might not be available for use when you start the partition.
     - Use the additional information in the Storage Groups table, as necessary, to decide which storage groups to attach. For descriptions of the columns in the Storage Groups table, see “Attach Storage Groups” on page 1109.

     When you have finished selecting storage groups to attach, select **OK** to close the **Attach Storage Groups** window.
   - On the **Attach Tape Links** window, select one or more tape links listed in the table to attach to this partition.
     - The suggested practice is to select tape links that are in the Complete fulfillment state, but you can select any tape link except for those with a fulfillment state of Incomplete, or those that are already attached to the maximum number of partitions. If you do select links in states other than Complete, some storage might not be available for use when you start the partition.
     - Use the additional information in the table, as necessary, to decide which tape links to attach. For descriptions of the columns in the table, see “Attach Tape Links” on page 1151.

     When you have finished selecting tape links to attach, select **OK** to close the **Attach Tape Links** window.
2. Check the entries for the storage groups or tape links that you selected, which are now displayed in the Storage Groups table or Tape Links table in the Storage section. If necessary, you can use the minus icon in the table toolbar to remove a storage group or tape link from the table.

   For FCP storage groups and FCP tape links only, you can expand the table entry to show the system-generated host bus adapters (HBAs) and their assigned adapters. You can change the device numbers that DPM automatically assigned to the HBAs when you selected the FCP storage group or FCP tape link. An error icon is displayed if you try to specify a device number that is already in use. For more details, see “Host Bus Adapters (HBA) table for an FCP storage group or tape link” on page 1106.
3. When you have finished, review another section or click **OK** to save the partition definition.

   When you start the new partition, you might need to enter Linux commands to make the storage groups available to the operating system that the partition hosts. NVMe storage groups are automatically detected by the operating system, so you do not need to enter Linux commands to make that type of storage group available to the operating system. Similarly, the tape devices that are

available through attached tape links are automatically detected by the operating system, so you do not need to enter Linux commands for tape devices either.

When attaching a storage group in Complete state

- For an FCP storage group:
  - If the storage group contained the boot volume, the operating system brings online all of the HBAs for this storage group, and all volumes in the storage group are available. No action is required unless you have attached other storage groups.
  - If the storage group does not contain the boot volume, and the operating system is not configured to bring HBAs online automatically, you need to issue the **chccwdev** command to bring online all of the HBAs.
- For a FICON storage group, the operating system brings online only the boot volume. You need to issue the **chccwdev** command to bring online all of the remaining volumes in the storage group that contains the boot volume, as well as the volumes in any other storage groups that you attached.

When attaching an unfulfilled storage group that becomes Complete as the partition is running

- For an FCP storage group:
  - If adapters were assigned to HBAs while the partition is running, you need to use the **chchp** command to activate the channel paths for those new adapters.
  - To access the volumes in the storage group, you need to issue the **chccwdev** command to bring online all of the HBAs.
- For a FICON storage group:
  - If the adapters connecting the storage group to the storage subsystem were assigned while the partition is running, use the **chchp** command to activate the channel paths for those new adapters.
  - All volumes are offline. You need to issue the **chccwdev** command to bring online all of the volumes in the storage group.

To find the IDs that you need to use for the Linux commands, use the following tasks.

- HBA device numbers are available in the Host Bus Adapters (HBA) table when you expand the storage group table entry in the Storage section of the **Partition Details** task.
- Channel path IDs for FCP adapters are shown in the Host Bus Adapters (HBA) table when you expand the storage group table entry in the Storage section of the **Partition Details** task.
- Channel path IDs for FICON adapters are shown on the **ADAPTERS** tab of the Storage Group details; open the **Configure Storage** task and select the storage group in the **Storage Overview** to open the Storage Group details page.
- FICON volume device numbers are shown on the **VOLUMES** tab of the Storage Group details page; open the **Configure Storage** task and select the storage group in the **Storage Overview** to open the Storage Group details page.

Host Bus Adapters (HBA) table for an FCP storage group or tape link

For FCP storage groups or tape links only, you can expand the Storage Groups or Tape Links table entry to show the Host Bus Adapters (HBA) table. The following list describes the columns in the table; depending on the fulfillment state of the storage group or tape link, some information might not be available.

Name
Displays the system-generated name of the HBA.

Device Number
Displays the system-generated hexadecimal device number for the HBA. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by typing a new value in the column field.

WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a port in a disk storage subsystem or tape library that is connected to the system.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Adapter ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

Assigned Adapter
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

Accessing FCP storage through HBAs (DPM R3.0 or earlier)

Host bus adapters (HBAs) provide a partition with access to external storage area networks (SANs) and devices that are connected to a system. Each HBA represents a unique connection between the partition and a physical FICON channel that is configured on the system. When you create an HBA, you can select the adapter that you want to use from a list of all of the storage adapters that are currently configured on the system.

- For availability, select at least two storage adapters of the same type, and create an HBA for each one.
- If you are creating a Secure Service Container partition to install a software appliance, define at least one HBA to access the storage device on which the appliance installation image resides.

To work with the information on the Storage page, complete the following steps.

1. When you first use the **New Partition** task, the Storage display contains an empty HBAs table. From the Actions list in the HBAs table, select **New** to open the **New Host Bus Adapter** window.
2. On the **New Host Bus Adapter** window, define an HBA for each storage area network that is required for the applications that run in this partition. For each HBA that you define, complete the following steps. For more detailed descriptions of the **New Host Bus Adapter** window elements, see “New Host Bus Adapter” on page 1111.
   a. Enter a unique, meaningful name and, optionally, a description of the new HBA.
   b. Review the entries in the Adapter Ports table to determine which storage adapters are configured on the system.
      1) Check the percentage listed in the Adapter HBA Allocation column. If the percentage is high (for example, 90%) for a specific port, consider selecting a different port.
      2) Look for a warning icon next to the name in the Adapter Name column; if the warning icon is displayed for a specific port, select a different one.
      3) Select one port by clicking the radio button in the Select column.

      Click **OK** to create the new HBA and close the **New Host Bus Adapter** window.
   c. Check the entry for the new HBA that is displayed in the HBAs table in the Storage section. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by selecting the **Details** action and editing the HBA device number.
3. Repeat the preceding steps, as necessary, to create a new HBA for each storage area network that your new partition requires.
4. When you have finished, click **Next** to navigate to the next page in the task.

   The next page to open might be either Accelerators, Cryptos, or Boot, depending on the system configuration.

The following topics describe the HBAs table actions and elements.

- “The HBAs table toolbar” on page 1108
- “Columns in the HBAs table” on page 1108
- “Standard table functions” on page 1109

The HBAs table toolbar

The HBAs table lists all HBAs to be defined for the new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Host Bus Adapter** window, through which you can create a new host bus adapter (HBA). For more information, see "New Host Bus Adapter" on page 1111.

Details
Opens the **HBA Details** window. This action is enabled when only one HBA is selected in the table. The **HBA Details** window fields and controls are the same as those for the **New Host Bus Adapter** window, with the following exceptions:

- The name, description (if any), device number, and adapter port selection are displayed for the selected HBA.
- The Device number field is marked as a required field.

Delete
Opens the **Delete HBA** confirmation window through which you can delete one or more HBAs. This action is enabled when one or more HBAs are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected HBAs. The confirmation window closes, and the resulting HBAs table display does not contain any entries for the deleted HBAs.
- Click **Cancel** to close the confirmation window and return to the Storage section, without deleting any HBAs.

Adapter Details
Opens the **Adapter Details** task in a separate window. This action is enabled when one or more HBAs are selected in the table.

Columns in the HBAs table

The HBAs table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a host bus adapter (HBA). The name is a hyperlink through which you can open the **HBA Details** window. To edit the name, double-click in the table cell and type the new name.

If this HBA represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Type
Indicates the HBA type, which matches the type of adapter port that is selected when the HBA is created. The valid value is FCP, which represents Fibre Channel Protocol mode.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the HBA. The operating system to be installed on the partition will use this device number to access the HBA. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by selecting the **Details** action and editing the HBA device number. To edit the device number, double-click in the table cell and type a new hexadecimal value.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Description
Displays the user-provided description, if any, of the host bus adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Attach Storage Groups

Use the **Attach Storage Groups** window to select one or more storage groups to attach to the partition. This window contains the Storage Groups table, which lists all storage groups that system administrators have defined for use by partitions on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The Storage Groups table contains the following information and controls.

Select
Use check boxes in the Select column to identify which storage groups you want to attach to the partition. If a check box is disabled, either the storage group is attached to the maximum number of partitions, or you do not have permission to access the storage group.

Name
Specifies the user-defined name of the storage group.

Type
Specifies the type of storage group: FICON or FCP or NVMe.

Partitions
Specifies the number of partitions to which the storage group is attached.

Shareable
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

Total Capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Description
Specifies the user-provided description, if any, of this storage group.

Fulfillment state
Identifies the current state of the storage group. DPM runs a background check of storage resources for FCP storage groups and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours)..

Checking migration
This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

OK
After you have selected one or more storage groups, click **OK** to return to the Storage page of the **New Partition** task.

CANCEL
To close the window without saving any selections, click **CANCEL**.

Attach Tape Links

The table contains the following information and controls.

☐
Use check boxes in each table row or in the table header to identify which tape links you want to attach to the partition. If a check box is disabled, either the storage group is attached to the maximum number of partitions, or you do not have permission to access the storage group.

Name
Specifies the user-defined name of the tape link. The name is a hyperlink that opens to the Tape Link details page in the **Configure Storage** task.

Type
Specifies the type of tape link: FCP.

Partitions
Specifies the number of partitions to which the tape link is attached.

Shareable
Specifies whether the tape link can be shared among partitions, or whether it is dedicated to only one partition.

Description
Specifies the user-provided description, if any, of this tape link. The description can be up to 200 characters in length.

Fulfillment state
Identifies the current state of the tape link. DPM runs a background check of storage resources for FCP tape links and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours).

Complete
All of the storage resources listed in a create or modify request are available, properly configured and zoned, and DPM detects only those resources.

Incomplete
One or more storage resources for the tape link are marked as incomplete because the resource is missing, or in an error or degraded condition. Because DPM periodically checks the availability of storage adapters, switches, and tape libraries that are in use for a tape link, resources that were functioning properly can become incomplete.

Pending
One or more requested storage resources are not yet available or zoned correctly, or the tape link is not yet attached to all partitions that were specified in the original create request or a modify request.

Pending with mismatches
DPM detects system adapters that do not match the original create request or a modify request. Either the number of system adapters does not match the number of connecting paths, or the detected adapters do not match specific adapters that were assigned to the tape link.

OK
After you have selected one or more tape links, click **OK** to return to the Storage section of the **New Partition** task.

CANCEL
To close the window without saving any selections, click **CANCEL**.

New Host Bus Adapter

Use the **New Host Bus Adapter** window to create a new host bus adapter (HBA). On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Initially displays a system-generated name for the new HBA, which you can edit by double-clicking in the name field and typing a new name. The HBA name must be different from the name of any other HBA that you define for this new partition.

Description
Optionally, provide a description for this new HBA. The description can be up to 1024 characters in length.

Adapter Ports table
Lists all of the configured ports for all of the configured storage adapters on this system. To successfully define a new HBA, you must select only one table entry.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Adapter HBA Allocation
Indicates the percentage of HBAs that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter port. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Each storage adapter port has enough allocation space to support a maximum of 254 HBAs, but your system planner can change that maximum to a lower value. If you select an adapter port that does not have sufficient allocation space for this new HBA, a warning message is displayed above the table. The message indicates that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Location
Displays the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the port or adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new HBA, click **OK** to create the HBA definition and close the **New Host Bus Adapter** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Accelerators

An accelerator virtual function provides a partition with access to specific features, such as zEnterprise Data Compression (zEDC), that are installed on a system. Each virtual function represents a unique connection between the partition and a physical feature card that is configured on the system. This section is displayed only when a system that supports accelerators is managed through this HMC, and is enabled only for systems that support accelerators.

Use the Accelerators page to create virtual functions that enable the partition to access specific features installed on the DPM-enabled system. When you create a virtual function, you can select the adapter that you want to use from a list of all of the accelerator adapters that are currently configured on the system.

Accelerators are optional features and, therefore, might not be installed on the system. If none are installed, the Accelerators page is disabled.

To work with the information on the Accelerators page, complete the following steps.

1. When you first use the **New Partition** task, the Accelerators display contains an empty Accelerator Virtual Functions table. From the Actions list in the Accelerator Virtual Functions table, select **New** to open the New Virtual Function window.
2. On the **New Virtual Function** window, define one or more virtual functions for each accelerator that is required for the applications that run in this partition. For each virtual function that you define, complete the following steps. For more detailed descriptions of the **New Virtual Function** window elements, see “New Virtual Function” on page 1114.
   a. Enter a unique, meaningful name and, optionally, a description of the new virtual function.
   b. Review the entries in the Adapters table to determine which accelerator adapters are configured on the system.

1) Check the percentage listed in the Virtual Function Allocation column. If the percentage is high (for example, 90%) for a specific adapter, consider selecting a different adapter.
2) Look for a warning icon next to the name in the Name column in the Adapter table; if the warning icon is displayed for a specific adapter, select a different one.
3) Select one adapter by clicking the radio button in the Select column.
4) Click **OK** to create the new virtual function and close the **New Virtual Function** window.

c. Check the entry for the new virtual function that is displayed in the Accelerator Virtual Functions table on the Accelerators page. Change the device number if your company uses a specific numbering convention for its accelerators.

3. Repeat the preceding steps, as necessary, to create additional virtual functions.
4. When you have finished, click **Next** to navigate to the next page in the task.

   The next page to open might be either Cryptos or Boot, depending on the system configuration. If the system does not have any configured cryptographic features, the Cryptos page cannot be accessed.

The following topics describe the Accelerator Virtual Functions table actions and elements.

- "The Accelerator Virtual Functions table toolbar" on page 1113
- "Columns in the Accelerator Virtual Functions table" on page 1113
- "Standard table functions" on page 1114

The Accelerator Virtual Functions table toolbar

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Virtual Function** window to create a new virtual function. For more information, see "New Virtual Function" on page 1114.

Delete
Opens the **Delete Virtual Function** confirmation window through which you can delete one or more virtual functions. This action is enabled when one or more virtual functions are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected virtual functions. The confirmation window closes, and the resulting Accelerator Virtual Functions table display does not contain any entries for the deleted virtual functions.
- Click **Cancel** to close the confirmation window and return to the Accelerators section, without deleting any virtual functions.

Adapter Details
Opens the **Adapter Details** task. This action is enabled when one or more virtual functions are selected in the table.

Columns in the Accelerator Virtual Functions table

The Accelerator Virtual Functions table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove

the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the virtual function. The name is a hyperlink through which you can open the **Virtual Function Details** window. To edit the name, double-click in the table cell and type the new name.

If this virtual function represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Type
Indicates the virtual function type, which matches the type of adapter that is selected when the virtual function is created. The valid value is zEDC, for the zEnterprise Data Compression (zEDC) feature, which provides hardware-based acceleration for data compression and decompression.

Device Number
Displays the system-generated hexadecimal device number for the virtual function. The operating system to be installed on the partition will use this device number to access the virtual function.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports.

Description
Displays the user-provided description, if any, of the virtual function. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

New Virtual Function

Use the **New Virtual Function** window to create a new virtual function. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Provide a name for the new virtual function. The virtual function name must be different from the name of any other virtual function that you define for this new partition.

Description
Optionally, provide a description for this new virtual function. The description can be up to 1024 characters in length.

Adapters table
Lists all of the configured accelerators on this system.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. Select only one adapter for the new virtual function.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports.

Utilization
Indicates the average utilization for the adapter over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different adapter. The utilization is shown in both a graphic progress bar and in numeric percentage.

Virtual Function Allocation
Indicates the percentage of virtual functions that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes virtual functions only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Up to 15 partitions can share a zEDC feature. If you select an adapter that does not have sufficient allocation space for this new virtual function, a warning message is displayed above the table, indicating that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new virtual function, click **OK** to create the virtual function definition and close the **New Virtual Function** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Cryptos

The term *cryptos* is a commonly used abbreviation for adapters that provide cryptographic processing functions. Use the Cryptos page to enable the new partition to use the cryptographic adapters that it

requires, to assign a usage domain and, optionally, to assign control domains. Usage domains provide access to cryptographic functions, and provide the ability to manage domains and keys. Control domains provide only the ability to manage domains and keys.

Crypto features are optional and, therefore, might not be installed on the system. If none are installed, the Cryptos page is disabled.

When crypto adapters are installed on a system, they are configured in either coprocessor or accelerator mode, depending on the type of cryptographic processing that is required by the applications that run on the system. Each coprocessor or accelerator contains a specific number of usage domains, identified by an index number, which contain an isolated set of master keys. When you create a new partition, you select only one usage domain index to assign to your partition, and that index assignment applies for each cryptographic adapter that your partition can access.

Depending on the type of crypto adapter that you select, you might also need to define one or more control domains.

To work with the information on the Cryptos page, complete the following steps.

1. When you first use the **New Partition** task, the Cryptos display contains an empty Adapters table. From the Actions list in the Adapters table, select **Add** to open the Add Adapters window.
2. On the Add Adapters window, review the list of installed cryptographic adapters in the Adapters table, and select the adapters that your partition needs to use.

   For availability, select at least two cryptographic adapters of the same type.

   a. Check the percentages listed in the Utilization and Usage Domain Allocation columns. If the percentage in either column is high (for example, 90%) for a specific adapter, consider selecting a different adapter.

   b. Look for a warning icon next to the name in the Adapter Name column; if the warning icon is displayed for a specific adapter, select a different one.

   c. Select one or more adapters by clicking the corresponding check boxes in the Select column.

   d. Click **Continue** to open the Add Usage Domains window.
3. On the Add Usage Domains window, select one or more domains by clicking the corresponding check boxes in the Select column, and click **Continue** to open the Add Control Domains window.
4. On the Add Control Domains window, optionally select one or more control domains by clicking the corresponding check boxes in the Select column, then click **Continue** to save your selections and return to the Cryptos page.
5. The Cryptos page display now contains an Adapter Domains table, which lists each selected usage or control domain in a table row, with a table column for each of the selected adapters that are associated with the domain. Depending on how many adapters you selected, you might need to use the horizontal scroll controls to see all of the table columns.
6. In the Adapter Domains table, look for a warning icon in the adapter columns.

   a. If the warning icon is displayed for a specific usage domain on an adapter, click the warning icon to view the other partitions that are also using this domain.

      Although more than one partition can be assigned to the same usage domain index, only one active partition can use that usage domain at any given time. DPM detects whether any other partition definitions contain the same usage domain index for the same cryptographic adapter, and indicates whether any conflicts exist so you can select a different index.

   b. When you have finished reviewing the domain conflicts, click Close to close the window.

   c. To resolve a domain conflict, use the appropriate function in the Actions list in the Adapter Domains table to first remove the domain in conflict, and then to add a new usage domain.
7. When you have finished, click **Next** to navigate to the next page in the task.

The following topics describe the table actions and elements on the Cryptos page.

- “The Adapters table toolbar” on page 1117

The Adapters table toolbar

The Adapters table contains an entry for each cryptographic coprocessor or accelerator, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

Add
Opens the **Add Adapters** window through which you can add one or more crypto adapters to be used by the partition. For more information, see "Adding cryptographic adapters and domains" on page 1119.

Remove
Opens the **Remove Adapters** confirmation window through which you can remove one or more adapters from the partition definition. This action is enabled when one or more adapters are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Remove** to confirm that you want to remove the selected adapters. The confirmation window closes, and the resulting Adapters table display does not contain any entries for the deleted adapters.
- Click **Cancel** to close the confirmation window and return to the Cryptos section, without removing any adapters.

Adapter Details
Opens the **Adapter Details** task. This action is enabled when one or more adapters are selected in the table.

Columns in the Adapters table

The Adapters table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Crypto Number
Indicates the adjunct processor number that is assigned to this adapter. This number is associated with the use of the Adjunct Processor Extended Addressing (APXA) facility, which is only available on

specific systems. This facility increases the number of usage domains that can be supported on one cryptographic adapter.

Conflicts
Displays a warning icon in the column, only if one or more domain conflicts exist for a specific adapter. To display additional information about the conflicts, click the warning icon to open the Crypto Conflicts window. For more details, see "Crypto Conflicts - adapter" on page 1121.

Type
Indicates the mode in which the cryptographic adapter is configured on this system.

CCA coprocessor
The adapter is configured as a Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

EP11 coprocessor
The adapter is configured as an Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.

Accelerator
The adapter is configured as an Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific Crypto Express adapter names.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

The Adapter Domains table toolbar

When you first use the **New Partition** task, the Cryptos display contains only an Adapters table; after you add crypto adapters, the display also includes an Adapter Domains table.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

Add Control Domains
Opens the **Add Control Domains** window through which you can add more control domains. For more information, see the Add Control Domains section in "Adding cryptographic adapters and domains" on page 1119.

Add Usage Domains
Opens the **Add Usage Domains** window through which you can add more usage domains. For more information, see the Add Usage Domains section in "Adding cryptographic adapters and domains" on page 1119.

Remove
Opens the **Remove Domains** confirmation window through which you can remove one or more domains from the partition definition. This action is enabled when one or more domains are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Remove** to confirm that you want to remove the selected domains. The confirmation window closes, and the resulting Adapter Domains table display does not contain any entries for the deleted domains.

- Click **Cancel** to close the confirmation window and return to the Cryptos section, without removing any domains.

Columns in the Adapter Domains table

The Adapter Domains table lists each selected usage or control domain in a table row, with a table column for each of the selected adapters that are associated with the domain. Depending on how many adapters you selected, you might need to use the horizontal scroll controls to see all of the table columns.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Displays the index number assigned to each of the usage domains or control domains added to the partition definition. A letter icon that precedes the index number indicates whether the domain is a usage domain (**U**) or a control domain (**C**).

Adapters
Each remaining column in the Adapter Domains table represents a selected adapter, with the adapter name shown as the column heading. For each domain listed in the table, the adapter column displays either a checkmark or a warning icon, to indicate whether any conflicts exist. To display additional information about the conflict, click the warning icon to display the Crypto Conflicts window. For more details, see “Crypto Conflicts - Usage Domain number” on page 1122

Standard table functions

In addition to the customized action icons and the Actions list, the Adapters table and Adapter Domains table toolbars include the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Adding cryptographic adapters and domains

When you first select **Add** to add cryptographic adapters to the new partition definition, DPM opens a dialog that consists of several windows through which you can select adapters and domains. On any window, you can click **Cancel** to close the dialog and return to the Cryptos page. Otherwise, make a selection and click **Continue** to advance to the next window.

In contrast, when you subsequently access the dialog windows through selections in the **Actions** list of the Adapter Domains table, you can access the domain dialog windows separately; DPM opens the appropriate dialog window, based on your selection. Clicking **OK** or **Cancel** returns you to the Cryptos page.

The following lists describe the contents of each dialog window, in the order in which DPM presents them. Each window contains a table through which you make your selections; each of these tables has a toolbar with standard table functions, such as filters.

Add Adapters

The **Add Adapters** window displays a table containing one entry for each available crypto adapter that is not already assigned to this new partition. Use the Select column to select one or more adapters for the new partition to use.

Select

Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name

Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Crypto Number

Indicates the adjunct processor number that is assigned to this adapter. This number is associated with the use of the Adjunct Processor Extended Addressing (APXA) facility, which is only available on specific systems. This facility increases the number of usage domains that can be supported on one cryptographic adapter.

Conflicts

Displays a warning icon in the column, only if one or more domain conflicts exist for a specific adapter. To display additional information about the conflicts, click the warning icon to open the Crypto Conflicts window. For more details, see “Crypto Conflicts - adapter” on page 1121.

Type

Indicates the mode in which the cryptographic adapter is configured on this system.

CCA coprocessor

The adapter is configured as a Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

EP11 coprocessor

The adapter is configured as an Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.

Accelerator

The adapter is configured as an Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Card Type

Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific Crypto Express adapter names.

Utilization

Indicates the average utilization for the adapter over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different adapter. The utilization is shown in both a graphic progress bar and in numeric percentage.

Usage Domain Allocation

Indicates the percentage of usage domains that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes usage domains only for started and reserved partitions. To display this numeric percentage along

with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions cannot exceed 100%.

Each adapter supports up to 16 usage domains, but that limit can be increased through the use of the adjunct processor extended addressing facility, depending on the machine type and configuration of the DPM-enabled system. If you select an adapter that does not have sufficient allocation space, an error message is displayed above the table, indicating that the new partition might fail to start because this adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Add Usage Domains
The **Add Usage Domains** window displays a table containing one entry that represents each available usage domain and control domain, with usage domains listed first, by default. To limit the table entries to only those domains that are not defined to any partition on the system, select the **Hide usage domains defined to other partitions** check box. By default, the check box is checked.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Indicates the index number assigned to the usage domain or control domain. Each coprocessor or accelerator contains a specific number of usage domains, identified by an index number, which contain an isolated set of master keys. When you create a new partition, you select only one usage domain index to assign to your partition, and that index assignment applies for each cryptographic adapter that your partition can access. If you select a control domain, it is converted into a usage domain.

Conflicts
When the **Hide usage domains defined to other partitions** check box is unchecked, the Conflicts column is shown in the table. If a conflict exists for a specific domain, a warning icon is shown in the column. To display additional information about the conflict, click the warning icon to display the Crypto Conflicts window. For more details, see “Crypto Conflicts - Usage Domain number” on page 1122.

Add Control Domains
The **Add Control Domain** window displays a table containing one entry that represents each available control domain.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Indicates the index number assigned to the control domain. Control domains provide only the ability to manage domains and keys. If the partition is configured as the TCP/IP host for the Trusted Key Entry (TKE) workstation, you need to assign control domain indexes to the partition. Otherwise, selecting a control domain is optional. You can select one or more control domains.

Crypto Conflicts - adapter

Use the Crypto Conflicts window to view details about domain conflicts for a specific adapter, the name of which is displayed in the window title. This window contains the Conflicting Partitions table, which contains an entry for each partition for which the definition includes the same cryptographic adapter and usage domains that you have selected for the new partition. The table contains the following columns.

Partition
Displays the name of a partition for which the definition contains one or more adapters or domains that match those you have selected for the new partition. The name is a hyperlink through which you can open the **Partition Details** task.

Active/Reserved
Indicates whether the existing partition is active or reserved. If the partition is either active or reserved, a checkmark is displayed.

Usage Domains
Specifies each of the domain index numbers that conflict with those index numbers you have selected for the new partition. If multiple index numbers are in conflict, each number is separated by a comma; if consecutive index numbers are in conflict, they are shown in ranges. For example: `0-3, 5, 8-10`

To close the window and return to the previous window, click **Close**.

Crypto Conflicts - Usage Domain number

Use the Crypto Conflicts window to view details about the conflicts for a specific usage domain, the index number of which is displayed in the window title. This window contains the Conflicting Partitions table, which contains an entry for each partition for which the definition includes the same usage domain for one or more cryptographic adapters that you have selected for the new partition. The table contains the following columns.

Partition
Displays the name of a partition for which the definition contains one or more adapters or domains that match those you have selected for the new partition. The name is a hyperlink through which you can open the **Partition Details** task.

Active/Reserved
Indicates whether the existing partition is active or reserved. If the partition is either active or reserved, a checkmark is displayed.

Adapters (Crypto Number)
Displays the name of each adapter that is associated with the usage domain. The name includes the crypto number, which is shown in parentheses. Each adapter name is a hyperlink through which you can open the **Adapter Details** task. If multiple adapters are listed for a specific partition, each adapter is shown on a separate line in the table.

To close the window and return to the previous window, click **Close**.

Boot

Partitions on a DPM-enabled system can host a single operating system or hypervisor. Use the Boot page to select the location of the executables for the hypervisor or operating system to be run in this partition, or to upload the required files to initialize the hypervisor or operating system when the partition itself is started. Some of these boot options require that you find and select an ISO image file, which is a collection of files and metadata for installing software, and an .INS file, which maps image components (for example, kernel, ramdisk, parameter file) to the appropriate storage addresses in main memory.

The "Boot from" menu lists the boot options that are available for the hypervisor or operating system. If an option in the list is disabled, hover your cursor over that option to display additional information for that option. If necessary, take appropriate action to make that selection available; for example, if you want to use the Storage device (SAN) option, return to the Storage page to attach a storage group with a boot volume.

Use the **Secure Boot** option to have DPM verify that the software signature matches the signature from the distributor. If the signature does not match, the boot process ends. This option is enabled only when:

- The partition has a partition type of Linux.
- The system that hosts the partition supports the Secure Boot for Linux function.
- You are booting the Linux operating system from a volume in an FCP or NVMe storage group.

For the supported boot options and more detailed instructions for installing z/VM in a partition, see the *DPM Guide*, which is available through the Library link on IBM Resource Link.

To define a boot option, complete the following steps.

1. Click the down arrow to display the available options in the "Boot from" list.
2. Choose one of the available options and provide any additional information that is required.

   When you select a specific boot option, the display shows editable fields and other information related to the selected option. The following list describes each boot option, and provides instructions for providing any required information.

   None
   Select this option if you want to start a partition without a hypervisor or operating system. Although the partition can be started, it is not in a usable state. This option is the default for partitions with a partition type of **Linux** and **z/VM**.

   Secure Service Container
   This boot option is the default for a Secure Service Container partition. This boot option cannot be changed unless you first change the partition type.

   With this option, the display includes the **Boot in Installer Mode** switch, which is set to **YES** and cannot be set to **NO**. With the switch set to **YES**, the partition start process initializes the Secure Service Container Installer so you can install an appliance in the partition.

   Storage Group (SAN) or Storage device (SAN)
   Select this option when the hypervisor or operating system executables reside on an internal or external storage device. This option is available only when storage groups or host bus adapters (HBAs) are defined for the partition.

   When you select this option, the Boot section contains either a Storage Groups table or an HBA table. The Storage Groups table is displayed only when the DPM R3.1 storage management feature or a later DPM version is applied on the system. Follow the instructions that correspond to the type of table displayed on the page.

   - “Boot from a boot volume in a storage group” on page 1123 (only for systems with the DPM R3.1 storage management feature or a later DPM version applied)
   - “Boot from a boot volume accessed through an HBA” on page 1124

   Boot from a boot volume in a storage group

   The Storage Groups table displays the available storage groups that contain a boot volume. To view the available boot volumes, expand any table entry by selecting the storage group. The Storage Group table contains the following columns.

   Select
   Use a radio button in the Select column to identify the storage group that contains the boot volume for the operating system or hypervisor. Depending on the fulfillment state of the storage group and availability of a boot volume, the radio button might be disabled.

   Name
   Specifies the user-defined name of the storage group.

   Type
   Specifies the type of storage group: FICON or FCP or NVMe. The expanded table display contains a Boot Volume table that lists all available boot volumes that the storage group contains. The Boot Volume table content varies, depending on the storage group type. Note that, if you select an FCP storage group as the boot source for Linux, you can select the Secure Boot option, only when the system that hosts the partition supports the Secure Boot for Linux function.

   - For each boot volume in an FCP storage group, the Boot Volume table provides the universally unique identifier (UUID) and capacity of the volume, along with a user-supplied description, if any.

- For each boot volume in a FICON storage group, the Boot Volume table provides the name of the storage subsystem in which the volume resides, along with the volume ID and capacity. If a user-supplied description is available, it is also displayed in the table.
- For each boot volume in an NVMe storage group, the Boot Volume table provides the boot volume serial number and capacity, along with a user-supplied description, if any. When you select an NVMe volume, note that NVMe namespace management is not supported, so you can boot programs only from namespace ID=1.

Partitions
Specifies the number of partitions to which the storage group is attached.

Shareable
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

Total Capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Description
Specifies the user-provided description, if any, of this storage group.

Fulfillment state

Checking migration
This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

Boot from a boot volume accessed through an HBA

The HBA table displays the available host bus adapters. Select the HBA connected to the storage subsystem that hosts the boot volume, provide the 64-bit worldwide port number (WWPN) of the storage subsystem, and provide the 64-bit hexadecimal logical unit number (LUN) of the volume that contains the boot image. For example:

Target WWPN: `50:0a:09:85:87:09:68:ad` or `500a0985870968` (hexadecimal)
Target LUN: `4021400000000000`

Network server (PXE)
Select this option when you want to use a preboot execution environment (PXE) on a network server. This option is available only if a network interface card (NIC) for either an OSA port or HiperSockets switch is defined for the partition.

When you select this option, the NIC table displays the available network interface cards. Select the NIC for the adapter that connects the partition to the network on which the network boot server resides.

FTP server
Select this option if you want to use FTP to boot an image that is located on a different system. Provide the following information:

Host name
Enter either the fully qualified domain name of the FTP server, or its IP address.

User name
Enter the user name on the target FTP server.

Password
Enter the password associated with the user name on the target FTP server.

INS file
Either click **Browse** to retrieve a list of INS files from the target FTP server and select one file, or enter the fully qualified name (relative to FTP root) of an INS file.

Depending on the size of the FTP site, browsing might require more time than manually entering the full path and name of the INS file. Also note that the browsing function returns INS files found in the user's home directory or its subdirectories. Because you cannot select a starting directory, or navigate to a directory above the user's home directory, manually entering the full path and name of the INS file might be more expedient.

If you click **Browse**, a separate window displays the user's home directory and its subdirectories. Select one INS file, and click **OK** to close the Browse FTP Server window.

FTPS server
Select this option if you want to use the FTP Secure (FTPS) protocol to boot an image that is located on a different system. FTPS uses the Secure Socket Layer (SSL) protocol to secure data. With this option, you need to supply a host name, user ID, password, and .INS file, as described for the **FTP server** boot option.

SFTP server
Select this option if you want to use the Secure File Transfer Protocol (SFTP) to boot an image that is located on a different system. SFTP uses the Secure Shell (SSH) protocol to secure data. With this option, you need to supply a host name, user ID, password, and .INS file, as described for the **FTP server** boot option.

Hardware Management Console removable media
Select this option if you want to use an INS file from a media drive that is connected to the HMC. The media drive must be available when you are creating the partition definition and when the partition is started. Possible drive selections are **CD/DVD drive** or **USB flash memory drive**, depending on what media drives are installed in the HMC.

When you select this option:

a. If more than one type of media drive is available on the HMC, select the radio button for the media drive on which the INS file resides. Otherwise, skip to the next step.
b. Either enter the fully qualified name (relative to the mount point) of an INS file, or complete the following steps.
    1) Select **Browse** to start a search on the target media drive to retrieve a list of INS files. Any INS files found are displayed in a separate window.
    2) Select only one INS file and click **OK** to close the Browse Removable Media window.

ISO image
Select this option when you want to upload an ISO file that is located on your workstation file system. This option is available only when you are connecting to the HMC through a remote browser.

When you select this option:

a. Select **Browse** to find the ISO image file on your workstation file system. You cannot select an ISO image from an HMC media drive. As soon as you select an ISO image file, DPM starts to upload the file, and displays a progress indicator for the upload operation.

b. After the upload operation completes, click **Browse** to search the ISO image file for the INS file that you want to use. Any INS files found are displayed in a separate window. Select only one INS file and click **OK** to close the Browse ISO Image window.

3. When you have finished, click **Next** to navigate to the next page in the task.

Summary

Use the Summary page to verify the information you provided through the preceding steps. You might need to vertically scroll the page to view all of the partition properties. If necessary, click **Back** to return to a particular page to change a property value or setting.

After you have verified the information, click **Finish** to save the partition definition. A progress indicator is displayed until DPM finishes creating the partition.

New Partition Advanced

Accessing the New Partition (Advanced) task

The **New Partition** task guides you through the process of creating a new partition on a Dynamic Partition Manager (DPM)-enabled system.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

You can access this task from the main HMC page by selecting the Systems Management node, by selecting a specific DPM-enabled system, or by selecting the task in the Tasks index. To access this task, you can use either the default SYSPROG user ID or a user ID that a system administrator authorized to this task through customization controls in the **User Management** task.

To create a new partition:

1. Select a DPM-enabled system.
2. From the **Configuration** task group, open the **New Partition** task.
   - If you are selecting this task for the first time, the basic format of the **New Partition** task opens in a new window. In this case, continue to step “3” on page 1126.
   - If you have already set the advanced format as the default format for this task, continue to step “4” on page 1126.
3. To switch from the basic mode to the advanced mode, click **Advanced**, which is located in the lower left corner of the **New Partition** window. Clicking **Advanced** opens a confirmation dialog through which you can set the advanced mode as the default mode whenever you launch the **New Partition** task.
   a. Optional: If you want to set the advanced format as the default format whenever you subsequently launch the **New Partition** task, select the **Always use Advanced** check box. By default, the check box is unchecked.
   b. To open the advanced format of the **New Partition** task, click **Switch** on the confirmation window.
4. Complete the fields in the **General**, **Status**, **Controls**, **Processors**, **Memory**, **Network**, **Storage**, **Accelerators**, **Cryptos**, and **Boot** sections. To access each section, click the link in the navigation frame, or scroll and use the expand and collapse buttons in the section headings, as necessary.

   Note: To access the **Controls** section, you must be using the default SYSPROG or SERVICE user ID, or a user ID that is authorized to one of those two default roles. If you are not logged on with a user ID that has the required authority, the **Controls** section is not displayed.
5. When you have finished, click **OK** to close the task window. A progress indicator is displayed until DPM finishes creating the partition.

When it finishes creating the partition definition, DPM opens the Validation window, which displays a message indicating that your partition has been created, and lists additional tasks that you can use to work with the new partition. To work with the partition, click any of the links on the Validation window to open a related task in a separate window. When you are finished reviewing the information on the Validation window or using the provided links to related tasks, click **Close** to close the Validation window.

New Partition (Advanced)

The **New Partition** task guides you through the process of creating a new partition on a Dynamic Partition Manager (DPM) system.

The **New Partition** task offers two modes through which you can create a partition: basic and advanced. This online documentation describes the advanced mode of the **New Partition** task. For a comparison of the two modes and the implications of switching between them, see "New Partition task modes" on page 1128.

Regardless of the task mode that you use, note that you are only creating a partition, not starting it. After you have finished creating the partition by defining its properties through either task mode, you can start it by using the **Start** task.

The advanced mode task is organized into the following sections, each of which are listed in the navigation pane. To access each section, click the appropriate link in the navigation pane, or scroll down the main page and expand or collapse each section as necessary.

The navigation pane also includes the following links to related tasks.

System Details
Opens the **System Details** task for the DPM-enabled system.

Manage Adapters
Opens the **Manage Adapters** task for the DPM-enabled system.

Monitor System
Switches the foreground window to the **Monitor** tab for the selected DPM system node.

You can find more detailed help on the following elements of this window:

Basic
To switch to the basic mode of the **New Partition** task, click **Basic**. Clicking **Basic** opens a confirmation dialog through which you can set the basic mode as the default mode whenever you launch the **New Partition** task. The confirmation window contains the following controls.

Always use Basic
Sets the basic mode as the default mode whenever you open the **New Partition** task. By default, this check box is unchecked.

Switch
Changes the mode of the task to the basic mode. If you click **Switch** to change to the basic mode, any changes you made while in advanced mode are discarded.

Cancel
Returns to the advanced mode of the **New Partition** task.

For the implications of switching between task modes, see "New Partition task modes" on page 1128.

OK
To close the window, click **OK**.

If you made changes in editable fields in the window, those changes are applied. A progress indicator is displayed until DPM finishes creating the partition.

When it finishes creating the partition definition, DPM opens the Validation window, which displays a message indicating that your partition has been created, and lists additional tasks that you can use to work with the new partition. To work with the partition, click any of the links on the Validation window to open a related task in a separate window. When you are finished reviewing the information on the Validation window or using the provided links to related tasks, click **Close** to close the Validation window.

Cancel
To exit the task without creating a new partition, click **Cancel**.

Help
To display help for the current window, click **Help**.

New Partition task modes

The **New Partition** task offers two modes through which you can create a partition: basic and advanced. Basic is the default mode, but you have the option of setting advanced as the default mode.

Basic
The basic task, which is presented the first time that you open the **New Partition** task, provides a quick, guided method of creating a partition; DPM either provides default values or automatically generates many of the values for partition properties that are required to successfully start a partition. Some of these properties are not displayed or editable in the basic task mode. To navigate through the task, use the **Next** and **Back** buttons. When you have finished entering values in the required fields, click **Finish** to create the partition definition.

Advanced
The advanced task, which you can launch from the basic task, enables experienced users to view all partition properties and to change any default values. To access each section in the advanced task, click the appropriate link in the navigation pane, or scroll down the main page and expand or collapse each section as necessary. When you have finished entering values in the required fields, click **OK** to create the partition definition.

To use the **New Partition** task in either mode, you need to use either the default SYSPROG user ID or a user ID that a system administrator authorized to this task through customization controls in the **User Management** task.

Comparing the task modes

Table 16 on page 1129 lists key partition properties, and indicates whether you can edit those properties using the **New Partition** task in either basic or advanced mode.

- A dash (—) indicates a property that you cannot edit in the basic task mode. DPM either provides default values or automatically generates values for these properties.
- A check mark () indicates a property that you can edit.

*Table 16. Comparison of editable partition properties in the basic and advanced **New Partition** task modes*

Partition property	Basic mode	Advanced mode
Partition name	✓	✓
Partition short name and ID	—	✓
Partition type	✓	✓
Reserved resources	—	✓
Acceptable partition status values	—	✓
Controls: • **Partition access** • **Counter facility authorization** • **Sampling facility authorization**	—	✓ (editing requires SYSPROG or SERVICE user ID)
Shared processors	✓	✓
Dedicated processors	—	✓
Processing weights and capping	—	✓
Memory (initial allocation)	✓	✓
Maximum memory (dynamic allocation)	✓	✓
Network interface cards (NICs)	✓	✓
VLAN ID and MAC address for NICs	—	✓
Storage (storage groups, tape links, or HBAs)	✓	✓ (ability to edit device numbers for FCP storage groups and tape links, and to change adapters for FCP storage groups in this mode only)
Accelerators (virtual functions)	✓ (if supported by the system and installed)	✓ (if supported by the system and installed)
Cryptos (security)	✓ (if installed on system)	✓ (if installed on system) Permitting AES, DES, or ECC protected key import is available in this mode only.
Boot options, including Secure Boot for Linux	✓	✓

Switching between task modes

You have the option of switching between the basic and advanced task modes, and the option of setting the advanced mode as the default mode whenever you subsequently launch the **New Partition** task. To

switch from the basic mode to the advanced mode, click **Advanced**, which is located in the lower left corner of the **New Partition** window. Clicking **Advanced** opens a confirmation dialog through which you can set the advanced mode as the default mode whenever you launch the **New Partition** task.

If you start in basic mode and switch to advanced mode

- If you edited any fields in the basic mode and then switch to the advanced mode, your changes are automatically carried over into the advanced mode. For example, if you entered a name for your new partition on the **Name** page of the basic task, that name is displayed on the **General** page of the advanced task.
- To switch back to the basic task mode, click **Basic**, which is located in the lower left corner of the **New Partition** window.
  - Clicking **Basic** opens a confirmation dialog through which you can set the basic mode as the default mode whenever you launch the **New Partition** task.
  - If you edited **any** fields in the advanced mode, those changes are not preserved when you switch back to the basic mode. However, any edits that you originally made in the basic mode are preserved. In other words, switching from advanced mode to basic mode wipes out all changes that you made in advanced mode, and restores the changes that you made in basic mode.

If you start in advanced mode and switch to basic mode

If you edited any fields in the advanced mode and then switch to the basic mode, your changes are discarded, even if the partition property is available for editing in the basic mode.

General

Use the General section to provide a name and optional description for the new partition.

On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name

Specify the name of the new partition, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. A partition name must uniquely identify the partition from all other partitions defined on the same system.

Description

Optionally, specify a description for the partition. The description can be up to 1024 characters in length.

Short name

Specify the short name of the new partition, which is the name by which the operating system can identify the partition. The short name must consist of 1 - 8 alphanumeric uppercase characters, with the first character is alphabetic; the words PHYSICAL, REC, SYSTEM, and PRIMxxxx (where xxxx is a 4-digit decimal number) are reserved and cannot be used.

- If the short name that you provide has been specified for another partition, the name is valid only if you are not reserving resources for this partition. The best practice, however, is to supply a unique name that identifies the partition from all other partitions defined on the same system. An error or warning message is displayed if the short name is not unique.
- If you do not enter a value for this field, a unique short name is automatically generated.

Partition ID

Specify the identifier (ID) for the new partition if you want it to have the same ID every time that it is started. Select **Generate automatically** to allow the partition ID to be managed by the system; by default, this check box is selected. When **Generate automatically** is selected, the partition has a different ID each time it is started.

The partition ID must be a unique two-character hex number from 00 - 7F. If the partition ID that you provide has been specified for another partition, the ID is valid only if you are not reserving resources for this partition. Even in this case, however, the best practice is to supply a unique ID.

Partition type
Specify one of the following values that identifies the type of partition that you are creating.

Linux
In this type of partition, you can install and run a Linux on Z distribution as a single operating system, or as a hypervisor for multiple guests.

z/VM
In this type of partition, you can install and run z/VM as a hypervisor for multiple Linux guests.

Secure Service Container
This type of partition is a Secure Service Container, in which you can run only specific software appliances that the Secure Service Container supports.

When the selected partition type is **Secure Service Container**, the page display includes the following additional fields.

Master User ID
Enter the user ID to be used as the default master user ID for the Secure Service Container partition. This user ID has authority to perform any task that is available through the Secure Service Container graphical user interface (GUI).

A master user ID can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

Master Password
Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis (), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

Confirm Master Password
Reenter the password exactly as you typed it for the Master Password field.

Reserve resources to ensure they are available when the partition is started
Select this check box only if you want to reserve the configured resources for this partition, which include processors, memory, network interface cards, host bus adapters, virtual functions, and crypto domains.

- When this check box is not selected, other partitions on the system can use these resources when this partition is stopped. In this case, this partition might be unable to start if the required resources are not available.
- When this check box is selected, these resources cannot be used by any other partition on the system, even when this partition is stopped. This selection guarantees that the partition can be started at any point in time.

Status

Use the Status section to define the acceptable availability status values for the partition, based on the importance of its workload. For example, if this partition supports a critical workload on a production server, you might select only Active as an acceptable status value. In contrast, for a partition that supports low-priority software testing, you might select additional values as acceptable. When a partition is started and enters a state that is not selected as an acceptable status, the partition is highlighted in red in various HMC task displays.

You can select one or more status values as an acceptable status for the partition. When you have finished, review another section or click **OK** to save the partition definition.

By default, only Active is selected. Additional status values include the following:

Active
Indicates that the partition has successfully started and is operating normally.

Communications not active
Indicates a problem with the communication between the Hardware Management Console (HMC) and the Support Element (SE).

Degraded
Indicates that the partition successfully started and is operating, but the availability of physical resources to which it has access is less than required, as stated in the partition definition. This status might be acceptable, for example, for partitions that do not have reserved resources.

Paused
Indicates that, because a user has stopped all processors, the partition is not running its workload. In this case, because the partition was successfully started, its resources are shown as active and are still associated with this partition.

Reservation error
Indicates that the availability of physical resources does not match the reserved resources that are stated in the definition for this partition. The partition cannot start until sufficient resources are available.

Starting
Indicates the transitional phase between Stopped state and Active state, as the result of a Start task issued against this partition.

Status check
Indicates that the current status of the partition is unknown. This condition usually occurs under one of the following circumstances:

- When the SE is starting up; in this case, this partition status is temporary.
- When the SE and the DPM-enabled system to which it is attached cannot communicate.

Stopped
Indicates that the partition has normally ended its operation, and exists only as a partition definition.

Stopping
Indicates the transitional phase between Active state and Stopped state, as the result of a Stop task issued against this partition.

Terminated
Indicates that all of the processors for this partition are in a disabled wait state, or a system check stop occurred. The partition is not running its workload. In this case, because the partition was successfully started, its resources are shown as active and are still associated with this partition.

Controls

Use the Controls section to enable or disable partition access to various controls. By default, all settings are unchecked.

Note: To access the **Controls** section, you must be using the default SYSPROG or SERVICE user ID, or a user ID that is authorized to one of those two default roles. If you are not logged on with a user ID that has the required authority, the **Controls** section is not displayed.

Partition Access Controls
You can select one or more of the following security-related controls.

Access global performance data
Select this option:

- To allow the partition to view the CPU utilization data and the Input/Output Processor (IOP) data for all partitions in the configuration. If you do not select this option, the partition is only able to view its own CPU utilization data.
- To enable the collection of FICON channel measurements.

Permit cross-partition commands
Select this option to allow the partition to issue control program commands that affect other partitions; for example, perform a system reset of another partition, deactivate a partition, or provide support for the automatic reconfiguration facility.

CPU-Measurement Counter Facility Authorization Controls

The CPU-measurement counter facility provides a means to measure activities in the CPU and some shared peripheral processors. Select these options only when you want to collect measurement data for performance statistics.

Access basic counter set

Select this option to authorize the use of the basic counter set. This set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches.

Access problem state counter set

Select this option to authorize the use of the problem state counter set. This set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches only when the processor is in problem state.

Access crypto activity counter set

Select this option to authorize the use of the crypto activity counter set. This set includes counters for a central processing unit that are related to the following function counts.

- Pseudo Random Number Generation (PRNG)
- Secure Hash Algorithm (SHA)
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

Access extended counter set

Select this option to authorize the use of the extended counter set. The extended counters provide information about hardware facilities and structures that are specific to a machine family. The extended counters are designed to expand upon information provided by the basic counter set.

CPU-Measurement Sampling Facility Authorization Controls

CPU-measurement sampling facility provides a means to take a snapshot of the CPU at a specified sampling interval. Select this option only when you want to collect measurement data for performance statistics.

Access basic sampling

Select this option to authorize the use of the basic sampling function. Samples are taken and stored at the end of each sampling interval. If you select this option, the Controls display changes to enable you to select an additional option: **Access diagnostic sampling**, which authorizes the use of the diagnostic sampling function.

Processors

Partitions on a DPM system can have only one defined processor type: either Central Processor (CP) or Integrated Facility for Linux (IFL), depending on the processor types that are installed on the system. Use the Processors section to define the type, mode and number of virtual processors for the new partition, and to view various charts that are based on your selections. The processor charts displayed are based on the processor mode that you select. The virtual processors are allocated from physical processors of the selected type.

To work with the information in the Processors section, complete the following steps.

1. If the Processors type field is displayed, select a value. If you want to enable simultaneous multithreading for this partition, you must select the IFL processor type.
2. Select a Processor mode for the processors that the new partition can use. Dedicated processors are typically assigned only to partitions that handle critical workloads.
3. Review the Processors bar chart to determine how many processors are available on this system, and how many are already in use or reserved for other partitions.
4. Select the number of processors that you want to assign to your new partition. If you are creating a partition only to familiarize yourself with the process, you can accept the default value. Otherwise, base your selection on your knowledge of the processing requirements of the operating system and applications that you plan to run in this new partition.

5. Review the Processors bar chart and pie chart to understand how your selection affects the availability of processing resources on the system. Although you can select a number of processors greater than the number that is currently available, your new partition will not start unless currently active, unreserved partitions are stopped or more processors are added to the system.
6. If you have selected shared processor mode for your new partition, select processing weights and capping values to control the use of shared processor resources. The values that you select are dependent on your knowledge of the workloads that these system partitions support. Use the Processing weights pie chart to view the relative weights assigned to your new partition and other active partitions on the system.
7. When you have finished, review another section or click **OK** to save the partition definition.

The following list provides a description of each element in the Processors section. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Processor type
If this field is displayed in the Processors section, select either the **Central Processor (CP)** or **Integrated Facility for Linux (IFL)** processor type. If you want to enable simultaneous multithreading for this partition, you must select the IFL processor type.

If only one type of processor is installed on the system, this field is not displayed.

Processor mode
Select one of the following processor modes.

Shared
Select this option when you want the new partition to share processor resources from the pool of physical processors that are not dedicated to other partitions.

Dedicated
Select this option when you want the new partition to have exclusive use of a specific number of physical processors installed on the system.

Processors
Select the number of shared or dedicated processors for the new partition. You can use one of the following controls to modify the value.

Slider
The minimum value is 1 and the maximum value is the number of entitled processors on the system. The slider not only shows the total range of values that you can select, but also uses color to indicate the current state of processor resources on the system.

- Green indicates the range of available processor resources. If you select a value in this range, you can successfully start the partition.
- Yellow or red indicate the range of processor values that prevent the new partition from starting, or prevent the partition from receiving its required amount of processor resources. This range has a different significance, depending on the selected processor mode and whether you have selected the **Reserve resources** check box in the General section.

  For shared processor mode
  When the processor mode is shared, this range is the number of dedicated processors that are assigned to active and reserved partitions. If you select a number in this range, you receive an inline warning or error message indicating that the processor value you selected is greater than the number of shared physical processors.

  – If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition cannot be started unless the number of shared physical processors on the system is increased.

  – If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its processor resources cannot be reserved unless the number of shared physical processors on the system is increased.

For dedicated processor mode
When the processor mode is dedicated, this range is the sum of the number of dedicated processors assigned to active and reserved partitions, plus the minimum number of shared physical processors required (that is, the largest number of shared processors that is assigned to a single active or reserved partition). If you select a number in this range, the inline warning or error message indicates that the processor value you selected is greater than the number of available physical processors.

- If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition cannot be started unless the number of dedicated physical processors on the system is increased.
- If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its processor resources cannot be reserved unless the number of dedicated physical processors on the system is increased.

Text entry box and number spinner
Using the text box, enter a valid integer within the limits of the slider range. When you enter a value, the slider changes to reflect the value entered in the text box. Alternatively, use the number spinner to increment or decrement the value in the text entry box and slider. Each click increments or decrements the value by one, within the limits of the slider range.

Processors bar chart
Indicates the number of shared and dedicated physical processors on the system. The bar chart scale ranges from 0 to the system design limit. To show the actual number of processors that each bar segment represents, hover your cursor over the colored segment. A dotted line indicates the total number of entitled processors on the system. Entitled processors are processors that are licensed for use on the system; the number of entitled processors might be less than the total number of physical processors that are installed on the system.

To the right of the bar chart, a color legend identifies each segment of the bar chart:

- The number of shared or dedicated processors that you have currently specified for the new partition. This value varies when you change the Processors setting through the slider, text box, or number spinner.
- The number of shared processors, if any, that are available for use by partitions on the system.
- The number of dedicated physical processors that are assigned to active partitions and reserved partitions, if any exist. This number does not reflect any dedicated processors that are assigned to stopped or unreserved partitions.
- The total number of entitled processors on the system. If you have specified a number in the second range (yellow) for the new partition, the total number of processors for all partitions might exceed the number of entitled processors.

Shared Processors pie chart
Indicates the relative distribution of virtual processors for this new partition and all active partitions on the system that are using shared physical processors. This pie chart is displayed only when you have selected Shared as the processor mode.

To the right of the pie chart, a color legend identifies each of the partitions by name. To view details for a specific partition in the pie chart, hover your cursor over the pie wedge with the same color as shown in the legend, next to the partition name. The pie wedge is slightly enlarged and a tooltip displays details for the partition. The tooltip displays the partition name, the number of processors for that partition, and its relative percentage of the total shared partitions, rounded to two decimal places.

At most, the pie chart consists of 12 wedges, one of which is reserved for this new partition. If the system has more than 11 active partitions, the pie chart is divided as follows:

- One wedge for the new partition that you are defining. The wedge size and number of processors vary when you change the Processors setting through the slider, text box, or number spinner.

- One wedge for each of the 10 active partitions with the highest number of processors.
- One wedge that represents all remaining active partitions on the system and the total number of processors shared by this group. In the legend, this group wedge is labeled Others, with the total number of partitions in parentheses.

Processing weight
Select the relative amount of processor time that a specific active partition receives when it is in contention with other active partitions that share the same pool of processor resources. Processing weight options, and a link that opens the **Manage Processor Sharing** task, are displayed only when you have selected Shared as the processor mode.

The processing weight scale ranges from 1 to 999, with specific values labeled as Very Low (100), Low (300), Medium (500), High (700), and Very High (900). These labels are hyperlinks that you can select. Use either the vertical slider on the scale, the hyperlink labels, the text box, or the number spinner to select a value. If you use the number spinner, each click increments or decrements the value by one. The suggested practice is to specify a processing weight that satisfies the peak workload requirements of the partition.

Enforce weight capping
Select this option to enforce weight capping for the partition. When weight capping is enforced, the partition cannot use more processor time than its weight, relative to other partitions that share the same pool of processor resources, even when additional processor resources are available.

Enforce absolute processor capping
Select this option to enforce absolute processor capping for the partition. When absolute capping is enforced, this partition cannot use any more than a specific number of physical processors when it is active. When you select this option, you can enter the absolute capping value, which is the maximum number of physical processors that this partition can use. The absolute capping value ranges from 0.01 - 255.0, in increments of 0.01.

Active Processing Weights pie chart
Indicates the relative distribution of processor weights for this partition and all active partitions on the system. This pie chart is displayed only when you have selected Shared as the processor mode.

To the right of the pie chart, a color legend identifies each of the partitions by name. To view details for a specific partition in the pie chart, hover your cursor over the pie wedge with the same color as shown in the legend, next to the partition name. The pie wedge is slightly enlarged and a tooltip displays details for the partition. The tooltip displays the partition name, its weight value, and its relative percentage of the total processing weight, rounded to two decimal places.

Manage Processor Sharing
Launches the **Manage Processor Sharing** task, which provides the controls through which you can set weights, weight capping, and absolute capping for partitions with shared processors.

Memory

Each partition on a DPM-enabled system has exclusive use of a user-defined portion of the total amount of entitled memory that is installed on the system. Use the Memory page to define the initial and maximum amounts of memory to be assigned to the new partition.

When you define the amount of memory to be assigned, or allocated, to a specific partition, you specify an initial amount of memory, and a maximum amount that must be equal to or greater than the initial amount. The partition receives its initial amount when it is started. If the maximum amount of memory is greater than the initial amount, you can add memory up to this maximum to the active partition, without stopping and restarting it.

To work with the information in the Memory section, complete the following steps.

1. Review the Installed Memory bar chart to determine how much memory is available on this system, and how much is already in use or reserved for other partitions.
2. Select the amounts of initial and maximum memory that you want to assign to your new partition. If you are creating a partition only to familiarize yourself with the process, you can accept the default values for both the Memory and Maximum Memory fields. Otherwise, base your selection on your

knowledge of the memory requirements of the operating system and applications that you plan to run in this new partition.

3. To understand how your selection affects the availability of memory resources on the system, review the updated Installed Memory bar chart.
4. When you have finished, review another section or click **OK** to save the partition definition.

The following list provides a description of each element in the Memory section. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional. You can set the memory amounts in different units: megabytes (MB), gigabytes (GB), or terabytes (TB). The default unit is GB. To change the unit, hover your cursor over the unit in a field label, and select another unit from the popup display. When you change the unit for one field, the same unit change is replicated to the other display elements on the page.

Memory

Define the amount of memory to be assigned to the partition. This value represents the initial amount of memory that the partition receives when it is started. If you set this initial amount to a value greater than the value currently displayed for the Maximum Memory field, the maximum memory is automatically set to the same value. You can use one of the following controls to modify the Memory value. If you are creating a Secure Service Container partition, you must specify an initial amount of at least 4096 MB (4 GB).

Slider

The minimum value that is displayed depends on the unit that you have selected (MB, GB, or TB); for example, the minimum value for the default unit (GB) is 0.5. The maximum value is the amount of entitled memory on the system; this maximum varies by system. The slider not only shows the total range of values that you can select, but also uses color to indicate the current state of memory resources on the system.

- Green indicates the range of available memory values that you can select and successfully assign to the partition.
- Yellow or red indicate the range of memory values that might prevent the partition from starting, or prevent the partition from receiving its required amount of memory resources. This range is the amount of memory that is assigned to active and reserved partitions; it has a different significance, depending on whether you have selected the **Reserve resources** check box in the General section.
  - If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition might fail to start until the amount of available memory on the system is increased.
  - If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its memory resources cannot be reserved unless the amount of available memory on the system is increased.

Text entry box and number spinner

Using the text box, enter a valid integer within the limits of the slider range. When you enter a value, the slider changes to reflect the value entered in the text box. Alternatively, use the number spinner to increment or decrement the value in the text entry box and slider. Each click increments or decrements the value by 0.5, within the limits of the slider range.

Maximum Memory

Define the amount of maximum memory assigned to the partition. The selected value must be equal to or greater than the value specified in the Memory field. If you want this new partition to have access to additional memory resources without having to stop and restart it, specify a value that is greater than the value specified in the Memory field.

The controls (slider, text box and number spinner) are the same as those for the Memory field. The slider ranges and colors also have the same significance as those for the Memory field.

Installed Memory bar chart

Indicates the distribution and amounts of system memory, including the memory assigned to this partition. The bar chart scale ranges from 0 to the total amount of memory that is installed on the system. To show the actual amount of memory that each bar segment represents, hover your cursor over the colored segment.

To the right of the bar chart, a color legend identifies each segment of the bar chart:

- The amount of memory that you have currently specified for this partition. This value varies when you change the Memory setting through the slider, text box, or number spinner.
- The maximum amount of memory that you have currently specified for this partition. This value is represented as a dotted line in the bar chart, and its position moves when you change the Maximum Memory setting through the slider, text box, or number spinner.
- The total amount of allocated memory, which is the total memory assigned to all active and reserved partitions on this system.
- The amount of entitled memory for this system. Entitled memory is the amount of memory that is licensed for use, which might be less than the total amount of memory that is installed on the system. This value is represented as a dotted line in the bar chart.

Network

Network interface cards (NICs) provide a partition with access to internal or external networks that are part of or connected to a system. Each NIC represents a unique connection between the partition and a specific network adapter that is defined or installed on the system.

Use the Network section to create NICs that enable the partition to access the networks connected to the DPM-enabled system. When you create a NIC, you can select the adapter that you want to use from a list of all of the network adapters that are currently configured on the system.

- For availability, select at least two network adapters of the same type, and create a NIC for each one.
- If you are creating a Secure Service Container partition, you must specify at least one NIC for communication with the Secure Service Container web interface.

To work with the information in the Network section, complete the following steps.

1. When you first use the **New Partition** task, the Network display contains an empty NICs table. If you are creating a Secure Service Container partition, the display includes additional information that you need to provide after you successfully define a NIC.

   From the Actions list in the NICs table, select **New** to open the **New Network Interface Card** window.
2. On the **New Network Interface Card** window, define a NIC for each network connection that is required for the operating system or hypervisor that runs on this partition, or for the applications that the operating system or hypervisor supports. For each NIC that you define, complete the following steps. For more detailed descriptions of the **New Network Interface Card** window elements, see "New Network Interface Card" on page 1142.
   a. Enter a unique, meaningful name and, optionally, a description of the new NIC. For partitions with a type of **Linux** or **z/VM** only, you also can optionally specify a virtual LAN (VLAN) identifier only if you plan to select an OSA-Express or HiperSockets adapter. For any type of partition, you can optionally specify a media access control (MAC) address, also only if you plan to select an OSA-Express or HiperSockets adapter.
   b. If you are creating a Secure Service Container partition, the display includes additional information about the network connection that is required to access the Secure Service Container web interface. This information includes an optional, virtual local area network (VLAN) identifier, the required IP address and type, and a mask / prefix.
   c. Review the entries in the Adapter Ports and Switches table to determine which network adapters are configured on the system.

1) Check the percentages listed in the Uplink Utilization and Adapter NIC Allocation columns. If the percentage in either column is high (for example, 90%) for a specific port or switch, consider selecting a different port or switch on the same network.
2) Look for a warning icon next to the name in the Adapter Name column; if the warning icon is displayed for a specific port or switch, select a different one on the same network.
3) Select one port or switch by clicking the radio button in the Select column. Note that, if you select an OSA-Express adapter port other than port 0, you need to manually specify the relative port number through a Linux `qeth` device driver command, before entering the Linux command to bring the device online.

d. Click **OK** to create the new NIC and close the **New Network Interface Card** window.
e. Check the entry for the new NIC that is displayed in the NICs table in the Network section. Change the device number if your company uses a specific numbering convention for its networks.
f. If the new NIC provides access to the Secure Service Container web interface, provide the required network settings that are displayed after the NICs table. If you need more detailed descriptions as you provide these configuration values, see “Secure Service Container Web Interface Communication” on page 1141.

3. Repeat the preceding steps, as necessary, to create a new NIC for each network connection that your new partition requires. If you define multiple NICs for a Secure Service Container partition, use the "Use to access the web interface" switch to identify whether the NIC provides access to the web interface.
4. When you have finished, review another section or click **OK** to save the partition definition.

The following topics describe the NICs table actions and elements, and the elements in the "Secure Service Container Web Interface Communication" section.

The NICs table toolbar

The NICs table contains an entry for each network interface card, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Network Interface Card** window, through which you can create a new network interface card. For more information, see “New Network Interface Card” on page 1142.

Details
Opens the **NIC Details** window. This action is enabled when only one NIC is selected in the table. The **NIC Details** window fields and controls are the same as those for the **New Network Interface Card** window, with the following exceptions:

- The name, description (if any), device number, and adapter port or switch selection are displayed for the selected NIC.
- The Device number field is marked as a required field.
- If the NIC is the only NIC that provides access to the Secure Service Container web interface, the "Use to access the web interface" switch is set on and cannot be set off.

- The Adapter Ports and Switches table contains entries for only those configured ports and switches that have the same card type as the selected NIC, because you cannot change the type of network interface card.

Delete
Opens the **Delete NIC** confirmation window through which you can delete one or more NICs. This action is enabled when one or more NICs are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected NICs. The confirmation window closes, and the resulting NICs table display does not contain any entries for the deleted NICs.
- Click **Cancel** to close the confirmation window and return to the Network section, without deleting any NICs.

Adapter Details
Opens the **Adapter Details** task in a separate window. This action is enabled when one or more NICs are selected in the table.

Columns in the NICs table

The NICs table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a virtual network interface card (NIC). The name is a hyperlink through which you can open the **NIC Details** window. To edit the name, double-click in the table cell and type the new name.

If this NIC represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

IP Address
Displays one of the following values:

- For a NIC that provides access to the Secure Service Container web interface, the value is either a specific IPv4 or IPv6 address or, for IP address types of DHCP and Link Local, the word Automatic.
- For all other NICs, the value displayed is a dash (-).

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the NIC. The operating system to be installed on the partition will use this device number to access the NIC. When creating a new NIC for an OSA card or HiperSockets switch, DPM generates three consecutive device numbers for the operating system to use for unit addresses, and displays only the first number in this field.

Change the device number if your company uses a specific numbering convention for its networks. To edit the device number, double-click in the table cell and type a new hexadecimal value. When you edit the device number for an OSA card or HiperSockets switch, DPM uses this new value as the first device number, and generates two consecutive device numbers based on the new value.

Notes:

- You cannot use a device number of 0000 for a PCI adapter, such as a RoCE adapter.

- The z/VM hypervisor does not support a device number of 0000 for an OSA card or HiperSockets switch.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port
Displays the adapter port value in decimal.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

VLAN ID & Type
Displays the identifier of the virtual local area network (VLAN) through which the network adapter sends and receives network traffic. This field also displays the type of VLAN configuration, such as VLAN Enforcement.

MAC Address
Displays the user-provided or system-generated unique media access control (MAC) address for this NIC.

Description
Displays the user-provided description, if any, of the network interface card. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Secure Service Container Web Interface Communication

The "Secure Service Container Web Interface Communication" section displays network settings that you need to define for the Secure Service Container partition. Some of the values that you supply depend on the IP address type of the NIC that you created to access the web interface. An asterisk (*) preceding the label indicates that a value is required.

Host Name
Enter the Linux host name of the appliance to run in the Secure Service Container partition. To access the Secure Service Container web interface, users need to specify a URL that contains either a host name or an IP address for the Secure Service Container partition. A host name can be 1 - 32

characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (any case), and the following special characters: period (.), colon (:), and hyphen (-).

Default IPv4 Gateway
Enter an IPv4 address for the default gateway. A default IPv4 gateway is required if you specified a Static IPv4 IP address type for the NIC.

Default IPv6 Gateway
Enter an IPv6 address for the default gateway. A default IPv6 gateway is required if you specified a Static IPv6 IP address type for the NIC.

DNS Server 1
Enter an IPv4 or IPv6 address for the primary domain name system (DNS) server. A DNS server definition is required if you specified a Dynamic Host Configuration Protocol (DHCP) IP address for the NIC.

DNS Server 2
Enter an IPv4 or IPv6 address for a secondary DNS server.

New Network Interface Card

Use the **New Network Interface Card** window to create a network interface card (NIC). On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Initially displays a system-generated name for the new NIC, which you can edit by double-clicking in the name field and typing a new name. The NIC name must be different from the name of any other NIC that you define for this new partition.

Description
Optionally, provide a description for this new NIC. The description can be up to 1024 characters in length.

Device Number
Optionally, provide a 4-digit hexadecimal device number in the range 0000 - ffff. If you do not provide a value, the system automatically generates a unique device number. When creating a new NIC for an OSA card or HiperSockets switch, DPM generates three consecutive device numbers for the operating system to use for unit addresses; if you supply a value, the system uses this value as the first device number.

For a NIC that is backed by a PCI-based adapter, DPM generates a unique identifier (UID) that is used as the PCI device number. The value is used only if the operating system supports PCI device numbers.

VLAN ID
For partitions with a type of **Linux** or **z/VM** only, optionally specify the identifier of the virtual local area network (VLAN) through which the network adapter is to send and receive network traffic for this partition and the operating system or hypervisor that it hosts.

- The valid range of VLAN IDs is 1 - 4094.
- You can specify a VLAN ID for this NIC only when you select an OSA-Express or HiperSockets adapter.

  This field is not displayed for partitions with a type of **Secure Service Container**, but you can specify a VLAN ID for that partition type by setting the **Use to access the web interface** switch to **YES**, and entering a value in the **VLAN ID** field displayed in the section under that switch.

VLAN Type
If you provide a VLAN ID, this field, which specifies the type of VLAN configuration, is displayed. The default value is VLAN Enforcement. To complete the setup for VLAN enforcement, you must specify the same VLAN ID in the network configuration files for the operating system or hypervisor.

MAC Address
Optionally, specify a unique media access control (MAC) address that is both locally administered and unicast. A MAC address consists of six groups of two lower-case hexadecimal digits, separated by colons; for example: `02:ff:12:34:56:78`

You can specify a MAC address for any type of partition, but only when you select an OSA-Express or HiperSockets adapter for the NIC. DPM checks the validity and uniqueness of the value that you supply, and issues a message if it finds an error. If you do not specify a value, DPM automatically generates a unique MAC address for the NIC.

Use to access the web interface

Only when the partition type of this partition is **Secure Service Container**, the display includes a switch to indicate whether you can configure this NIC to access the Secure Service Container web interface. When the switch is set to **YES**, the display includes the following configuration settings, which Secure Service Container partitions require for access to the web interface. For a Secure Service Container partition, you can select only an OSA or HiperSockets adapter.

VLAN ID

Specify the virtual local area network (VLAN) if the link you are using is defined in TRUNK mode. The valid range of VLAN IDs is 1 - 4094. Note that DPM does not provide VLAN enforcement for Secure Service Container partitions.

IP Address Type

Select one of the following types:

- **DHCP** (Dynamic Host Configuration Protocol)
- **Link Local**
- **Static IPv4 Address**
- **Static IPv6 Address**

The selected type determines which of the remaining fields require values. An asterisk (*) preceding the label indicates that a value is required.

IP Address

Enter the IP address of the network adapter. This field is required only for IP addresses of type **Static IPv4 Address** and **Static IPv6 Address**.

Mask/Prefix

For an IPv4 address type, enter the mask/prefix in either bit notation (for example, `/24`) or mask notation (for example, `255.255.255.0`). For an IPv6 address type, enter the mask/prefix in bit notation only.

Adapter Ports and Switches table

Lists all of the configured ports or switches for all of the configured network adapters on this system. To successfully define a new NIC, you must select only one table entry.

Select

Enables the selection of table entries. No rows are selected when the table is first displayed. Select only one adapter port or switch for the new NIC.

Adapter Name

Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port

Displays the adapter port value in decimal.

Card Type

Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

Uplink Utilization

Indicates the average uplink utilization for the port or switch over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different port or switch on the same network. The utilization is shown in both a graphic progress bar and in numeric percentage. For

OSA and RoCE adapters, the physical port utilization is displayed; for HiperSockets, the switch utilization is displayed.

Adapter NIC Allocation
Indicates the percentage of NICs that are currently allocated to the adapter for this port or switch. If the percentage is high (for example, 90%), consider selecting a different port or switch on the same network. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes NICs only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Each network adapter port or switch has enough allocation space to support a maximum number of NICs; the maximum number varies depending on the adapter type. If you select a port or switch on an adapter that does not have sufficient allocation space for this new NIC, a message is displayed above the table:

- If you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a port or switch on a different adapter.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the port or adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new NIC, click **OK** to create the NIC definition and close the **New Network Interface Card** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Storage

Use the Storage section to attach storage groups and tape links, or to create host bus adapters (HBAs) that enable the partition to access storage networks and hardware that is connected to the DPM-enabled system.

Depending on the version of DPM that is applied on the system, the Storage section contains a Storage Groups table, a Tape Links table, or an HBAs table with controls that you can use to attach storage groups and tape links, or to create HBAs. Follow the instructions that correspond to the type of table displayed on the page.

- "Attaching storage groups or tape links (DPM R3.1 or later)" on page 1144
- "Accessing FCP storage through HBAs (DPM R3.0 or earlier)" on page 1147

Attaching storage groups or tape links (DPM R3.1 or later)

System administrators create storage groups and tape links to enable partitions (and the operating systems and applications that they host) to use physical storage hardware that is connected to the system. A *storage group* is a logical group of storage volumes that share certain attributes. A *tape link* defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN.

DPM supports the following types of storage groups and tape links.

- FICON storage groups, which consist of volumes that reside on external Fibre Connection (FICON) extended count key data (ECKD) direct-access storage devices (DASD). This type of storage group is available starting with DPM R3.1.
- FCP storage groups, which consist of volumes that reside on external Fibre Channel Protocol (FCP) Small Computer System Interface (SCSI) disk storage devices. This type of storage group is available starting with DPM R3.1.
- Non-Volatile Memory Express (NVMe) storage groups, which consist of solid state drives (SSDs) that are installed in carrier cards in the system I/O drawers. NVMe storage is available only when the system has one or more IBM Adapter for NVMe1.1 features. This type of storage group is available starting with DPM R4.2.
- FCP tape links, each of which defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN. These connection attributes include storage resources such as system adapters, world wide port names (WWPNs), and the number of partitions that can share the connection. Support for FCP tape links is available starting with DPM R4.3.

FICON and FCP storage groups can be shared by multiple partitions, and multiple storage groups can be attached to one partition. FCP tape links also can be shared by multiple partitions, and multiple tape links can be attached to one partition. In contrast, only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared. However, a partition that has attached NVMe storage groups can also have attached FICON and FCP storage groups, and FCP tape links.

To attach one or more storage groups or tape links to the partition, complete the following steps.

1. When you first use the **New Partition** task, the Storage display contains an empty Storage Groups table and Tape Links table. Select the plus icon in the table toolbar to open the **Attach Storage Groups** or **Attach Tape Links** window.
   - On the **Attach Storage Groups** window, select one or more storage groups listed in the Storage Groups table to attach to this partition.
     - The suggested practice is to select storage groups that are in the Complete fulfillment state, but you can select any storage group except for those with a fulfillment state of Incomplete, or those that are already attached to the maximum number of partitions. If you do select groups in states other than Complete, some storage might not be available for use when you start the partition.
     - Use the additional information in the Storage Groups table, as necessary, to decide which storage groups to attach. For descriptions of the columns in the Storage Groups table, see “Attach Storage Groups” on page 1150.

     When you have finished selecting storage groups to attach, select **OK** to close the **Attach Storage Groups** window.
   - On the **Attach Tape Links** window, select one or more tape links listed in the table to attach to this partition.
     - The suggested practice is to select tape links that are in the Complete fulfillment state, but you can select any tape link except for those with a fulfillment state of Incomplete, or those that are already attached to the maximum number of partitions. If you do select links in states other than Complete, some storage might not be available for use when you start the partition.
     - Use the additional information in the table, as necessary, to decide which tape links to attach. For descriptions of the columns in the table, see “Attach Tape Links” on page 1151.

     When you have finished selecting tape links to attach, select **OK** to close the **Attach Tape Links** window.
2. Check the entries for the storage groups or tape links that you selected, which are now displayed in the Storage Groups table or Tape Links table in the Storage section. If necessary, you can use the minus icon in the table toolbar to remove a storage group or tape link from the table.
   - For FCP storage groups and FCP tape links only, you can expand the table entry to show the system-generated host bus adapters (HBAs) and their assigned adapters. You can change the device numbers that DPM automatically assigned to the HBAs when you selected the FCP storage group or FCP tape link. An error icon is displayed if you try to specify a device number that is already in use.

- For FCP storage groups only, the expanded display also includes a link through which you can open the FCP adapter assignment window, and remove or replace the adapters that DPM automatically assigned to the HBAs.

For more details, see the following topics.

- "Host Bus Adapters (HBA) table for an FCP storage group or tape link" on page 1147
- "FCP adapter assignment" on page 1152

3. When you have finished, review another section or click **OK** to save the partition definition.

When you start the new partition, you might need to enter Linux commands to make the storage groups available to the operating system that the partition hosts. NVMe storage groups are automatically detected by the operating system, so you do not need to enter Linux commands to make that type of storage group available to the operating system. Similarly, the tape devices that are available through attached tape links are automatically detected by the operating system, so you do not need to enter Linux commands for tape devices either.

The actions required for FCP or FICON storage groups depend on the type and fulfillment state, and whether the storage group contained the boot volume for the operating system. Typically, the operating system stores the FCP HBA or FICON volume configuration so it can automatically bring the devices online on the next reboot, so you need to take action only for the initial boot of the operating system.

When attaching a storage group in Complete state

- For an FCP storage group:
  - If the storage group contained the boot volume, the operating system brings online all of the HBAs for this storage group, and all volumes in the storage group are available. No action is required unless you have attached other storage groups.
  - If the storage group does not contain the boot volume, and the operating system is not configured to bring HBAs online automatically, you need to issue the **chccwdev** command to bring online all of the HBAs.
- For a FICON storage group, the operating system brings online only the boot volume. You need to issue the **chccwdev** command to bring online all of the remaining volumes in the storage group that contains the boot volume, as well as the volumes in any other storage groups that you attached.

When attaching an unfulfilled storage group that becomes Complete as the partition is running

- For an FCP storage group:
  - If adapters were assigned to HBAs while the partition is running, you need to use the **chchp** command to activate the channel paths for those new adapters.
  - To access the volumes in the storage group, you need to issue the **chccwdev** command to bring online all of the HBAs.
- For a FICON storage group:
  - If the adapters connecting the storage group to the storage subsystem were assigned while the partition is running, use the **chchp** command to activate the channel paths for those new adapters.
  - All volumes are offline. You need to issue the **chccwdev** command to bring online all of the volumes in the storage group.

To find the IDs that you need to use for the Linux commands, use the following tasks.

- HBA device numbers are available in the Host Bus Adapters (HBA) table when you expand the storage group table entry in the Storage section of the **Partition Details** task.
- Channel path IDs for FCP adapters are shown in the Host Bus Adapters (HBA) table when you expand the storage group table entry in the Storage section of the **Partition Details** task.

- Channel path IDs for FICON adapters are shown on the **ADAPTERS** tab of the Storage Group details; open the **Configure Storage** task and select the storage group in the **Storage Overview** to open the Storage Group details page.
- FICON volume device numbers are shown on the **VOLUMES** tab of the Storage Group details page; open the **Configure Storage** task and select the storage group in the **Storage Overview** to open the Storage Group details page.

Host Bus Adapters (HBA) table for an FCP storage group or tape link

For FCP storage groups or tape links only, you can expand the Storage Groups or Tape Links table entry to show the Host Bus Adapters (HBA) table. The following list describes the columns in the table; depending on the fulfillment state of the storage group or tape link, some information might not be available.

Name
Displays the system-generated name of the HBA.

Device Number
Displays the system-generated hexadecimal device number for the HBA. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by typing a new value in the column field.

WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a port in a disk storage subsystem or tape library that is connected to the system.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Adapter ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

Assigned Adapter
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

Accessing FCP storage through HBAs (DPM R3.0 or earlier)

Host bus adapters (HBAs) provide a partition with access to external storage area networks (SANs) and devices that are connected to a system. Each HBA represents a unique connection between the partition and a physical FICON channel that is configured on the system. When you create an HBA, you can select the adapter that you want to use from a list of all of the storage adapters that are currently configured on the system.

- For availability, select at least two storage adapters of the same type, and create an HBA for each one.
- If you are creating a Secure Service Container partition to install a software appliance, define at least one HBA to access the storage device on which the appliance installation image resides.

To create an HBA, complete the following steps.

1. When you first use the **New Partition** task, the Storage display contains an empty HBAs table. From the Actions list in the HBAs table, select **New** to open the **New Host Bus Adapter** window.
2. On the **New Host Bus Adapter** window, define an HBA for each storage area network that is required for the applications that run in this partition. For each HBA that you define, complete the following steps. For more detailed descriptions of the **New Host Bus Adapter** window elements, see "New Host Bus Adapter" on page 1153.
   a. Enter a unique, meaningful name and, optionally, a description of the new HBA.
   b. Review the entries in the Adapter Ports table to determine which storage adapters are configured on the system.
      1) Check the percentage listed in the Adapter HBA Allocation column. If the percentage is high (for example, 90%) for a specific port, consider selecting a different port.

2) Look for a warning icon next to the name in the Adapter Name column; if the warning icon is displayed for a specific port, select a different one.
3) Select one port by clicking the radio button in the Select column.

Click **OK** to create the new HBA and close the **New Host Bus Adapter** window.

c. Check the entry for the new HBA that is displayed in the HBAs table in the Storage section. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by selecting the **Details** action and editing the HBA device number.

3. Repeat the preceding steps, as necessary, to create a new HBA for each storage area network that your new partition requires.
4. When you have finished, review another section or click **OK** to save the partition definition.

The following topics describe the HBAs table actions and elements.

- "The HBAs table toolbar" on page 1148
- "Columns in the HBAs table" on page 1148
- "Standard table functions" on page 1149

The HBAs table toolbar

The HBAs table contains an entry for each host bus adapter, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Host Bus Adapter** window, through which you can create a new host bus adapter (HBA). For more information, see "New Host Bus Adapter" on page 1153.

Details
Opens the **HBA Details** window. This action is enabled when only one HBA is selected in the table. The **HBA Details** window fields and controls are the same as those for the **New Host Bus Adapter** window, with the following exceptions:

- The name, description (if any), device number, and adapter port selection are displayed for the selected HBA.
- The Device number field is marked as a required field.

Delete
Opens the **Delete HBA** confirmation window through which you can delete one or more HBAs. This action is enabled when one or more HBAs are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected HBAs. The confirmation window closes, and the resulting HBAs table display does not contain any entries for the deleted HBAs.
- Click **Cancel** to close the confirmation window and return to the Storage section, without deleting any HBAs.

Adapter Details
Opens the **Adapter Details** task in a separate window. This action is enabled when one or more HBAs are selected in the table.

Columns in the HBAs table

The HBAs table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a host bus adapter (HBA). The name is a hyperlink through which you can open the **HBA Details** window. To edit the name, double-click in the table cell and type the new name.

If this HBA represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Type
Indicates the HBA type, which matches the type of adapter port that is selected when the HBA is created. The valid value is FCP, which represents Fibre Channel Protocol mode.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the HBA. The operating system to be installed on the partition will use this device number to access the HBA. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by selecting the **Details** action and editing the HBA device number. To edit the device number, double-click in the table cell and type a new hexadecimal value.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Description
Displays the user-provided description, if any, of the host bus adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Attach Storage Groups

Use the **Attach Storage Groups** window to select one or more storage groups to attach to the partition. This window contains the Storage Groups table, which lists all storage groups that system administrators have defined for use by partitions on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The Storage Groups table contains the following information and controls.

Select
Use check boxes in the Select column to identify which storage groups you want to attach to the partition. If a check box is disabled, either the storage group is attached to the maximum number of partitions, or you do not have permission to access the storage group.

Name
Specifies the user-defined name of the storage group.

Type
Specifies the type of storage group: FICON or FCP or NVMe.

Partitions
Specifies the number of partitions to which the storage group is attached.

Shareable
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

Total Capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Description
Specifies the user-provided description, if any, of this storage group.

Fulfillment state
Identifies the current state of the storage group. DPM runs a background check of storage resources for FCP storage groups and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours)..

Checking migration
This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

OK
After you have selected one or more storage groups, click **OK** to return to the Storage section of the **New Partition** task.

CANCEL
To close the window without saving any selections, click **CANCEL**.

Attach Tape Links

Use the **Attach Tape Links** window to select one or more tape links to attach to the partition. This window contains a table listing all tape links that system administrators have defined for use by partitions on a system on which DPM R4.3 or a later version is applied.

The table contains the following information and controls.

☐
Use check boxes in each table row or in the table header to identify which tape links you want to attach to the partition. If a check box is disabled, either the storage group is attached to the maximum number of partitions, or you do not have permission to access the storage group.

Name
Specifies the user-defined name of the tape link. The name is a hyperlink that opens to the Tape Link details page in the **Configure Storage** task.

Type
Specifies the type of tape link: FCP.

Partitions
Specifies the number of partitions to which the tape link is attached.

Shareable
Specifies whether the tape link can be shared among partitions, or whether it is dedicated to only one partition.

Description
Specifies the user-provided description, if any, of this tape link. The description can be up to 200 characters in length.

Fulfillment state
Identifies the current state of the tape link. DPM runs a background check of storage resources for FCP tape links and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours).

Complete
All of the storage resources listed in a create or modify request are available, properly configured and zoned, and DPM detects only those resources.

Incomplete
One or more storage resources for the tape link are marked as incomplete because the resource is missing, or in an error or degraded condition. Because DPM periodically checks the availability of storage adapters, switches, and tape libraries that are in use for a tape link, resources that were functioning properly can become incomplete.

Pending
One or more requested storage resources are not yet available or zoned correctly, or the tape link is not yet attached to all partitions that were specified in the original create request or a modify request.

Pending with mismatches
DPM detects system adapters that do not match the original create request or a modify request. Either the number of system adapters does not match the number of connecting paths, or the detected adapters do not match specific adapters that were assigned to the tape link.

OK
After you have selected one or more tape links, click **OK** to return to the Storage section of the **New Partition** task.

CANCEL
To close the window without saving any selections, click **CANCEL**.

FCP adapter assignment

Use the **FCP adapter assignment** window to review the adapters assigned to a storage group and remove or replace them with other adapters that are available for use by a partition. This window is available only on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The **FCP adapter assignment** window displays two tables: Assigned Adapters and Adapter Candidates. Each table contains the same columns and has a footer that indicates the total number of adapters in the table. You might need to scroll to see all table entries, or use the Search field to filter the table entries. The search string applies to both tables. Note that any incomplete adapters are indicated by an incomplete icon ( ).

If an FCP adapter is configured while the storage group is attached to an active partition, DPM cannot detect and list the new adapter as available for use by any partition. To make sure that you can choose from a complete list of available adapters, stop all active partitions to which the storage group is attached, and select the **Connection Report** icon to start a background check of the available connections for this storage group. To view all partitions that are using the storage group, go to **Configure Storage** > **Storage Overview**, open the Storage Details page for the storage group, and select the **PARTITIONS** tab.

If you need to assign new adapters, the Assigned Adapters table contains a placeholder row for each required adapter. To fill those placeholders, use one of the following methods.

- Use the **Automatically assign** icon ( ) to have DPM automatically select redundant adapters across all fabrics. DPM selects the adapters with the lowest allocation percentage and the fastest card type.
- Use the buttons in the Action table column to manually change adapter assignments, one adapter at a time. The suggested practice is to assign at least two adapters from each fabric for redundancy.
  1. In the Assigned Adapters table, select **UNASSIGN** to remove individual adapters.
  2. In the Adapter Candidates table, select **ASSIGN** to assign different adapters. Newly assigned adapters are indicated by a blue dot next to the table row in the Assigned Adapters table.

If you need to change all of the currently assigned adapters, use the **Unassign all** icon ( ) to empty the Assigned Adapters table. Then use either the **Automatically assign** icon or the Action buttons to assign new adapters.

When you have finished, select **SAVE** to return to the Storage section of the **New Partition** task.

The following list describes the columns that are displayed in both of the tables on the **FCP adapter assignment** window.

Adapter Name
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

Adapter ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

Location
Specifies the physical location of the adapter in the I/O drawer of the system.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Allocation
Indicates the percentage of host bus adapters (HBAs) that are currently allocated to this adapter, shown in a bar graph and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. If the percentage is high (for example, 90%), consider assigning a different adapter.

Action
Contains one of the following buttons.

- In the Assigned Adapters table, **UNASSIGN** removes the adapter in the table row and moves the table row into the Adapter Candidates table.
- In the Adapter Candidates table, **ASSIGN** assigns the adapter in the table row and moves the table row into the Assigned Adapters table.

New Host Bus Adapter

Use the **New Host Bus Adapter** window to create a new host bus adapter (HBA). On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Initially displays a system-generated name for the new HBA, which you can edit by double-clicking in the name field and typing a new name. The HBA name must be different from the name of any other HBA that you define for this new partition.

Description
Optionally, provide a description for this new HBA. The description can be up to 1024 characters in length.

Device number
Optionally, provide a 4-digit hexadecimal device number in the range 0000 - ffff. If you do not provide a value, the system automatically generates a unique device number.

Adapter Ports table
Lists all of the configured ports for all of the configured storage adapters on this system. To successfully define a new HBA, you must select only one table entry.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Adapter HBA Allocation
Indicates the percentage of HBAs that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter port. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Each storage adapter port has enough allocation space to support a maximum of 254 HBAs, but your system planner can change that maximum to a lower value. If you select an adapter port that does not have sufficient allocation space for this new HBA, a message is displayed above the table:

- If you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different adapter.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Location
Displays the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the port or adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new HBA, click **OK** to create the HBA definition and close the **New Host Bus Adapter** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Accelerators

An accelerator virtual function provides a partition with access to specific features, such as zEnterprise Data Compression (zEDC), that are installed on a system. Each virtual function represents a unique connection between the partition and a physical feature card that is configured on the system. This section is displayed only when a system that supports accelerators is managed through this HMC, and is enabled only for systems that support accelerators.

Use the Accelerators section to create virtual functions that enable the partition to access specific features installed on the DPM-enabled system. When you create a virtual function, you can select the adapter that you want to use from a list of all of the accelerator adapters that are currently configured on the system.

Accelerators are optional features and, therefore, might not be installed on the system. If none are installed, the Accelerators section is disabled.

To work with the information in the Accelerators section, complete the following steps.

1. When you first use the **New Partition** task, the Accelerators display contains an empty Accelerator Virtual Functions table. From the Actions list in the Accelerator Virtual Functions table, select **New** to open the New Virtual Function window.
2. On the **New Virtual Function** window, define one or more virtual functions for each accelerator that is required for the applications that run in this partition. For each virtual function that you define, complete the following steps. For more detailed descriptions of the **New Virtual Function** window elements, see "New Virtual Function" on page 1156.
   a. Enter a unique, meaningful name and, optionally, a description of the new virtual function.
   b. Review the entries in the Adapters table to determine which accelerator adapters are configured on the system.
      1) Check the percentage listed in the Virtual Function Allocation column. If the percentage is high (for example, 90%) for a specific adapter, consider selecting a different adapter.
      2) Look for a warning icon next to the name in the Name column in the Adapter table; if the warning icon is displayed for a specific adapter, select a different one.
      3) Select one adapter by clicking the radio button in the Select column.
      4) Click **OK** to create the new virtual function and close the **New Virtual Function** window.
   c. Check the entry for the new virtual function that is displayed in the Accelerator Virtual Functions table in the Accelerators section. Change the device number if your company uses a specific numbering convention for its accelerators.
3. Repeat the preceding steps, as necessary, to create additional virtual functions.
4. When you have finished, review another section or click **OK** to save the partition definition.

The following topics describe the Accelerator Virtual Functions table actions and elements.

- "The Accelerator Virtual Functions table toolbar" on page 1155
- "Columns in the Accelerator Virtual Functions table" on page 1155

- “Standard table functions” on page 1156

The Accelerator Virtual Functions table toolbar

The Accelerator Virtual Functions table contains an entry for each virtual function, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Virtual Function** window to create a new virtual function. For more information, see “New Virtual Function” on page 1156.

Details
Opens the **Virtual Function Details** window. This action is enabled when only one virtual function is selected in the table. The **Virtual Function Details** window fields and controls are the same as those for the **New Virtual Function** window, with the following exceptions:

- The name, description (if any), device number, and adapter selection are displayed for the selected virtual function.
- The Device number field is marked as a required field.

Delete
Opens the **Delete Virtual Function** confirmation window through which you can delete one or more virtual functions. This action is enabled when one or more virtual functions are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected virtual functions. The confirmation window closes, and the resulting Accelerator Virtual Functions table display does not contain any entries for the deleted virtual functions.
- Click **Cancel** to close the confirmation window and return to the Accelerators section, without deleting any virtual functions.

Adapter Details
Opens the **Adapter Details** task. This action is enabled when one or more virtual functions are selected in the table.

Columns in the Accelerator Virtual Functions table

The Accelerator Virtual Functions table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the virtual function. The name is a hyperlink through which you can open the **Virtual Function Details** window. To edit the name, double-click in the table cell and type the new name.

If this virtual function represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Type
Indicates the virtual function type, which matches the type of adapter that is selected when the virtual function is created. The valid value is zEDC, for the zEnterprise Data Compression (zEDC) feature, which provides hardware-based acceleration for data compression and decompression.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the virtual function. The operating system to be installed on the partition will use this device number to access the virtual function.

Change the device number if your company uses a specific numbering convention for its accelerators. To edit the device number, double-click in the table cell and type a new hexadecimal value. Note that you cannot use a device number of 0000 for accelerator adapters.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports.

Description
Displays the user-provided description, if any, of the virtual function. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

New Virtual Function

Use the **New Virtual Function** window to create a new virtual function. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Provide a name for the new virtual function. The virtual function name must be different from the name of any other virtual function that you define for this new partition.

Description
Optionally, provide a description for this new virtual function. The description can be up to 1024 characters in length.

Device Number
Optionally, provide a 4-digit hexadecimal device number in the range 0000 - ffff. If you do not provide a value, the system automatically generates a unique device number. The number is used only if the operating system supports device numbers.

Adapter table
Lists all of the configured accelerators on this system.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. Select only one adapter for the new virtual function.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports.

Utilization
Indicates the average utilization for the adapter over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different adapter. The utilization is shown in both a graphic progress bar and in numeric percentage.

Virtual Function Allocation
Indicates the percentage of virtual functions that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes virtual functions only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Up to 15 partitions can share a zEDC feature. If you select an adapter that does not have sufficient allocation space for this new virtual function, a message is displayed above the table:

- If you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different adapter.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new virtual function, click **OK** to create the virtual function definition and close the **New Virtual Function** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Cryptos

The term *cryptos* is a commonly used abbreviation for adapters that provide cryptographic processing functions. Use the Cryptos section to enable the new partition to use the cryptographic adapters that it requires, to assign a usage domain and, optionally, to assign control domains. Usage domains provide access to cryptographic functions, and provide the ability to manage domains and keys. Control domains provide only the ability to manage domains and keys.

Crypto features are optional and, therefore, might not be installed on the system. If none are installed, the Cryptos section is disabled.

When crypto adapters are installed on a system, they are configured in either coprocessor or accelerator mode, depending on the type of cryptographic processing that is required by the applications that run on the system. Each coprocessor or accelerator contains a specific number of usage domains, identified by an index number, which contain an isolated set of master keys. When you create a new partition, you select only one usage domain index to assign to your partition, and that index assignment applies for each cryptographic adapter that your partition can access.

Depending on the type of crypto adapter that you select, you might also need to define one or more control domains.

Additionally, you can enable or disable the key import functions that are available through the CP Assist for Cryptographic Functions (CPACF) feature. CPACF supports clear and protected key encryption based on the Advanced Encryption Standard (AES) algorithm, and the Secure Hash Algorithm (SHA) with the Data Encryption Standard (DES) algorithm, and the Elliptic Curve Cryptography (ECC) algorithm. For operating systems and applications to take advantage of key encryption support, the partition in which they run must be configured to permit AES, or DES, or ECC protected key import functions.

To work with the information in the Cryptos section, complete the following steps.

1. Review the options for the CPACF Key Management Operations that are, by default, selected for this partition. If necessary, click the check box to deselect one or all options.

   Permit AES key import functions
   When selected, this option enables applications that run in this partition to generate and manage AES protected keys through the CPACF feature.

   Permit DES key import functions
   When selected, this option enables applications that run in this partition to generate and manage DES protected keys through the CPACF feature.

   Permit ECC key import functions
   When selected, this option enables applications that run in this partition to generate and manage ECC protected keys through the CPACF feature. Note that only specific systems support the ECC algorithm; if this system does not support ECC, this key import selection is disabled.
2. When you first use the **New Partition** task, the Cryptos display contains an empty Adapters table. From the Actions list in the Adapters table, select **Add** to open the Add Adapters window.
3. On the Add Adapters window, review the list of installed cryptographic adapters in the Adapters table, and select the adapters that your partition needs to use.

   For availability, select at least two cryptographic adapters of the same type.

   a. Check the percentages listed in the Utilization and Usage Domain Allocation columns. If the percentage in either column is high (for example, 90%) for a specific adapter, consider selecting a different adapter.

   b. Look for a warning icon next to the name in the Adapter Name column; if the warning icon is displayed for a specific adapter, select a different one.

   c. Select one or more adapters by clicking the corresponding check boxes in the Select column.

   d. Click **OK** to open the Add Usage Domains window.
4. On the Add Usage Domains window, select one or more domains by clicking the corresponding check boxes in the Select column, and click **OK** to open the Add Control Domains window.

5. On the Add Control Domains window, optionally select one or more control domains by clicking the corresponding check boxes in the Select column, then click **OK** to save your selections and return to the Cryptos section.
6. The Cryptos section display now contains an Adapter Domains table, which lists each selected usage or control domain in a table row, with a table column for each of the selected adapters that are associated with the domain. Depending on how many adapters you selected, you might need to use the horizontal scroll controls to see all of the table columns.
7. In the Adapter Domains table, look for a warning icon in the adapter columns.
   a. If the warning icon is displayed for a specific usage domain on an adapter, click the warning icon to view the other partitions that are also using this domain.

      Although more than one partition can be assigned to the same usage domain index, only one active partition can use that usage domain at any given time. DPM detects whether any other partition definitions contain the same usage domain index for the same cryptographic adapter, and indicates whether any conflicts exist so you can select a different index.
   b. When you have finished reviewing the domain conflicts, click Close to close the window.
   c. To resolve a domain conflict, use the appropriate function in the Actions list in the Adapter Domains table to first remove the domain in conflict, and then to add a new usage domain.
8. When you have finished, review another section or click **OK** to save the partition definition.

The following topics describe the table actions and elements in the Cryptos section.

- "The Adapters table toolbar" on page 1159
- "Columns in the Adapters table" on page 1160
- "The Adapter Domains table toolbar" on page 1161
- "Columns in the Adapter Domains table" on page 1161
- "Standard table functions" on page 1161

The Adapters table toolbar

The Adapters table contains an entry for each cryptographic coprocessor or accelerator, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

Add
Opens the **Add Adapters** window through which you can add one or more crypto adapters to be used by the partition. For more information, see "Adding cryptographic adapters and domains" on page 1162.

Remove
Opens the **Remove Adapters** confirmation window through which you can remove one or more adapters from the partition definition. This action is enabled when one or more adapters are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Remove** to confirm that you want to remove the selected adapters. The confirmation window closes, and the resulting Adapters table display does not contain any entries for the deleted adapters.
- Click **Cancel** to close the confirmation window and return to the Cryptos section, without removing any adapters.

Adapter Details
Opens the **Adapter Details** task. This action is enabled when one or more adapters are selected in the table.

Columns in the Adapters table

The Adapters table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Crypto Number
Indicates the adjunct processor number that is assigned to this adapter. This number is associated with the use of the Adjunct Processor Extended Addressing (APXA) facility, which is only available on specific systems. This facility increases the number of usage domains that can be supported on one cryptographic adapter.

Conflicts
Displays a warning icon in the column, only if one or more domain conflicts exist for a specific adapter. To display additional information about the conflicts, click the warning icon to open the Crypto Conflicts window. For more details, see “Crypto Conflicts - adapter” on page 1164.

Type
Indicates the mode in which the cryptographic adapter is configured on this system.

CCA coprocessor
The adapter is configured as a Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

EP11 coprocessor
The adapter is configured as an Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.

Accelerator
The adapter is configured as an Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific Crypto Express adapter names.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

The Adapter Domains table toolbar

When you first use the **New Partition** task, the Cryptos display contains only an Adapters table; after you add crypto adapters, the display also includes an Adapter Domains table.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

Add Control Domains
Opens the **Add Control Domains** window through which you can add more control domains. For more information, see the Add Control Domains section in "Adding cryptographic adapters and domains" on page 1162.

Add Usage Domains
Opens the **Add Usage Domains** window through which you can add more usage domains. For more information, see the Add Usage Domains section in "Adding cryptographic adapters and domains" on page 1162.

Remove
Opens the **Remove Domains** confirmation window through which you can remove one or more domains from the partition definition. This action is enabled when one or more domains are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Remove** to confirm that you want to remove the selected domains. The confirmation window closes, and the resulting Adapter Domains table display does not contain any entries for the deleted domains.
- Click **Cancel** to close the confirmation window and return to the Cryptos section, without removing any domains.

Columns in the Adapter Domains table

The Adapter Domains table lists each selected usage or control domain in a table row, with a table column for each of the selected adapters that are associated with the domain. Depending on how many adapters you selected, you might need to use the horizontal scroll controls to see all of the table columns.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Displays the index number assigned to each of the usage domains or control domains added to the partition definition. A letter icon that precedes the index number indicates whether the domain is a usage domain (**U**) or a control domain (**C**).

Adapters
Each remaining column in the Adapter Domains table represents a selected adapter, with the adapter name shown as the column heading. For each domain listed in the table, the adapter column displays either a checkmark or a warning icon, to indicate whether any conflicts exist. To display additional information about the conflict, click the warning icon to display the Crypto Conflicts window. For more details, see "Crypto Conflicts - Usage Domain number" on page 1164.

Standard table functions

In addition to the customized action icons and the Actions list, the Adapters table and Adapter Domains table toolbars include the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose

the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Adding cryptographic adapters and domains

When you first select **Add** to add cryptographic adapters to the partition definition, DPM opens a dialog that consists of several windows through which you can select adapters and domains. On any window, you can click **Cancel** to close the dialog and return to the Cryptos section. Otherwise, make a selection and click **OK** to advance to the next window.

In contrast, when you subsequently access the dialog windows through selections in the **Actions** list of the Adapter Domains table, you can access the domain dialog windows separately; DPM opens the appropriate dialog window, based on your selection. Clicking **OK** or **Cancel** returns you to the Crypto section.

The following lists describe the contents of each dialog window, in the order in which DPM presents them. Each window contains a table through which you make your selections; each of these tables has a toolbar with standard table functions, such as filters.

Add Adapters
The **Add Adapters** window displays a table containing one entry for each available crypto adapter that is not already assigned to this new partition. Use the Select column to select one or more adapters for the new partition to use.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Crypto Number
Indicates the adjunct processor number that is assigned to this adapter. This number is associated with the use of the Adjunct Processor Extended Addressing (APXA) facility, which is only available on specific systems. This facility increases the number of usage domains that can be supported on one cryptographic adapter.

Conflicts
Displays a warning icon in the column, only if one or more domain conflicts exist for a specific adapter. To display additional information about the conflicts, click the warning icon to open the Crypto Conflicts window. For more details, see “Crypto Conflicts - adapter” on page 1164.

If you select an adapter that has domain conflicts, a message is displayed above the table:

- If you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different adapter.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because at least one other partition definition contains the same adapter and usage domain.

Type
Indicates the mode in which the cryptographic adapter is configured on this system.

CCA coprocessor
The adapter is configured as a Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

EP11 coprocessor
The adapter is configured as an Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.

Accelerator
The adapter is configured as an Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific Crypto Express adapter names.

Utilization
Indicates the average utilization for the adapter over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different adapter. The utilization is shown in both a graphic progress bar and in numeric percentage.

Usage Domain Allocation
Indicates the percentage of usage domains that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes usage domains only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions cannot exceed 100%.

Each adapter supports up to 16 usage domains, but that limit can be increased through the use of the adjunct processor extended addressing facility, depending on the machine type and configuration of the DPM-enabled system. If you select an adapter that does not have sufficient allocation space, an error message is displayed above the table, indicating that the new partition might fail to start because this adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Add Usage Domains
The **Add Usage Domains** window displays a table containing one entry that represents each available usage domain and control domain, with usage domains listed first, by default. To limit the table entries to only those domains that are not defined to any partition on the system, select the **Hide usage domains defined to other partitions** check box. By default, the check box is checked.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Indicates the index number assigned to the usage domain or control domain. Each coprocessor or accelerator contains a specific number of usage domains, identified by an index number, which contain an isolated set of master keys. When you create a new partition, you select only one usage domain index to assign to your partition, and that index assignment applies for each cryptographic adapter that your partition can access. If you select a control domain, it is converted into a usage domain.

Conflicts
When the **Hide usage domains defined to other partitions** check box is unchecked, the Conflicts column is shown in the table. If a conflict exists for a specific domain, a warning icon is shown in the column. To display additional information about the conflict, click the warning icon to display the Crypto Conflicts window. For more details, see "Crypto Conflicts - Usage Domain number" on page 1164.

If you select a domain that has conflicts, a message is displayed above the table:

- If you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different usage domain.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because at least one other partition definition contains the usage domain for one or more of the same adapters.

Add Control Domains
The **Add Control Domain** window displays a table containing one entry that represents each available control domain.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Indicates the index number assigned to the control domain. Control domains provide only the ability to manage domains and keys. If the partition is configured as the TCP/IP host for the Trusted Key Entry (TKE) workstation, you need to assign control domain indexes to the partition. Otherwise, selecting a control domain is optional. You can select one or more control domains.

Crypto Conflicts - adapter

Use the Crypto Conflicts window to view details about domain conflicts for a specific adapter, the name of which is displayed in the window title. This window contains the Conflicting Partitions table, which contains an entry for each partition for which the definition includes the same cryptographic adapter and usage domains that you have selected for the new partition. The table contains the following columns.

Partition
Displays the name of a partition for which the definition contains one or more adapters or domains that match those you have selected for the new partition. The name is a hyperlink through which you can open the **Partition Details** task.

Active/Reserved
Indicates whether the existing partition is active or reserved. If the partition is either active or reserved, a checkmark is displayed.

Usage Domains
Specifies each of the domain index numbers that conflict with those index numbers you have selected for the new partition. If multiple index numbers are in conflict, each number is separated by a comma; if consecutive index numbers are in conflict, they are shown in ranges. For example: `0-3, 5, 8-10`

To close the window and return to the previous window, click **Close**.

Crypto Conflicts - Usage Domain number

Use the Crypto Conflicts window to view details about the conflicts for a specific usage domain, the index number of which is displayed in the window title. This window contains the Conflicting Partitions table,

which contains an entry for each partition for which the definition includes the same usage domain for one or more cryptographic adapters that you have selected for the new partition. The table contains the following columns.

Partition
Displays the name of a partition for which the definition contains one or more adapters or domains that match those you have selected for the new partition. The name is a hyperlink through which you can open the **Partition Details** task.

Active/Reserved
Indicates whether the existing partition is active or reserved. If the partition is either active or reserved, a checkmark is displayed.

Adapters (Crypto Number)
Displays the name of each adapter that is associated with the usage domain. The name includes the crypto number, which is shown in parentheses. Each adapter name is a hyperlink through which you can open the **Adapter Details** task. If multiple adapters are listed for a specific partition, each adapter is shown on a separate line in the table.

To close the window and return to the previous window, click **Close**.

Boot

Partitions on a DPM-enabled system can host a single operating system or hypervisor. Use the Boot section to select the location of the executables for the hypervisor or operating system to be run in this partition, or to upload the required files to initialize the hypervisor or operating system when the partition itself is started. Some of these boot options require that you find and select an ISO image file, which is a collection of files and metadata for installing software, and an .INS file, which maps image components (for example, kernel, ramdisk, parameter file) to the appropriate storage addresses in main memory.

The "Boot from" menu lists the boot options that are available for the hypervisor or operating system. If an option in the list is disabled, hover your cursor over that option to display additional information for that option. If necessary, take appropriate action to make that selection available; for example, if you want to use the Storage device (SAN) option, return to the Storage page to attach a storage group with a boot volume.

Use the **Secure Boot** option to have DPM verify that the software signature matches the signature from the distributor. If the signature does not match, the boot process ends. This option is enabled only when:

- The partition has a partition type of Linux.
- The system that hosts the partition supports the Secure Boot for Linux function.
- You are booting the Linux operating system from a volume in an FCP or NVMe storage group.

For the supported boot options and more detailed instructions for installing z/VM in a partition, see the *DPM Guide*, which is available through the Library link on IBM Resource Link.

To define a boot option, complete the following steps.

1. Click the down arrow to display the available options in the "Boot from" list.
2. Choose one of the available options and provide any additional information that is required.

   When you select a specific boot option, the display shows editable fields and other information related to the selected option. The following list describes each boot option, and provides instructions for providing any required information.

   None
   Select this option if you want to start a partition without a hypervisor or operating system. Although the partition can be started, it is not in a usable state. This option is the default for partitions with a partition type of **Linux** and **z/VM**.

   Secure Service Container
   This boot option is the default for a Secure Service Container partition. This boot option cannot be changed unless you first change the partition type.

With this option, the display includes the **Boot in Installer Mode** switch, which is set to **YES** and cannot be set to **NO**. With the switch set to **YES**, the partition start process initializes the Secure Service Container Installer so you can install an appliance in the partition.

Storage Group (SAN) or Storage device (SAN)
Select this option when the hypervisor or operating system executables reside on an internal or external storage device. This option is available only when storage groups or host bus adapters (HBAs) are defined for the partition.

When you select this option, the Boot section contains either a Storage Groups table or an HBA table. The Storage Groups table is displayed only when the DPM R3.1 storage management feature or a later DPM version is applied on the system. Follow the instructions that correspond to the type of table displayed on the page.

- "Boot from a boot volume in a storage group" on page 1166 (only for systems with the DPM R3.1 storage management feature or a later DPM version applied)
- "Boot from a boot volume accessed through an HBA" on page 1167

Boot from a boot volume in a storage group

The Storage Groups table displays the available storage groups that contain a boot volume. To view the available boot volumes, expand any table entry by selecting the storage group. The Storage Group table contains the following columns.

Select
Use a radio button in the Select column to identify the storage group that contains the boot volume for the operating system or hypervisor. Depending on the fulfillment state of the storage group and availability of a boot volume, the radio button might be disabled.

Name
Specifies the user-defined name of the storage group.

Type
Specifies the type of storage group: FICON or FCP or NVMe. The expanded table display contains a Boot Volume table that lists all available boot volumes that the storage group contains. The Boot Volume table content and Advanced Boot Volume Settings fields vary, depending on the storage group type. Note that, if you select an FCP storage group as the boot source for Linux, you can select the Secure Boot option, only when the system that hosts the partition supports the Secure Boot for Linux function.

- For each boot volume in an FCP storage group, the Boot Volume table provides the universally unique identifier (UUID) and capacity of the volume, along with a user-supplied description, if any.
- For each boot volume in a FICON storage group, the Boot Volume table provides the name of the storage subsystem in which the volume resides, along with the volume ID, capacity, type, and device number. If a user-supplied description is available, it is also displayed in the table.
- For each boot volume in an NVMe storage group, the Boot Volume table provides the boot volume serial number and capacity, along with a user-supplied description, if any. When you select an NVMe volume, note that NVMe namespace management is not supported, so you can boot programs only from namespace ID=1.
- For descriptions of the optional fields in the Advanced Boot Volume Settings area, see Advanced (optional) boot settings.

Partitions
Specifies the number of partitions to which the storage group is attached.

Shareable
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

Total Capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Description
Specifies the user-provided description, if any, of this storage group.

Fulfillment state

Checking migration
This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

Boot from a boot volume accessed through an HBA

The HBA table displays the available host bus adapters. Select the HBA connected to the storage subsystem that hosts the boot volume, provide the 64-bit worldwide port number (WWPN) of the storage subsystem, and provide the 64-bit hexadecimal logical unit number (LUN) of the volume that contains the boot image. For example:

Target WWPN: `50:0a:09:85:87:09:68:ad` or `500a0985870968` (hexadecimal)
Target LUN: `4021400000000000`

Advanced (optional) boot settings

In addition, you can provide values for the following optional fields. The optional fields in the display vary, depending on whether you selected an HBA, an NVMe storage group, an FCP storage group, or a FICON storage group. If you selected a storage group, the optional fields are displayed under the list of boot volumes in the expanded table entry for the storage group.

Boot program selector (0-30)
The boot program selector is a single number that identifies a boot configuration on the SAN device, which can contain up to 31 (decimal 0 – 30) different configurations. Each configuration can be a Linux kernel, a kernel parameter file, or optionally a ram disk. Configurations are prepared through the Linux zipl tool.

Specifying a value is optional but useful for backup purposes. If you do not supply a value, DPM uses the default value of 0.

Boot record logical block address
The boot record logical block address identifies the entry or anchor point where the boot loader can find the hypervisor or operating system. For Linux operating systems, this address is the master boot record and is usually the first block on the IPL device. Through this optional setting, you can provide a different block address as the entry point. If you provide a value, specify the 64-bit load block address as a 16-digit hexadecimal string.

IPL load parameter
This optional field can contain initial program load (IPL) parameters to be passed to the operating system or hypervisor. You can specify a maximum of eight alphanumeric characters.

OS load parameters
Through this optional setting, you can provide operating system-specific parameters to be passed to the hypervisor or operating system during SCSI IPL (initial program load). The hypervisor or operating system has to support load parameters being passed during IPL.

For a Linux operating system, use this field to specify kernel parameters. During the boot process, these parameters are concatenated to the end of the existing kernel parameters that are used by your boot configuration.

- The specifications must contain ASCII characters only. If characters other than ASCII are present, the content of the field is ignored during IPL.
- If you specify the kernel parameters with a leading equal sign (=), the existing kernel parameters are ignored and replaced with the kernel parameters in this field.
- If you replace the existing kernel parameters, be sure not to omit any kernel parameters required by your boot configuration.

You can also specify load parameters to log in to the operating system or hypervisor through either the **Operating System Messages** task or the **Integrated 3270 Console** task:

- For the **Operating System Messages** task, type `sysc`
- For the **Integrated 3270 Console** task, type `sysg`

Network server (PXE)
Select this option when you want to use a preboot execution environment (PXE) on a network server. This option is available only if a network interface card (NIC) for either an OSA port or HiperSockets switch is defined for the partition.

When you select this option, the NIC table displays the available network interface cards. Select the NIC for the adapter that connects the partition to the network on which the network boot server resides.

FTP server
Select this option if you want to use FTP to boot an image that is located on a different system. Provide the following information:

Host name
Enter either the fully qualified domain name of the FTP server, or its IP address.

User name
Enter the user name on the target FTP server.

Password
Enter the password associated with the user name on the target FTP server.

INS file
Either click **Browse** to retrieve a list of INS files from the target FTP server and select one file, or enter the fully qualified name (relative to FTP root) of an INS file.

Depending on the size of the FTP site, browsing might require more time than manually entering the full path and name of the INS file. Also note that the browsing function returns INS files found in the user's home directory or its subdirectories. Because you cannot select a starting directory, or navigate to a directory above the user's home directory, manually entering the full path and name of the INS file might be more expedient.

If you click **Browse**, a separate window displays the user's home directory and its subdirectories. Select one INS file, and click **OK** to close the Browse FTP Server window.

FTPS server
Select this option if you want to use the FTP Secure (FTPS) protocol to boot an image that is located on a different system. FTPS uses the Secure Socket Layer (SSL) protocol to secure data.

With this option, you need to supply a host name, user ID, password, and .INS file, as described for the **FTP server** boot option.

SFTP server
Select this option if you want to use the Secure File Transfer Protocol (SFTP) to boot an image that is located on a different system. SFTP uses the Secure Shell (SSH) protocol to secure data. With this option, you need to supply a host name, user ID, password, and .INS file, as described for the **FTP server** boot option.

Hardware Management Console removable media
Select this option if you want to use an INS file from a media drive that is connected to the HMC. The media drive must be available when you are creating the partition definition and when the partition is started. Possible drive selections are **CD/DVD drive** or **USB flash memory drive**, depending on what media drives are installed in the HMC.

When you select this option:

a. If more than one type of media drive is available on the HMC, select the radio button for the media drive on which the INS file resides. Otherwise, skip to the next step.
b. Either enter the fully qualified name (relative to the mount point) of an INS file, or complete the following steps.
   1) Select **Browse** to start a search on the target media drive to retrieve a list of INS files. Any INS files found are displayed in a separate window.
   2) Select only one INS file and click **OK** to close the Browse Removable Media window.

ISO image
Select this option when you want to upload an ISO file that is located on your workstation file system. This option is available only when you are connecting to the HMC through a remote browser.

When you select this option:

a. Select **Browse** to find the ISO image file on your workstation file system. You cannot select an ISO image from an HMC media drive. As soon as you select an ISO image file, DPM starts to upload the file, and displays a progress indicator for the upload operation.
b. After the upload operation completes, click **Browse** to search the ISO image file for the INS file that you want to use. Any INS files found are displayed in a separate window. Select only one INS file and click **OK** to close the Browse ISO Image window.

3. Review the boot loader time-out setting and, if necessary, change it. By default, the time-out setting for most boot options has a value of 60 seconds. For only the **Network server (PXE)** boot option, the default time-out setting is 600 seconds, to account for network traffic. If the boot loader takes longer than the time-out value to load the hypervisor or operating system executables, DPM cancels the operation and issues an error message.
4. When you have finished, review another section or click **OK** to save the partition definition.

Object Locking Settings

Accessing the Object Locking Settings task

This task allows you to control whether managed objects are automatically locked and whether they are re-locked after being used as target objects for a task.

To lock or unlock objects:

1. Open the **Object Locking Settings** task. The Locking window is displayed.
2. Select the setting you want set for the object.
3. Click **OK** to proceed or **Cancel** to exit the task without changing the setting.

Locking

You can control whether managed objects are to be automatically locked after changes to this window are applied or they are locked automatically after used as target objects for a task. Changes apply only to objects that support lockout disruptive tasks

Customize the settings to indicate your preferences, then click **OK**.

Automatically lock all managed objects
To control whether or not managed objects, such as Central Processor Complexes (CPCs) or their images, should be automatically locked after they are used as target objects for a task, select **Automatically lock all managed objects**.

- If this is not selected (no check mark appears), the managed objects are not to be automatically locked after they are used as target objects for a task.
- If this is selected (a check mark appears), the managed objects that support lockout disruptive tasks are to be automatically locked when the changes to this window are applied. In addition, all managed objects are to be locked when the console is started and an object is automatically locked when created.

Relock after a task has been run
To relock the managed objects after a task has been run, select **Relock after a task has been run**.

OK
To customize the settings to your selected preferences, click **OK**.

Reset
To discard any changes you made to the settings in this window and to re-display the current settings for this window, click **Reset**.

Defaults
To return to the object locking settings that are the default for the current user, click **Defaults**.

Cancel
To exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Offload Problem Analysis Data to Removable Media

Accessing the Offload Problem Analysis Data to Removable Media task

Note: You cannot perform this task remotely.

Problem Analysis is a set of subdirectories that contain all the files that would have been transmitted to the support system if a connection to support system were available. A subdirectory is dynamically created for each problem reported on a machine that was unable to send data to the support system.

To offload the data for a given problem within one of these subdirectories directly to removable media on the Hardware Management Console:

1. Open the **Offload Problem Analysis Data to Removable Media** task. The Problem Analysis Data Offload window is displayed.
2. Select the *problem number* of the subdirectory you want to offload from the list.
3. Insert a formatted removable media.
4. Click **OK**. The offload process takes several minutes to complete, depending on the size and quantity of the files to be transferred to removable media.

Offload Problem Analysis Data to Removable Media

Problem analysis is a set of subdirectories that contain all the files that would have been transmitted to the support system if a connection to the support system were available. A subdirectory is dynamically created for each problem reported on a machine that was unable to send data to the support system. You

can offload the data for a given problem within one of these subdirectories directly to removable media on the Hardware Management Console.

The label of each subdirectory represents a problem number.

Use this window to choose which problem data to offload to removable media. Load a removable media which is formatted with no volume label or a volume label of VIRTRET into the removable media drive. Select the problem number from the list in the window; then, click **OK** to begin the offload.

The offload process takes several minutes to complete, depending on the size and quantity of the files to be transferred to removable media.

After the offload process is started, a busy dialog is displayed while the process is in progress. After the process has completed, a message window is displayed indicating that the offload was completed successfully or that an error was encountered during the offload.

Possible error messages include:

- Error transmitting data to the Hardware Management Console.
- Media does not have enough space for file offload.
- Format removable media with VIRTRET as volume label.
- There is no problem analysis data to offload.
- Error mounting, media not inserted...
- Error mounting, unrecognized file system... possibly unformatted media.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again

Problem number
A problem number corresponds to the label of each subdirectory. Select a problem number in the list to select the problem data to offload to the removable media.

OK
To begin the offload for the problem number you selected, click **OK**.

Cancel
To close the window without performing the offload, click **Cancel**.

Help
To display help for the current window, click **Help**.

Operating System Messages

Accessing Operating System Messages

Displays consolidated operating system generated messages for all selected images. These messages are available to all default user IDs.

An image is a set of central processor complex (CPC) resources capable of running a control program or operating system. An operating system running in an image sends messages to operating system consoles to notify you of significant events that involve or affect the use of the operating system. The messages are referred to as *operating system messages*.

If an operating system running in an image supports console integration and is customized to allow using the console as an operating system console, then the console can also receive operating system messages.

An operating system may issue any number of messages at any time. The console receives the messages automatically and stores them in a message log. The console also turns on several console indicators to

help you recognize that priority or held operating system messages were received. A *priority* or held operating system message either requires a response from the console operator or notifies the console operator of a critical condition that requires immediate attention.

The console can store an average of approximately 200 (depending on the length of each message) messages in its operating system message log per image. If the message log becomes full, the console continues to receive and store new messages, but deletes one or more of the log's oldest non-held, non-priority messages to make room for each new message. If there are not any non-held, non-priority messages, the oldest non-held priority, held, or priority message will be deleted.

Coupling Facility Control Code (CFCC) commands can be sent from the Hardware Management Console to a CF.

For more information about the CFCC commands and messages, expand the **Introduction** section from the help Table of Contents to locate **CFCC Messages** and **CFCC Commands**.

Note: Depending on your user task role, you may only be able to view the operating system messages.

To display the **Operating System Messages:**

1. Select the desired CPC or images.
2. Open the **Operating System Messages** task.
3. The Operating System Messages window opens.
4. Select the operation you want to perform from the Operating system Messages.

Operating System Messages

If operating systems running in one or more Central Processor Complex (CPC) images support console integration and are customized to allow by using the console as an operating system console, then use **Operating System Messages** to:

- Display, manage, and respond to operating system messages from the CPC images.
- Send operating system commands to the CPC images.

Note: This task may be view only for some user task roles.

Console integration is a facility of the console. An operating system that supports console integration can be customized to allow by using the console, if necessary, as an operating system console.

Under normal conditions, while other operating system consoles are available, the console should *not* be used as an operating system console. That is, the console integration facility is not intended to make the console the primary user interface to an operating system.

The console integration facility is intended instead to allow by using the console as an operating system console only when other operating system consoles are not available. For example, other operating system consoles are not available:

- During initialization of the operating system
- During outages or failures
- For Coupling Facility Control Code (CFCC).

This window displays and manages messages that are issued by operating systems running images managed by this console.

System
Select the operating system running image from the drop-down list to display system their messages.

Toolbar
Click the toolbar icons or **Actions** drop-down arrow to perform the following:

Respond 

Enter a response to the selected message from the partition list you want to send a message, then click **Send**. You can also right-click on the message from the list, and then click **Respond**.

If the operating system sent a default response for the selected message, then the default response displays in this field. Otherwise, you can specify any other response, up to 200 characters.

Note: The **Respond** icon does not display if the current operating system does not support the **Respond** function.

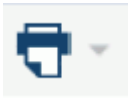
Delete 

Delete selected messages for the partition list, then click **Yes**. You can also right-click on the message from the list, and then click **Delete**

Export 

Select from the drop-down arrow to **Export as HTML** or **Export All to CSV** messages for the selected running system image.

Note: The **Export** and **Print** options are available remotely only.

Print 

Select from the drop-down arrow to **Print All** messages, **Print Selected** messages, or **Print Preview** display of messages for the selected running system image.

Note: The **Export** and **Print** options are available remotely only.

Actions

Select from the drop-down arrow to **Delete** or **Respond** to a message for the selected running system image.

Note: The **Export** and **Print** actions are available remotely only.

Filter

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Message

Displays operating system messages for the current selected image and any message that was received.

Command

Enter a command message to send to the operating system, then click **Send**.

Priority message

Sends message commands with greater importance when checked.

Note: Some systems do not accept priority messages.

Close

To close the current window, click **Close**.

Help

To display help for the current window, click **Help**.

Viewing operating system messages

View operating system messages to remain informed of events that involve or affect the use of images supported by the central processor complex (CPC). Upon viewing operating system messages, you can also:

- Send responses to messages.
- Delete messages you no longer need.
- Use the online Help for more information to view, respond to, or delete operating system messages.

To view operating system messages:

Black
Indicates an informational message that normally does not require a response from the console operator.

Blue
Indicates a held message that requires a response from the console operator.

Red
Indicates a priority message about a critical condition that requires immediate attention.

Responding to an operating system message requires receiving an operating system message first. You can use **Operating System Messages** also to send commands to an operating system, regardless of whether you've received messages from it.

Sending commands to the operating system

You can use the console to send commands, at any time, to operating systems running in images supported by the central processor complex (CPC).

To send commands to an operating system:

1. Locate a target: either a group of images or individual images. Using a group of images allows sending commands to each operating system running on images in the group, while using individual images allows sending commands to their operating systems only.
2. Locate and open the **Operating System Messages** task.

   This opens the Operating System Messages window. The window lists the operating system messages, if any, from each image in the target group or among the selected images.
3. If the current operating system supports priority messages, a priority checkbox displays on the window. Select the checkbox to send a priority message.
4. Enter a command in the **Command** field.
5. Click **Send** to send the command to the operating system running on the images.

   Note: The **Priority** checkbox is not available if the operating system running on an image does not support receiving priority commands from the console.

Related information

- Refer to the publications provided with your operating system for more information about whether it supports console integration, and how to customize it to allow using the console as an operating system console.
- You can use the **Operating System Messages** task to receive messages from and send commands to an image running Coupling Facility Control Code (CFCC). For more information on the CFCC commands and CFCC messages, expand the **Introduction** section from the help Table of Contents to locate:
  - Coupling Facility Control Code (CFCC) Commands
  - Coupling Facility Control Code (CFCC) Messages

OSA Advanced Facilities

Accessing the OSA Advanced Facilities task

The Open Systems Adapter (OSA) is an integrated hardware feature plug-in as a channel card, becoming an integral component of the I/O subsystem, enabling convenient Local Area Network (LAN) attachment. This brings the strengths of the architecture to the client/server environment: security, availability, enterprise-wide access to data, and systems management.

Note: Depending on your user task role, you may only be able to view this task.

You can use the Hardware Management Console to open a facility for monitoring, operating, and customizing an OSA channel.

To work with an OSA channel:

1. Select a CPC (server).
2. Open the **OSA Advanced Facilities** task. The OSA Advanced Facilities window is displayed.
3. The OSA Advanced Facilities window displays.
4. Use the OSA Advanced Facilities table and drop-down actions to launch OSA channel tasks.

OSA Advanced Facilities

The Open Systems Adapter (OSA) is an integrated hardware feature plug-in as a channel card, becoming an integral component of the I/O subsystem, enabling convenient Local Area Network (LAN) attachment. This brings the strengths of the architecture to the client/server environment: security, availability, enterprise-wide access to data, and systems management. Use this window to select the Open System Adapter (OSA) channel you want to work with.

The window lists all OSA channels for the Central Processor Complex (CPC).

PCHID
Displays the PCHID assigned to the OSA channels

Hardware Type
Displays the hardware types for the OSA channels

Status
Displays the status for the OSA channels

CHPID Type
Displays the CHPID type for the OSA channels

Code Level
Displays the machine code level for the OSA channels

Port 0 Status
Displays the Port 0 status for the OSA channels

Port 0 MAC Address
Displays the Media Access Control (MAC) Port 0 for the OSA channels

Port 1 Status
Displays the Port 1 status for the OSA channels

Port 1 MAC Address
Displays the Port 1 Media Access Control (MAC) Port 1 for the OSA channels.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Note: Most drop-down menu actions are not available when OSA channels are offline.

- “View port parameters” on page 387
- “Display OSA Address Table (OAT) Entries” on page 388
- “Export adapter diagnostic data” on page 387

- Card Trace/Log/Dump Facilities
- “Card Specific Advanced Facilities” on page 391
- Reset To Defaults

The icons perform the following functions in the PCI service partition table:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Close
To close the window and exit the task, click **Close.**

Help
To display help for the current window, click **Help**.

View port parameters

The view port parameters window displays various information about the selected port on the channel. This information (which varies based on channel hardware type and specified CHPID type) can contain current connection speed/mode, configured speed/mode, counter for various data items processed, as well as counters for various errors detected.

Additional functions on this window include:

Close
To close the current window, click **Close**.

Export to USB Flash Memory Drive
To export the selected channel port parameter data to a USB Flash Memory Drive, click **Export to USB Flash Memory Drive**.

Export to FTP Location
To export the selected channel port parameter data to an FTP location, click **Export to FTP Location**.

Help
To display help for the current window, click **Help**.

View port parameters

The view port parameters window displays information about the selected port on the channel.

Channel Path:
Identifies the channel path for the selected port on the channel.

LAN port type:
Identifies the LAN port type for the selected port on the channel.

Physical port identifier:
Enter the port identifier or use the drop-down arrow to select an existing port identifier.

Additional functions on this window include:

OK
To display details of the selected physical port identifier, click **OK**.

Cancel
To close the window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Export adapter diagnostic data

Use this window to export all the adapter diagnostic data for the OSA channels defined on the system. Verify the **User name** is the specific FTP destination. Use the **File path** field to type the fully qualified path destination.

The export function copies of a source file from the console to the FTP destination:

Host name
Specify the host computer of the FTP source.

User name
Specify the user name for the target FTP destination.

Password
Specify the password for the user ID.

Protocol
Select this option to enable a secure FTP connection to your server.

File path
Specify the fully qualified file path for the target file.

Additional functions on this window include:

Export
To export the OSA channel diagnostic data to an FTP location, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel**.

Help
To display help for the current window, click **Help**.

Display OSA Address Table (OAT) Entries

Use this window to configure the OSA for the OSE, OSD, or OSN defined channel type in TCP/IP Passthru, SNA modes, or both concurrently.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSE, OSD, or OSN defined channel type.

LAN port type
Identifies the type of network the selected OSE, OSD, or OSN defined channel type can be connected to through cable connections to its port or ports.

The Edit OSA Address Table (OAT) entries define

CSS
Displays the channel subsystem (CSS) for the selected OSE, OSD, or OSN defined channel type.

IID
Displays the logical partition ID assigned to the selected OSE, OSD, or OSN defined channel type.

Unit Address
Displays the unit address assigned to the selected OSE, OSD, or OSN defined channel type.

Device Number
Displays a unique number that is assigned for each device that was defined in the IOCDS for the OSE, OSD, or OSN defined channel type.

LPAR Name
Displays the name of the logical partition assigned to the OAT entry.

Port Number
Displays the number that uniquely identifies the port for the selected OSE, OSD, or OSN defined channel type.

Session Type
Displays one of the following active session types for the selected OSE, OSD, or OSN defined channel type:

- TCP/IP
- SNA

IP Address
Indicates the client's IP address for the selected OSE, OSD, or OSN defined channel type.

Isolated
Indicates if the OAT entries are in isolation mode.

Router Indicator
Indicates the router identifier.

The icons perform the following functions for the selected OSE, OSD, or OSN defined channel type in the Edit OAT Entries table:

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this downloaded CSV file into most spreadsheet applications.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Additional functions on this window include:

Save
To save the configuration values for selected OSA defined OCE channel type, click **Save**.

Cancel
To close the window without saving the current selected changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit OSA Address Table (OAT) Entries

Use the Edit OSA Address Table (OAT) Entry window to define which devices the OSA for the selected OSE defined channel type uses to transfer data and commands to/from each attached host. For a TCP/IP Passthru mode, an OSA transfers data between a host IP program, to which it is defined, and certain clients on the networks. For SNA mode, an OSA acts as a SNA passthru agent to the clients that use the SNA protocol on the LAN that is directly attached to the OSA.

Port Number
Use the drop down box to select or type the port number for the selected OSE defined channel type.

CSS
Use the drop down box to select or type the channel subsystem (CSS) for the selected OSE defined channel type.

Image Number
Use the drop down box to select or type the logical partition number of the LPAR for the selected OSE defined channel type.

Unit Address
Use the drop down box to select or type the address for the selected port for the OSE defined channel type..

Default entry indicator
Select Primary for one of the LPARs using the selected OSA port for the OSE defined channel type. The LPAR designated as the Primary receives any datagrams that are not specifically addressed to any of the home IP addresses associated with the selected OSA port.

Home IP address
Enter the TCP/IP Home IP addresses for the selected OSE defined channel type.

Additional functions on this window include:

OK
To save the new values, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Advanced Facilities

Use this window to select a function to monitor, operate, or customize a selected channel type for the system. The list of actions you can take from the list depends on the channel type selected. The list may include:

- Force error recovery log
- Card display or alter memory...
- View code level
- Card trace/log/dump facilities
- “Card Specific Advanced Facilities” on page 391
- Look up generic access...
- Reset to defaults...

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Force log

Use this window to select a force log function for the selected Integrated Coupling Adapter (ICA) SR channel type in the system.

Channel ID:
Displays a four-digit physical channel identifier (PCHID) of the selected Integrated Coupling Adapter (ICA) defined channel type.

Channel type:
Identifies specific channel type

Card description:
Displays the card description for the channel type.

Select a force log function for the selected Integrated Coupling Adapter channel type:

- Force adapter error recover log
- Force port error recover log
- Force channel error recover log
- Force adapter log
- Force channel log

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Card Specific Advanced Facilities

Use this window to select a card specific function for a selected channel type for the system. The list of card specific facilities actions you can take from the list depends on the channel type selected. The list may include:

- Query port status...
- Display or alter MAC address...
- Enable or disable ports...
- Run port diagnostics
- Set card mode...
- Display client connections...
- Display active sessions configuration...
- Display active server configuration...
- Panel configuration options...
- Manual configuration options...
- Activate configuration
- Display activate configuration errors...
- Debug utilities...
- Manage security certificates...

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Query port status

Displays the local area network (LAN) port record of each LAN port on the selected Open Systems Adapter (OSA)-Express channel.

A LAN port record:

- Displays the port identifier
- Indicates whether the port is enabled or disabled
- Indicates whether the port is in Support Element control mode
- Indicates the source of the command that disabled the port if the port becomes disabled while it is not in Support Element control mode.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Query port table

First line list column:

Port ID
Displays the number that uniquely identifies the port on the OSA-Express card.

Type
Identifies the type of LAN supported by the port.

Port state
Indicates the current state of the port.

Disabled
Indicates if the port was disabled by the Support Element.

External disabled
Indicates if the port was disabled by an external LAN request.

Host program disabled
Indicates if the port was disabled by a host support program.

Second line list column:

Port ID
Displays the number that uniquely identifies the port on the OSA-Express card.

Support Element Control Mode
Indicates if the port accepts commands only from its Support Element.

Port Configuration Change
Indicates if the port has changed configuration.

Port Failure
Indicates if a licensed internal code problem has occurred which stops the port from being enabled.

Link Threshold Exceeded
Indicates if the port has been disabled because the number of link failures has exceeded the threshold.

Link Monitor
Describes why the port is in Link Monitor State. This is a bit field. The bits are numbered from left (bit 0) to right (bit 15).

- Bit 0: *loss of signal* - most likely cause is an improperly installed or broken cable. Please check your connection or cable.
- Bit 1: *not used*.

- Bit 2: *registration failure* - registration was rejected by ATM switch or the switch is not operational. This is most likely the result of the configuration not matching the configuration of the LES. Fix the configuration and make sure that the required switch is operational.
- Bit 3: *loss of SAAL connection* - this is set when there is a problem with the communication to the switch. Have your network person check the switch connection.
- Bit 4-15: *Reserved*

Definition Error Code
Describes why the port is in Definition Error State.

- "00" - Unspecified Error
- "01" - Invalid Type
- "02" - Invalid Parameter

Additional functions on this window include:

OK
To close the window when you finish reviewing the LAN port records, click **OK**.

Help
To display help for the current window, click **Help**.

Query port status

Displays the local area network (LAN) port record of each LAN port on the selected Open Systems Adapter (OSA)-Express channel.

A LAN port record:

- Displays the port identifier
- Indicates whether the port is enabled or disabled
- Indicates whether the port is in Support Element control mode
- Indicates the source of the command that disabled the port if the port becomes disabled while it is not in Support Element control mode.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Query port status table

Port Identifier
Displays the number that uniquely identifies the port on the OSA-Express card.

Type
Identifies the type of LAN supported by the port.

Port State
Indicates the current state of the port.

Disable
Indicates if the port was disabled by the Support Element.

Support Element Control Mode
Indicates if the port accepts commands only from its Support Element.

Port Block
Indicates the port was disabled by a LAN request.

External Disabled
Indicates if the port was disabled by an external LAN request.

Internal Port Failure
Indicates if a licensed internal code problem has occurred which stops the port from being enabled.

Additional functions on this window include:

OK
To close the window when you finish reviewing the LAN port records, click **OK**.

Help
To display help for the current window, click **Help**.

View port parameters

The view port parameters window displays various information about the selected port on the channel. This information (which varies based on channel hardware type and specified CHPID type) can contain state, current connection speed/mode, configured speed/mode, counter for various data items processed, as well as counters for various errors detected.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected zHyperLink or RoCE Express2 channel.

Port
Identify the physical port of the selected zHyperLink or RoCE Express2 channel.

Additional functions on this window include:

Close
To close the current window, click **Close**.

Export to USB Device
To export the selected channel port parameter data to a USB Device, click **Export to USB Device**.

Export to FTP Server
To export the selected channel port parameter data to an FTP Server, click **Export to FTP Server**.

Help
To display help for the current window, click **Help**.

Display or alter MAC address

Displays the medium access control (MAC) addresses of the ports on the selected Open Systems Adapter (OSA)-Express channel.

You can also use the window to change one or more MAC addresses.

Note: This window might only allow view only for some user task roles.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

MAC address LAN port *n*
Initially displays the current medium access control (MAC) address of port number *n*. Each field in the group displays the hexadecimal value of one byte in the 6-byte (48-bit) MAC address of the port. The leftmost field displays byte 0; the rightmost field displays byte 5.

Use the fields to change the MAC address of the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Retrieve Universal MAC
To display the universally administered medium access control (MAC) address of each port, click **Retrieve Universal MAC**.

Note: This only displays each port's universal MAC address in its **MAC address LAN port *n*** field.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Enable or disable port

Use this window to enable or disable the local area network (LAN) ports for the selected Open Systems Adapter (OSA)-Express channel and to set the Support Element control mode of the port.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Attention: Make sure the port is not being used by other partitions before it is disabled.

Port number
Identify the port of the selected Open Systems Adapter (OSA)-Express channel.

Port status commend

Enable port
Enable a port to allow it to communicate with other devices attached to the LAN. An enabled port can receive information from other devices attached to the LAN, and can send information to them.

Disable port
Disable a port to prevent it from communicating with other devices attached to the LAN.

Support Element control code command

Set control on
Set the Support Element control mode of a port on.

Set control off
Set the Support Element control mode of a port off.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Run port diagnostics

Use this window to test the hardware of local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express, IBM zHyperLink Express (zHyperLink), and RoCE Express2 channels.

Attention: A diagnostic test cannot be stopped once it has started.

When testing is complete, a message displays to indicate whether the test completed with errors or without errors. In either case, the tested port is displayed to show the results of the testing.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express, zHyperLink, or RoCE Express2 channel.

LAN port type
Identifies the type of network the selected OSA-Express, zHyperLink, or RoCE Express2 channel can be connected to through cable connections to its port or ports.

Physical Port Identifier
Identify the physical port of the selected OSA-Express, zHyperLink, or RoCE Express2 channel.

Diagnostic type

Select the type of test you want to perform:

Normal
Test port hardware that supports the internal operation of the specified port.

- The port must be disabled.
- All PCHIDs must be configured off.

Wrap plug test
Test port hardware that supports the external connection of the specified port to a local area network (LAN).

- The port must be disabled.
- A wrap plug must be installed on the port. Identify the part number of the correct wrap plug for each type of OSA-Express, zHyperLink, and RoCE Express2 port.
- All FIDs must be configured off.

Optical Power Measurement
Test port hardware that supports fiber optics of the specified port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Run port diagnostics

Use this window to view the sense data set during diagnostic testing of an Open Systems Adapter (OSA)-Express port.

The sense data indicates the results of running diagnostics.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Sense data

LAN port status word 0 displays the hexadecimal values of sense data bytes 0, 1, 2, and 3.

LAN port status word 1 displays the hexadecimal value of sense data bytes 4, 5, 6, and 7.

LAN port status word 2 displays the hexadecimal values of sense data bytes 8, 9, 10, and 11.

LAN port status word 3 displays the hexadecimal values of sense data bytes 12, 13, 14, and 15.

LAN port status word 4 displays the hexadecimal values of sense data bytes 16, 17, 18, and 19.

LAN port status word 5 displays the hexadecimal values of sense data bytes 20, 21, 22, and 23.

LAN port status word 6 displays the hexadecimal values of sense data bytes 24, 25, 26, and 27.

LAN port status word 7 displays the hexadecimal values of sense data bytes 28, 29, 30, and 31.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission mode of local area network (LAN) ports.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical port identifier
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode

Select the transmission mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Full duplex
Enable sending and receiving data transmissions at the same time.

Half duplex
Enable sending and receiving data transmissions, but not at the same time.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission speed and mode of local area network (LAN) ports.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical port identifier
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode/speed

Select the transmission speed and mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Auto Negotiate
Set the port at the current network speed.

Mode/Speed
Set the transmission speed and mode you want for the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission speed and mode of local area network (LAN) ports.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode/speed

Select the transmission speed and mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Auto Sense
Set the port at the current network speed.

Speed/Mode
Set the transmission speed and mode you want for the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Display client connections

Use this window to display Network Interface Card information for the selected Open Systems Adapter (OSA)-Express channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client connections table

Session Index
Displays the session numbers for the selected OSA-Express channel. A valid range for the session numbers is 0 to 120.

Status
Displays one of the following client session connections for the selected OSA-Express channel:

- **Ready** - Indicates the session has been configured and the client can be connected.
- **Active** - Indicates the session has been configured and the client is connected.
- **Not configured** - Indicates the session has not yet been configured.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Connected** - Indicates the session has been configured and the client is connected to it.
- **DHD Pending** - Indicates the client has been disconnected. However, since DHD was enabled, OSA-ICC has not notified the host operating system.

MAC
Displays the media address control (MAC) address of the client that is being connected. A MAC address identifies a port as a destination and source of information it receives and transmits, respectively, on the local area network (LAN).

Client IP
Indicates the client's IP address.

Port
Indicates the number that identifies the port for the client connection.

Socket Number
Displays the TCP socket number that uniquely defines the connection.

LT Index
Displays the index in the LT table. A valid range for the LT index is 0 to 119.

Connect Rule
Indicates one of the following connect rules:

- IP only
- LU only
- IP and LU
- Unknown

Disable Logo
Displays the OSA-ICC logo that appears when the session is first connected.

Additional functions on this window include:

OK
To close the current window, click **OK**.

Help
To display help for the current window, click **Help**.

Panel configuration options

Use this window to determine if you can select a configuration option for the selected Open Systems Adapter (OSA)-Express channel to validate the session configuration or view the validate error.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Configuration file options

Edit OAT entries
To open a window to configure OSA Address Table (OAT) entries for the selected OSA defined OSE channel type.

Edit SNA timers
To open a window to configure SNA timer values for the selected OSA defined OSE channel type.

Validate panel values
To open a window to validate panel values for a session configuration for the selected Open Systems Adapter (OSA)-Express channel.

Display validate panel errors
To open a window to display validate panel errors, if any exist.

Note: After the values have been validated, select the Activate configuration option on the Advanced Facilities window to active them or your current changes are lost.

Additional functions on this window include:

OK
To apply the selected options, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit SNA timers

Use this window select or enter SNA timer values to configure the OSA for the selected OSE defined channel type.

Port Number
Indicate the port number the SNA timers are associated with the selected OSE defined channel type.

Inactivity Timer/Ti (ms)
Use the drop down box to select or type the inactivity timer to be initialized for the selected OSE defined channel type. If the Ti timer is enabled, you can set its timeout value in increments of 0.12 seconds from 0.24 to 90.00 second. An enabled inactivity timer (ti) periodically tests the viability of the network media. The timer setting applies to all the clients on the target LAN, not to individual clients. The timer interval indicates how quickly a failure of the network media can be detected when the connection is quiescent.

Response timer/T1 (ms)
Use the drop down box to select or type the response timer for the selected OSE defined channel type. The T1 timer clocks link events that require responses from clients on the network. T1 can be set to a timeout value from 0.20 up to 51.00 seconds in increments of 0.20 seconds. Set the T1 timer to a value not less than the average round-trip transit time from the OSA to the clients and back.

Acknowledgment timer/T2 (ms)
Use the drop down box to select or type the acknowledgment timer for the selected OSE defined channel type. An OSA starts the T2 timer when it receives an I-format LPDU and stops when it sends an acknowledgment. An acknowledgment is sent either when an outgoing I frame is sent or when N3 number of I-format link protocol data units (LPDUs) has been received. Set a value from 0.08 seconds up to 20.40 seconds in increments of 0.08 seconds.

Maximum Frames Before Transmit Window/N3
Use the drop down box to select or type the maximum frames before transmit window for the selected OSE defined channel type. When determining the maximum I-frames that can be sent before an acknowledgment is sent (N3 count) and the maximum number of outstanding I-format link protocol data units (LPDUs) (TW count), consider the N3 and TW counts that are set at the clients as well.

Maximum Transmit Window/TW
Use the drop down box to select or type the maximum transmit window for the selected OSE defined channel type. The TW count allows the sender to transmit before that sender is forced to halt and wait for an acknowledgment. The TW count can be set as an integer from 1-16.

Additional functions on this window include:

OK
To save the new values, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit/display sessions configuration

Use this window to display or allow you to select a configuration edit session for the selected Open Systems Adapter (OSA)-Express channel. The window displays information that can be configured for the selected OSA-Express channel edit session configuration.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Edit/display sessions configuration table

Session index
Displays the session index number for the selected OSA-Express channel.

State
Displays one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS
Displays the channel subsystem (CSS). A valid range for the CSS is 0 to 3.

MIFID
Displays the logical partition ID. A valid range for the Image ID is 1 to F.

Device Number
Displays a unique number that is assigned for each device that was defined in the IOCDS.

LU Name (3270 OSC OSA channels only)
Indicates what active session you are connecting to. The LU name defines a group pool of devices.

Client IP
Indicate the IP address that a client will use to connect to the session. The client IP address can remain 0.0.0.0 or empty in order to allow any client to connect to a specific session. If a nonzero IP is specified, any client with a nonmatching IP will be rejected.

IP Filter
Displays the IP Filter address that is used for routing to specific subnets.

Session Type (3270 OSC OSA channels only)
Displays one of the following active session types for the selected OSA-Express channel:

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect (DHD) (3270 OSC OSA channels only)
Displays the defer host disconnect (DHD) time for the active session configuration to wait until the session instructs the host it has disconnected. The defer host disconnect can be:

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Response mode (RSP) (3270 OSC OSA channels only)
Displays the response mode (RSP) for the active session configuration. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgment.

Read Timeout (RTO) (3270 OSC OSA channels only)
Displays the read timeout (RT0) for the active session configuration to wait (in seconds) for a response from the client before performing a client disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Additional functions on this window include:

OK
To close the window when you finish reviewing the sessions, click **OK.**

Save
To save edit session data, click **Save**.

Change
To change edit session data, select a line and click **Change**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window.

Edit sessions configuration

Use this window to select a configuration session for the selected Open Systems Adapter (OSA)-Express channel. The window displays information that can be configured for the selected OSA-Express channel session configuration.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Edit sessions configuration table

Session Index
Display the session index number for the selected OSA-Express channel.

State
Display one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS Value
Display the channel subsystem (CSS). A valid range for the CSS is 0 to 3.

MIFID
Display the logical partition ID. A valid range for the Image ID is 1 to F.

Device Number
Display a unique number that is assigned for each device that was defined in the IOCDS.

LU Name
Indicate what active session you are connecting to. The LU name defines a group pool of devices.

Client's IP
Indicate the IP address that a client will use to connect to the session. The client's IP address can remain 0.0.0.0 or empty in order to allow any client to connect to a specific session. If a nonzero IP is specified, any client with a nonmatching IP will be rejected.

IP Filter
Display the IP Filter address that is used for routing to specific subnets.

Session Type
Display one of the following active session types for the selected OSA-Express channel:

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect (DHD)
Display the defer host disconnect (DHD) time for the active session configuration to wait until the session instructs the host it has disconnected. The defer host disconnect can be:

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Response mode (RSP)
Display the response mode (RSP) for the active session configuration. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgment.

Read Timeout (RTO)
Display the read timeout (RT0) for the active session configuration to wait (in seconds) for a response from the client before performing a client disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Additional functions on this window include:

Save
To save session data, click **Save**.

Change
To change session data, select a line and click **Change**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit session configuration

Use this window to change a configuration session for the selected Open Systems Adapter (OSA)-Express channel.

Channel ID
Display a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identify the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Session Index
Display the session number for the selected OSA-Express channel.

Session State
Display one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Active** - Indicates the session has been configured and the client is connected.
- **Connected** - Indicates the session has been configured and the client is connected to it.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS Value
Use the drop down box to select or type the channel subsystem (CSS) value for the session configuration of the selected Open System Adapter (OSA)-Express channel. A valid range for the CSS is 0 to 3.

MIFID
Use the drop down box to select or type the logical partition ID for the session configuration of the selected Open Systems Adapter (OSA)-Express channel.

Device Number
Use the drop down box to select or type the unique number for each device for the session configuration of the selected Open System Adapter (OSA)-Express channel.

LU Name
Enter the session you are connecting to for the selected Open Systems Adapter (OSA)-Express channel. The LU name defines a group pool of devices.

Client's IP address
Enter the client's IP address for the selected OSC channel. This entry field is optional.

IP Filter
Enter the IP filter address that is used for routing to specific subnets.

Session Type
Select one of the following choices to indicate the session type for the selected Open Systems Adapter (OSA)-Express channel.

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect
Select a one of the following to indicate the type of defer host disconnect (DHD) you want the session configuration to wait before instructing the host to disconnect.

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Defer host disconnect time value (seconds)
Enter your own defer host disconnect (DHD) time value in seconds that you want to specify for the session to wait before instructing the host to disconnect.

Response mode
Select a response (RSP) mode choice for the host to wait for the client to respond to the last packet of data. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgement.

Read Timeout
Select a choice to indicate the read timeout (RTO) for a response (in seconds) from the client before instruction the host to perform a disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Read timeout value
Enter your own read timeout (RTO) response (in seconds) value you want to specify for the session to wait before instructing the host to disconnect.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Delete Session
To delete the currently selected sessions configuration, click **Delete Session**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Display/Edit server configuration

Use this window to enter server configuration information for selected channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port 0/1

You can edit the server configuration information for the selected channel. To define a physical port, valid parameter values must be entered as displayed on the ranges adjacent to the parameter field. If a physical port is not defined, the IP address, Gateway, and TCP Port must all be set to 0 and the Prefix must be set to 1.

Note: By default all physical port parameters are set to 0. If the default value of 0 is not present in the IP address, Gateway, and TCP Port and 1 is not present in the in the Prefix physical port fields, that physical port is considered defined.

Server name
Enter the server name that the client is connected to for the selected Open Systems Adapter (OSA)-Express channel.

Enable IPv4
Check this box to enable IPv4

Host IPv4 address
Enter the host IP4v address for the active server configuration

Prefix
Enter the prefix of the IPv4 address for the active server configuration

IPv4 TCP port
Enter the IPv4 TCP port identifier for the active server configuration

IPv4 secure TCP port
Enter the IPv4 secure TCP port identifier for the active server configuration

Enable IPv6
Check this box to enable IPv6

Address type
Use this pull down to select the address for this IPv6 address

Host IPv6 address
Enter the host IPv6 address for the active server configuration

Prefix
Enter the prefix of the IPV6 address

IPv6 TCP port
Enter the IPv6 TCP port identifier for the active server configuration

IPv6 secure TCP port
Enter the IPv6 secure TCP port identifier for the active server configuration.

MTU size
Enter the maximum transfer (MTU) size to be transferred in one frame. A valid range is from 256 to 1492.

TLS version
Use this pull down to select the TLS version

- Select TLS 1.0 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.0, TLS 1.1, and TLS 1.2
- Select TLS 1.1 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.1 and TLS 1.2
- Select TLS 1.2 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.2 .

IPv4 default Gateway
Enter the IPv4 default gateway. The IPv4 default gateway is the network that connects the hosts

IPv6 default Gateway
Enter the IPv6 default gateway. The IPv6 default gateway is the network that connects the hosts.

Additional functions on this window include:

OK
To apply the changes displayed in the fields, click **OK**.

Close
To close the window without saving the current selected changes, click **Close**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Display/Edit server configuration

Use this window to enter server configuration information for selected channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port 0/1

You can edit the server configuration information for the selected channel. To define a physical port, valid parameter values must be entered as displayed on the ranges adjacent to the parameter field. If a physical port is not defined, the IP address, Gateway, and TCP Port must all be set to 0.

Note: By default all physical port parameters are set to 0. If the default value of 0 is not present in the IP address, Gateway, Subnet Mask, and TCP Port physical port fields, that physical port is considered defined.

Server name
Enter the server name that the client is connected to for the selected Open Systems Adapter (OSA)-Express channel.

Host IP address
Enter the host IP address for the active server configuration.

TCP port
Enter the TCP port identifier for the active server configuration.

Secure TCP port
Enter the secure TCP port identifier for the active server configuration.

Subnet Mask
Enter the subnet mask. The subnet mask identifies the TCP/IP protocol that is used for routing to specific subnets.

Default Gateway
Enter the default gateway. The default gateway is the network that connects the hosts.

MTU Size(B)
Enter the maximum transfer unit (MTU) size to be transferred in one frame. A valid range is from 256 to 1492.

Frame types

Select a choice to indicate the Ethernet standards that you want the network to follow. Every host in a network must have the same frame type.

DIX
Select the DIX frame type for the session configuration. It is **strongly recommended** that you use DIX as your frame type.

SNAP
Select the SNAP frame type for the session configuration.

Note: The recommended frame type for OSA-ICC is DIX. Changing the frame type to another mode without checking with your Network Administrator could cause a loss of data.

Additional functions on this window include:

OK
To apply the changes displayed in the fields, click **OK**.

Close
To close the window without saving the current selected changes, click **Close**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Manual configuration options

Use this window to select the manual configuration option for the session configuration of the selected Open Systems Adapter (OSA)-Express channel. You can export a session source file to a media source, then edit the file on your workstation with an editor. After you have completed editing your file, import the session source file back on the Support Element using the import source file choice.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Configuration file options

Import source file
Import a session configuration file that was exported to a diskette for editing.

Note: In order to make the imported edited source file the active configuration, you must *Validate source file* and then *Activate configuration*.

Insert the media source containing the source file into your disk drive, then highlight the file you would like to import and click **OK**.

Export source file
Export a session configuration file to a media source to edit with your workstation editor. You can also use this panel to export your configuration file as a backup.

Insert the media source containing the source file into your disk drive, then type the name to be given to the exported configuration file in the field and click **OK**.

Import source file by FTP
Import a session configuration file from a designated FTP site.

Export source file by FTP
Export a session configuration file to a designated FTP site.

Load default source file
To load the default source file.

Edit source file
Edit the session source configuration file.

Validate source file
Validate the session source configuration file to ensure that the file is valid before activating it.
Attention: In order to make the validated source file the active configuration, you must activate it. Activating a configuration makes any changes you made effective immediately. This could result in active sessions being dropped.

If the source file you are validating is incorrect, the errors and warnings will be commented in the source file. You must fix any errors before activating your configuration. When the validate is successful, you will receive a message stating that your source file is successful, then click **OK**.

Note: After the source file has been validated, select the Activate configuration option on the Advanced Facilities window to active them or your current changes are lost.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Import Source File

Select **Import Source File** to copy a configuration source file from one medium to the Support Element.

The import function copies a source file from the FTP destination to the Support Element hard disk.

Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import data configuration files from a FTP destination, click **Import**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Source File

Select **Export Source File** to export a configuration source file from the Support Element hard disk to an FTP destination.

The export function copies a source file from the Support Element to an FTP destination.

Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the file path and the file name of the data file that is to be saved.

Additional functions on this window include:

Export
To export configuration data files to an FTP destination, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Debug utilities

Use this window to select a debug option for the selected Open Systems Adapter (OSA)-Express channel. This window identifies the channel ID and LAN port type of the selected OSA-Express channel.

Ping utility
Select the ping utility to ping an active session to verify the status of the connection.

Trace route utility
Select the trace route utility to trace the route of a packet of data to a session.

Drop session
Select drop session to enter the session number to drop for the ping utility to identify.

Logo controls
Select the logo controls to enter the operating system session number to enable or disable a three line logo screen.

Query command
Select the query command to enter a command to the OSC channel for information.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Ping utility

Use this to open a window to ping an active session to verify the status of the connection.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client IP address
Indicate the client's IP address.

Length (in bytes)

Use this entry field to indicate the ping custom length of 8 to 32000 bytes.

Default (256)
Use the length default value. The default length value is 256 bytes.

Custom length
Set your own custom length of 8 to 32000 bytes.

Count

Use this entry field to indicate a custom count for the ping between 1 and 10.

Default (1)
Use the count default value. The default count value is 1.

Custom count
Set a custom count for the ping between 1 and 10.

Timeout (in seconds)

Use this entry field to indicate you own ping custom timeout value.

Default (1)
Use the timeout default value. The default timeout value is 10.

Custom timeout
Set your own custom timeout value between 1 and 30.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Trace route utility

Opens a window to trace the route of a packet of data to a session.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client IP address
Indicate the client's IP address.

MAX TTL

Use to select the trace route maximum time to live (TTL) for the packet that is being sent.

Default(30)
Use the MAX TTL default value. The default MAX TTL value is 30.

Custom MAX TTL
Set a custom MAX TTL.

Attempts

Use to select the attempts value for the trace route.

Default(3)
Use the attempts default value. The default attempts value is 3.

Custom attempts
Set a custom attempts value of between 1 and 20.

Port

Use to select the trace route port value you want set for the trace route.

Default(4096)
Use the port default value. The default port value is 4096.

Custom port
Set a custom port identifier between 2048 and 60000.

Wait time in seconds

Default(5)
Use the wait time default value. The default wait time value is 5 seconds.

Custom wait time
Set a custom wait time value of between 1 and 255.

Extra debug messages

No
Do not display extra debug messages.

Yes
Display the extra debug messages.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Drop session

Use the entry field to identify what session index number to drop.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Session index
Identify what session index number to drop.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To stop the command currently being processed by the selected channel, click **Cancel.**

Help
To display help for the current window, click **Help**.

Logo controls

Use this window to enter the operating system session index for the selected OSA-Express channel when enabling or disabling a three line logo screen for the operating system screen.

Enable Logo
Clear the operating system screen and display a three line logo screen for the operating system session index entered.

Disable Logo
Do not display a three line logo screen for the operating system session index entered.

Additional functions on this window include:

OK
To close the window after making changes, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Query command

Use this window to enter a query command to request information from the channel. The query command can be up to 50 alpha-numeric ASCII characters.

Note: This command should be used only under the guidance of service support.

Additional functions on this window include:

OK
To continue with the query command operation, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Manage security certificate

Use this window to manage Secure Socket Layer (SSL) certificates. Select an action and location to manage the security certificates.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

OSA-ICC certificate scope
Displays the current OSA-ICC certificate scope that is used for this physical channel identifier (PCHID). Click **Change** to select a different certificate scope action for the selected PCHID.

OSA-ICC certificate type
Displays the OSA-ICC certificate type of this physical channel identifier (PCHID)

OSA-ICC certificate expiration
Displays the OSA-ICC certificate expiration of this physical channel identifier (PCHID).

Actions

- Select **Export self-signed certificate** to generate a self-signed certificate and store in the configuration file to export via USB drive or FTP site
- Select **Reload self-signed certificate** to install the self-signed certificate
- Select **Regenerate OSA-ICC key and self-signed certificate** to regenerate the self-signed certificate
- Select **Create certificate signing request** to generate a certificate signing request and store in the configuration file to export via USB drive or FTP site
- Select **Import signed certificate** to import and install a file via USB drive or FTP site
- Select **View certificate** to view the certificate that is currently being used
- Select **Edit certificate** to edit the certificate signing request (CSR) attributes.

Location

- Select **USB drive** to export or import the selected action
- Select **FTP site** to export or import the selected action.

Additional functions on this window include:

Apply
To save the new values, click **Apply**.

Change
To change the OSA-ICC certificate scope, click **Change**.

Close
To close the window without saving the current selected changes, click **Close.**

Help
To display help for the current window, click **Help**.

Edit Certificate

Use this window to provide the necessary information to create a new certificate or to modify the values of the existing certificate.

Common name
Specify the common name for the certificate

Organization
Optionally, specify the name of the corporation, limited partnership, university, or government agency

Organization unit
Optionally, specify the organization name, which differentiates between divisions within an organization (for example, Hardware Development or Human Resources)

Country or region
Optionally, select or specify the two-character ISO format country code for your country (for example, a two-character code of GB for Great Britain or US for the United States).

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the list.

State or province
Optionally, select or specify the state or province name.

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the list

Locality
Optionally, specify the city or locality name

Valid until
Specify the ending date that the certificate can be valid until, beginning from the time the certificate is created or modified

DNS name
Optionally, add DNS names to the list of valid entries for the certificate

IP Address
Optionally, add IPv4 and IPv6 addresses to the list. The IPv4 address must be specified as 4 decimal numbers separated by a period (for example, dd.ddd.ddd.ddd). The IPv6 address can be specified in several different ways with one form being 8 hexadecimal numbers separated by a colon (for example, xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Email address
Optionally, add email addresses to the list.

Additional functions on this window include:

Save
To save the new values, click **Save**.

Next
To proceed to the next window, click **Next**.

Cancel
To close the window without saving the new values, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Certificate Signing Request

Use this window to select an export method for the certificate signing request.

Export to FTP
To export to an FTP location, select **Export to FTP**

Export to USB
To export to a USB media, select **Export to USB**

Note: This option is not available remotely.

Export to file system
To export to a local file system, select **Export to file system**

Note: This option is only available remotely.

Additional functions on this window include:

Export
To continue with the selected export method, click **Export**.

Back
To go back to the previous window, click **Back**.

Help
To display help for the current window, click **Help**.

Change OSA-ICC Certificate Scope

Select the certificate scope action that will apply for the PCHID:

Use the shared certificate for this PCHID
Select **Use the shared certificate for this PCHID** to use the shared certificate for this physical channel identifier (PCHID)

Use an individual certificate for this PCHID
Select **Use an individual certificate for this PCHID** to use an individual certificate for this physical channel identifier (PCHID).

Additional functions on this window include:

OK
To save the new values, click **OK**.

Change Certificate Scope
To change the certificate scope, click **Change Certificate Scope**.

Cancel
To close the window without saving the current selected changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Import Source File

Select **Import Source File** to copy a configuration source file from one medium to the Support Element.

The import function copies a source file from the FTP destination to the Support Element hard disk.

Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import data configuration files to an FTP destination, click **Import**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Source File

Select **Export Source File** to export a configuration source file from the Support Element hard disk to an FTP destination.

The export function copies a source file from the Support Element to an FTP destination.

Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the file path and the file name of the data file that is to be saved.

Additional functions on this window include:

Export
To export configuration data files to an FTP destination, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Partition Details

Accessing the Partition Details task

Use the **Partition Details** task to view or modify an existing definition for a specific partition. You can access this task from the main HMC page by selecting a partition under a specific Dynamic Partition

Manager (DPM)-enabled system in the Systems Management node, or by selecting the task in the Tasks index.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

You must have the appropriate authorization to use the **Partition Details** task. You may use:

- One of the following default user IDs: SYSPROG, ADVANCED, OPERATOR, ACSADMIN, or SERVICE
- Or a user ID that a system administrator authorized to this task through customization controls in the **User Management** task.

The **Partition Details** task is also available on the Support Element (SE) in view-only mode.

To modify a partition definition:

1. On the HMC, select a DPM-enabled system in the Systems Management node.
2. On the Partitions tab, click the hyperlink in the Name column for a specific partition. The Partition Details window opens.
3. Review and, if necessary, modify values in the **General**, **Status**, **Controls**, **Processors**, **Memory**, **Network**, **Storage**, **Accelerators**, **Cryptos**, and **Boot** sections. To access each section, click the link in the navigation frame, or scroll and use the expand and collapse buttons in the section headings, as necessary.

   Note: To access the **Controls** section, you must be using the default SYSPROG or SERVICE user ID, or a user ID that is authorized to one of those two default roles. If you are not logged on with a user ID that has the required authority, the **Controls** section is not displayed.
4. When you have finished, click **OK** to save your changes. If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to save your changes. A progress indicator is displayed until DPM finishes the updating the partition.

When it has completed the operation, DPM opens the Validation window, which indicates whether the partition was successfully updated.

- If the save operation did not complete successfully, the Validation window displays an error message with details about the problem. In this case, click **Close** to return to the **Partition Details** task. Depending on the error, the task opens to either the main window or the first section, if any, that contains an error.
- If you have created one or more network interface cards (NICs) with associated VLAN IDs, the Validation window includes a list of each NIC device number and the associated VLAN ID to be used when configuring the device on the operating system that the partition hosts.

Partition Details

Use the **Partition Details** task to view or modify an existing definition for a specific partition on a Dynamic Partition Manager (DPM)-enabled system.

The **Partition Details** task opens in view-only mode under the following circumstances:

- When you access the task from the Support Element (SE), rather than the Hardware Management Console (HMC).
- When the current status of the DPM-enabled system is one of the following: No power, Not operating, Service, Status check, or Communications not active.

The **Partition Details** task is organized into the following sections, each of which are listed in the navigation pane. To access each section, click the appropriate link in the navigation pane, or scroll the main page and expand or collapse each section as necessary.

- “General” on page 1209
- “Status” on page 1211
- “Controls” on page 1212

- "Processors" on page 1213
- "Memory" on page 1216
- "Network" on page 1218
- "Storage" on page 1224
- "Accelerators" on page 1233 (This section is displayed only when a system that supports accelerators is managed through this HMC, and is enabled only for systems that support accelerators.)
- "Cryptos" on page 1236
- "Boot" on page 1243

The navigation pane also includes the following links to related tasks.

Start or Stop
Depending on the current status of the selected partition, only one of the following task links is displayed.

Start
Opens the **Start** task, with this partition selected as the partition to start.

Stop
Opens the **Stop** task, with this partition selected as the partition to stop.

System Details
Opens the **System Details** task for the DPM-enabled system.

Manage Adapters
Opens the **Manage Adapters** task for the DPM-enabled system.

Monitor System
Switches the foreground window to the **Monitor** tab for the selected DPM system node.

You can find more detailed help on the following elements of this window:

OK
To close the window, click **OK**. This action applies your changes and closes the Partition Details window.

- If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to save your changes or **Cancel** to close the window without saving any of your changes. If you click **Save**, a progress indicator is displayed until DPM finishes the updating the partition.
- If you made changes to a partition that is in Stopped state and click **OK**, a progress indicator is displayed until DPM finishes the updating the partition.

When it has completed the operation, DPM opens the Validation window, which indicates whether the partition was successfully updated. If not, the Validation window displays an error message with details about the problem. In this case, click **Close** to return to the **Partition Details** task. Depending on the error, the task opens to either the main window or the first section that contains an error.

Apply
To apply changes you made in editable fields on the page, click **Apply**. This action applies your changes without closing the Partition Details window.

- If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to apply the changes or **Cancel** to return to the previous window. If you click **Save**, a progress indicator is displayed until DPM finishes the updating the partition.
- If you made changes to a partition that is in Stopped state, a progress indicator is displayed until DPM finishes the updating the partition.

When it has completed the operation, DPM opens the Validation window, which indicates whether the partition was successfully updated. If not, the Validation window displays an error message with details about the problem. In this case, click **Close** to return to the **Partition Details** task. Depending on the error, the task opens to either the main window or the first section that contains an error.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

In view-only mode, only **Cancel** and **Help** are displayed.

General

Use the General section to view or modify the general details for this partition.

On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Specifies the name of the partition, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. A partition name must uniquely identify the partition from all other partitions defined on the same system.

Description
Specifies the user-supplied description, if any, of the partition. The description can be up to 1024 characters in length.

Object ID
Displays the DPM-generated identifier for this partition. This ID is also known as the universally unique identifier (UUID) of the partition.

Mode
Displays the operating mode of the hypervisor or operating system on the partition.

Short name
Specifies the short name of the partition, which is the name by which the operating system can identify the partition. The short name must consist of 1 - 8 alphanumeric uppercase characters, with the first character is alphabetic; the words PHYSICAL, REC, SYSTEM, and PRIMxxxx (where xxxx is a 4-digit decimal number) are reserved and cannot be used.

- If the short name that you provide has been specified for another partition, the name is valid only if you are not reserving resources for this partition. The best practice, however, is to supply a unique name that identifies the partition from all other partitions defined on the same system. An error or warning message is displayed if the short name is not unique.
- If you delete the value specified for this field, a unique short name is automatically generated when you save your changes.

Partition ID
Specifies the identifier (ID) for the partition. Select **Generate automatically** to allow the partition ID to be managed by the system; by default, this check box is selected. When **Generate automatically** is selected, the partition has a different ID each time it is started.

The partition ID must be a unique two-character hex number from 00 - 7F. If the partition ID that you provide has been specified for another partition, the ID is valid only if you are not reserving resources for this partition. Even in this case, however, the best practice is to supply a unique ID.

Partition type
Specifies one of the following values that identifies the type of partition. You cannot change the partition type.

Linux
In this type of partition, you can install and run a Linux on Z distribution as a single operating system, or as a hypervisor for multiple guests.

z/VM
In this type of partition, you can install and run z/VM as a hypervisor for multiple Linux guests.

Secure Service Container
This type of partition is a Secure Service Container, in which you can run only specific software appliances that the Secure Service Container supports.

When the selected partition type is **Secure Service Container**, the page display includes the following additional fields. These fields are read-only until you click **RESET LOGIN**.

Master User ID
Enter the user ID to be used as the default master user ID for the Secure Service Container partition. This user ID has authority to perform any task that is available through the Secure Service Container graphical user interface (GUI).

A master user ID can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

Master Password
Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis (), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

Confirm Master Password
Reenter the password exactly as you typed it for the Master Password field.

RESET LOGIN
Click **RESET LOGIN** to remove any previously supplied password and confirmation from the password text fields, so you can supply new values for **Master User ID**, **Master Password**, and **Confirm Master Password**. To save these new values, click **Apply**; to have the saved values take effect, you must stop and restart the partition. Otherwise, click **Cancel** to cancel the reset operation.

Reserve resources to ensure they are available when the partition is started
Specifies whether or not resources are reserved for this partition. Select this check box only if you want to reserve the configured resources for this partition, which include processors, memory, network interface cards, host bus adapters, virtual functions, and crypto domains.

- When this check box is not selected, other partitions on the system can use these resources when this partition is stopped. In this case, this partition might be unable to start if the required resources are not available.
- When this check box is selected, these resources cannot be used by any other partition on the system, even when this partition is stopped. This selection guarantees that the partition can be started at any point in time.

OS name
Displays the user-defined name of the hypervisor or operating system for this partition. The value for this field is displayed only when DPM has detected the hypervisor or operating system.

OS type and level
Displays the type and release level of the hypervisor or operating system that is running on this partition; for example: Linux 3.11.0. The value for this field is displayed only when DPM has detected the hypervisor or operating system.

Secure Execution
Indicates whether the operating system that runs on the partition is configured for secure execution, which isolates and protects any guests that run on a hypervisor by restricting host access to guest workloads and data.

On
This field value is displayed only when the operating system is configured for secure execution and is running, and the partition is active.

Off
This field value is displayed when one of the following conditions is true.

- The IBM Secure Execution for Linux feature is not enabled on the host system for this partition. In this case, the field value does not change to On, even if the operating system is configured for secure execution.
- The operating system is not configured for secure execution.
- The operating system is configured for secure execution but the partition is not active.

Status

Use the Status section to view the current status of the partition and, if necessary, to modify the acceptable availability status values for the partition, based on the importance of its workload. For example, if this partition supports a critical workload on a production server, you might select only Active as an acceptable status value. In contrast, for a partition that supports low-priority software testing, you might select additional values as acceptable. When a partition is started and enters a state that is not selected as an acceptable status, the partition is highlighted in red in various HMC task displays.

In this section, the Status field displays the current status of the partition. The current status value is preceded by an icon that indicates whether this current status value is defined as an acceptable status value. If the current status value is Degraded, the display includes a message indicating the reason why the status is Degraded, and lists the name of each resource that is causing the partition to be in the Degraded state. Each list item is a hyperlink through which you can open the details window for the resource. When one or more storage adapters are degraded, the list includes affected storage groups or tape links, along with a hyperlink to the appropriate storage group or tape link details page.

Under the "Acceptable statuses" label, you can select one or more status values as an acceptable status for the partition. When you have finished, review another section or click **OK** to save the partition definition.

By default, only Active is selected. Additional status values include the following:

Active
Indicates that the partition has successfully started and is operating normally.

Communications not active
Indicates a problem with the communication between the Hardware Management Console (HMC) and the Support Element (SE).

Degraded
Indicates that the partition successfully started and is operating, but the availability of physical resources to which it has access is less than required, as stated in the partition definition. This status might be acceptable, for example, for partitions that do not have reserved resources.

Paused
Indicates that, because a user has stopped all processors, the partition is not running its workload. In this case, because the partition was successfully started, its resources are shown as active and are still associated with this partition.

Reservation error
Indicates that the availability of physical resources does not match the reserved resources that are stated in the definition for this partition. The partition cannot start until sufficient resources are available.

Starting
Indicates the transitional phase between Stopped state and Active state, as the result of a Start task issued against this partition.

Status check
Indicates that the current status of the partition is unknown. This condition usually occurs under one of the following circumstances:

- When the SE is starting up; in this case, this partition status is temporary.
- When the SE and the DPM-enabled system to which it is attached cannot communicate.

Stopped
Indicates that the partition has normally ended its operation, and exists only as a partition definition.

Stopping
Indicates the transitional phase between Active state and Stopped state, as the result of a Stop task issued against this partition.

Terminated
Indicates that all of the processors for this partition are in a disabled wait state, or a system check stop occurred. The partition is not running its workload. In this case, because the partition was successfully started, its resources are shown as active and are still associated with this partition.

Controls

Use the Controls section to enable or disable partition access to various controls. By default, all settings are unchecked.

Note: To access the **Controls** section, you must be using the default SYSPROG or SERVICE user ID, or a user ID that is authorized to one of those two default roles. If you are not logged on with a user ID that has the required authority, the **Controls** section is not displayed.

Partition Access Controls
You can select one or more of the following security-related controls.

Access global performance data
Select this option:

- To allow the partition to view the CPU utilization data and the Input/Output Processor (IOP) data for all partitions in the configuration. If you do not select this option, the partition is only able to view its own CPU utilization data.
- To enable the collection of FICON channel measurements.

Permit cross-partition commands
Select this option to allow the partition to issue control program commands that affect other partitions; for example, perform a system reset of another partition, deactivate a partition, or provide support for the automatic reconfiguration facility.

CPU-Measurement Counter Facility Authorization Controls
The CPU-measurement counter facility provides a means to measure activities in the CPU and some shared peripheral processors. Select these options only when you want to collect measurement data for performance statistics.

Access basic counter set
Select this option to authorize the use of the basic counter set. This set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches.

Access problem state counter set
Select this option to authorize the use of the problem state counter set. This set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches only when the processor is in problem state.

Access crypto activity counter set
Select this option to authorize the use of the crypto activity counter set. This set includes counters for a central processing unit that are related to the following function counts.

- Pseudo Random Number Generation (PRNG)
- Secure Hash Algorithm (SHA)
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

Access extended counter set
Select this option to authorize the use of the extended counter set. The extended counters provide information about hardware facilities and structures that are specific to a machine family. The extended counters are designed to expand upon information provided by the basic counter set.

CPU-Measurement Sampling Facility Authorization Controls
CPU-measurement sampling facility provides a means to take a snapshot of the CPU at a specified sampling interval. Select this option only when you want to collect measurement data for performance statistics.

Access basic sampling
Select this option to authorize the use of the basic sampling function. Samples are taken and stored at the end of each sampling interval. If you select this option, the Controls display changes to enable you to select an additional option: **Access diagnostic sampling**, which authorizes the use of the diagnostic sampling function.

Processors

Partitions on a DPM system can have only one defined processor type: either Central Processor (CP) or Integrated Facility for Linux (IFL), depending on the processor types that are installed on the system. Use the Processors section to view or modify the type, mode and number of virtual processors for the partition, and to view various charts that are based on your selections. The processor charts displayed are based on the processor mode that you select. The virtual processors are allocated from physical processors of the selected type.

The following list provides a description of each element in the Processors section. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Processor type
If this field is displayed in the Processors section, the value indicates the currently selected processor type, which is either the **Central Processor (CP)** or **Integrated Facility for Linux (IFL)** processor type. If only one type of processor is installed on the system, this field is not displayed. If the partition is currently active, you cannot modify the selected type. Note that simultaneous multithreading is supported only for the IFL processor type.

Processor mode
Indicates the currently selected processor mode. If the partition is currently active, you cannot modify the selected mode.

Shared
Select this option when you want the new partition to share processor resources from the pool of physical processors that are not dedicated to other partitions.

Dedicated
Select this option when you want the new partition to have exclusive use of a specific number of physical processors installed on the system..

Processors
Indicates the currently defined number of shared or dedicated processors for the partition. You can use one of the following controls to modify the value.

Slider
The minimum value is 1 and the maximum value is the number of entitled processors on the system. The slider not only shows the total range of values that you can select, but also uses color to indicate the current state of processor resources on the system. The slider ranges and colors vary, depending on whether the partition is currently stopped or active.

When the partition is stopped
The slider displays two ranges: one range on the left, highlighted in green, and the other range on the right, highlighted in yellow or red.

- Green indicates the range of available processor resources. If you select a value in this range, you can successfully start the partition.

- Yellow or red indicate the range of processor values that prevent the new partition from starting, or prevent the partition from receiving its required amount of processor resources. This range has a different significance, depending on the selected processor mode and whether you have selected the **Reserve resources** check box in the General section.

  For shared processor mode
  When the processor mode is shared, this range is the number of dedicated processors that are assigned to active and reserved partitions. If you select a number in this range, you receive an inline warning or error message indicating that the processor value you selected is greater than the number of shared physical processors.

  – If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition cannot be started unless the number of shared physical processors on the system is increased.

  – If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its processor resources cannot be reserved unless the number of shared physical processors on the system is increased.

  For dedicated processor mode
  When the processor mode is dedicated, this range is the sum of the number of dedicated processors assigned to active and reserved partitions, plus the minimum number of shared physical processors required (that is, the largest number of shared processors that is assigned to a single active or reserved partition). If you select a number in this range, the inline warning or error message indicates that the processor value you selected is greater than the number of available physical processors.

  – If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition cannot be started unless the number of dedicated physical processors on the system is increased.

  – If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its processor resources cannot be reserved unless the number of dedicated physical processors on the system is increased.

When the partition is active
The slider displays three ranges: one range starting on the left, highlighted in red; another range in the middle, highlighted in green; and the final range on the right, highlighted in red.

- Green indicates the range of available processor resources that you can successfully select.
- Red indicates processor resources that are not available for use. If you try to select a number in one of the ranges highlighted in red, an error message is displayed.

  – The first range, on the left, indicates the number of processors that have been varied on by the hypervisor or operating system running on the partition. You cannot select fewer processors than the number that this partition is already using.

  – The other range, on the right, indicates the number of shared or dedicated processors that are assigned to active and reserved partitions. These processors are not available for use.

Text entry box and number spinner
Using the text box, enter a valid integer within the limits of the slider range. When you enter a value, the slider changes to reflect the value entered in the text box. Alternatively, use the number spinner to increment or decrement the value in the text entry box and slider. Each click increments or decrements the value by one, within the limits of the slider range.

Threads
Indicates the number of threads that are available for use when simultaneous multithreading (SMT) is enabled, and when the processor type for the partition is **Integrated Facility for Linux (IFL)**. DPM displays thread information only under the following circumstances:

- When an administrator has explicitly enabled SMT, or when SMT is enabled by default, for the operating system or hypervisor that runs on the partition.
- When DPM can retrieve SMT information from the operating system or hypervisor that runs on the partition. If the partition is stopped, for example, DPM cannot display thread information.

Processors bar chart

Indicates the number of shared and dedicated physical processors on the system. The bar chart scale ranges from 0 to the system design limit. To show the actual number of processors that each bar segment represents, hover your cursor over the colored segment. A dotted line indicates the total number of entitled processors on the system. Entitled processors are processors that are licensed for use on the system; the number of entitled processors might be less than the total number of physical processors that are installed on the system.

To the right of the bar chart, a color legend identifies each segment of the bar chart:

- The number of shared or dedicated processors that you have currently specified for the new partition. This value varies when you change the Processors setting through the slider, text box, or number spinner.
- The number of shared processors, if any, that are available for use by partitions on the system.
- The number of dedicated physical processors that are assigned to active partitions and reserved partitions, if any exist. This number does not reflect any dedicated processors that are assigned to stopped or unreserved partitions.
- The total number of entitled processors on the system. If you have specified a number in the second range (yellow) for the new partition, the total number of processors for all partitions might exceed the number of entitled processors.

Shared Processors pie chart

Indicates the relative distribution of virtual processors for this new partition and all active partitions on the system that are using shared physical processors. This pie chart is displayed only when you have selected Shared as the processor mode.

To the right of the pie chart, a color legend identifies each of the partitions by name. To view details for a specific partition in the pie chart, hover your cursor over the pie wedge with the same color as shown in the legend, next to the partition name. The pie wedge is slightly enlarged and a tooltip displays details for the partition. The tooltip displays the partition name, the number of processors for that partition, and its relative percentage of the total shared partitions, rounded to two decimal places.

At most, the pie chart consists of 12 wedges, one of which is reserved for this new partition. If the system has more than 11 active partitions, the pie chart is divided as follows:

- One wedge for the new partition that you are defining. The wedge size and number of processors vary when you change the Processors setting through the slider, text box, or number spinner.
- One wedge for each of the 10 active partitions with the highest number of processors.
- One wedge that represents all remaining active partitions on the system and the total number of processors shared by this group. In the legend, this group wedge is labeled Others, with the total number of partitions in parentheses.

Processing weight

Select the relative amount of processor time that a specific active partition receives when it is in contention with other active partitions that share the same pool of processor resources. Processing weight options, and a link that opens the **Manage Processor Sharing** task, are displayed only when you have selected Shared as the processor mode.

The processing weight scale ranges from 1 to 999, with specific values labeled as Very Low (100), Low (300), Medium (500), High (700), and Very High (900). These labels are hyperlinks that you can select. Use either the vertical slider on the scale, the hyperlink labels, the text box, or the number spinner to select a value. If you use the number spinner, each click increments or decrements the value by one. The suggested practice is to specify a processing weight that satisfies the peak workload requirements of the partition.

Enforce weight capping
Select this option to enforce weight capping for the partition. When weight capping is enforced, the partition cannot use more processor time than its weight, relative to other partitions that share the same pool of processor resources, even when additional processor resources are available.

Enforce absolute processor capping
Select this option to enforce absolute processor capping for the partition. When absolute capping is enforced, this partition cannot use any more than a specific number of physical processors when it is active. When you select this option, you can enter the absolute capping value, which is the maximum number of physical processors that this partition can use. The absolute capping value ranges from 0.01 - 255.0, in increments of 0.01.

Active Processing Weights pie chart
Indicates the relative distribution of processor weights for this partition and all active partitions on the system. This pie chart is displayed only when you have selected Shared as the processor mode.

To the right of the pie chart, a color legend identifies each of the partitions by name. To view details for a specific partition in the pie chart, hover your cursor over the pie wedge with the same color as shown in the legend, next to the partition name. The pie wedge is slightly enlarged and a tooltip displays details for the partition. The tooltip displays the partition name, its weight value, and its relative percentage of the total processing weight, rounded to two decimal places.

Manage Processor Sharing
Launches the **Manage Processor Sharing** task, which provides the controls through which you can set weights, weight capping, and absolute capping for partitions with shared processors.

Memory

Each partition on a DPM-enabled system has exclusive use of a user-defined portion of the total amount of entitled memory that is installed on the system. Use the Memory page to view or modify the initial and maximum amounts of memory that are assigned to a specific partition.

When you define the amount of memory to be assigned, or allocated, to a specific partition, you specify an initial amount of memory, and a maximum amount that must be equal to or greater than the initial amount. The partition receives its initial amount when it is started. If the maximum amount of memory is greater than the initial amount, you can add memory up to this maximum to the active partition, without stopping and restarting it.

The following list provides a description of each element in the Memory section. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional. You can set the memory amounts in different units: megabytes (MB), gigabytes (GB), or terabytes (TB). The default unit is GB. To change the unit, hover your cursor over the unit in a field label, and select another unit from the popup display. When you change the unit for one field, the same unit change is replicated to the other display elements on the page.

Memory
Specifies the amount of memory that is currently assigned to the partition. This value represents the initial amount of memory that the partition receives when it is started. If you set this initial amount to a value greater than the value currently displayed for the Maximum Memory field, the maximum memory is automatically set to the same value. When the partition is not active, you can use one of the following controls to modify the value. If you are modifying the value for a Secure Service Container partition, you must specify an initial amount of at least 4096 MB (4 GB).

Slider
The minimum value that is displayed depends on the unit that you have selected (MB, GB, or TB); for example, the minimum value for the default unit (GB) is 0.5. The maximum value is the amount of entitled memory on the system; this maximum varies by system. The slider not only shows the total range of values that you can select, but also uses color to indicate the current state of memory resources on the system. The slider ranges and colors vary, depending on whether the partition is currently stopped or active.

When the partition is stopped

The slider displays two ranges: one range on the left, highlighted in green, and the other range on the right, highlighted in yellow or red.

- Green indicates the range of available memory values that you can select and successfully assign to the partition.
- Yellow or red indicate the range of memory values that might prevent the partition from starting, or prevent the partition from receiving its required amount of memory resources. This range is the amount of memory that is assigned to active and reserved partitions; it has a different significance, depending on whether you have selected the **Reserve resources** check box in the General section.
  - If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition might fail to start until the amount of available memory on the system is increased.
  - If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its memory resources cannot be reserved unless the amount of available memory on the system is increased.

When the partition is active

The slider displays three ranges: one range starting on the left, highlighted in red; another range in the middle, highlighted in green; and the final range on the right, highlighted in red.

- Green indicates the range of available memory that you can successfully select.
- Red indicates memory resources that are not available for use. If you try to select a number in one of the ranges highlighted in red, an error message is displayed.
  - The first range, on the left, indicates the amount of memory that is allocated by the hypervisor or operating system running on the partition. You cannot select less memory than the amount that this partition is already using.
  - The other range, on the right, indicates the amount of memory that is assigned to active and reserved partitions.

Text entry box and number spinner

Using the text box, enter a valid integer within the limits of the slider range. When you enter a value, the slider changes to reflect the value entered in the text box. Alternatively, use the number spinner to increment or decrement the value in the text entry box and slider. Each click increments or decrements the value by 0.5, within the limits of the slider range.

Maximum Memory

Specifies the amount of maximum memory assigned to the partition. When the partition is not active, you can change the current value; the new value that you specify must be equal to or greater than the value specified in the Memory field.

The controls (slider, text box and number spinner) are the same as those for the Memory field; however, these controls are disabled when the partition is active. The slider ranges and colors also have the same significance as those for the Memory field.

Installed Memory bar chart

Indicates the distribution and amounts of system memory, including the memory assigned to this partition. The bar chart scale ranges from 0 to the total amount of memory that is installed on the system. To show the actual amount of memory that each bar segment represents, hover your cursor over the colored segment.

To the right of the bar chart, a color legend identifies each segment of the bar chart:

- The amount of memory that you have currently specified for this partition. This value varies when you change the Memory setting through the slider, text box, or number spinner.

- The maximum amount of memory that you have currently specified for this partition. This value is represented as a dotted line in the bar chart, and its position moves when you change the Maximum Memory setting through the slider, text box, or number spinner.
- The total amount of allocated memory, which is the total memory assigned to all active and reserved partitions on this system.
- The amount of entitled memory for this system. Entitled memory is the amount of memory that is licensed for use, which might be less than the total amount of memory that is installed on the system. This value is represented as a dotted line in the bar chart.

Network

Network interface cards (NICs) provide a partition with access to internal or external networks that are part of or connected to a system. Each NIC represents a unique connection between the partition and a specific network adapter that is defined or installed on the system.

Use the Network section to view, to modify, or to create NICs that enable the partition to access the networks connected to the DPM-enabled system. When you create a NIC, you can select the adapter that you want to use from a list of all of the network adapters that are currently configured on the system.

- For availability, select at least two network adapters of the same type, and create a NIC for each one.
- For a Secure Service Container partition, you must specify at least one NIC for communication with the Secure Service Container web interface.

The following topics describe the NICs table actions and elements, and the elements in the "Secure Service Container Web Interface Communication" section, which is displayed only for Secure Service Container partitions.

- “The NICs table toolbar” on page 1218
- “Columns in the NICs table” on page 1219
- “Standard table functions” on page 1220
- “Secure Service Container Web Interface Communication” on page 1221

The NICs table toolbar

The NICs table contains an entry for each network interface card, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Network Interface Card** window, through which you can create a new network interface card. For more information, see “New Network Interface Card” on page 1221.

Details
Opens the **NIC Details** window. This action is enabled when only one NIC is selected in the table. The **NIC Details** window fields and controls are the same as those for the **New Network Interface Card** window, with the following exceptions:

- The name, description (if any), device number, and adapter port or switch selection are displayed for the selected NIC.
- The Device number field is marked as a required field.
- If the NIC is the only NIC that provides access to the Secure Service Container web interface, the "Use to access the web interface" switch is set on and cannot be set off.
- The Adapter Ports and Switches table contains entries for only those configured ports and switches that have the same card type as the selected NIC, because you cannot change the type of network interface card.

If you plan to change either the VLAN ID or the MAC address of this NIC, note the following:

- If you change either the VLAN ID value or the MAC address after the partition is created and started, the NIC is deactivated and reactivated, which is disruptive to any network activity taking place over this device in the operating system or hypervisor.
- If you change VLAN ID value, make sure that you also use the new VLAN ID value in the network configuration files for the operating system or hypervisor.

Delete
Opens the **Delete NIC** confirmation window through which you can delete one or more NICs. This action is enabled when one or more NICs are selected in the table.

Note that, for a Secure Service Container partition, DPM does not process the delete operation if the end result is that all defined NICs are removed. For this type of partition, at least one NIC is required to access the Secure Service Container web interface.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected NICs. The confirmation window closes, and the resulting NICs table display does not contain any entries for the deleted NICs. The NICs are not actually deleted until you click **OK** or **Apply** on the main window of the **Partition Details** task.
- Click **Cancel** to close the confirmation window and return to the Network section, without deleting any NICs.

Adapter Details
Opens the **Adapter Details** task in a separate window. This action is enabled when one or more NICs are selected in the table.

Columns in the NICs table

The NICs table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a virtual network interface card (NIC). The name is a hyperlink through which you can open the **NIC Details** window. To edit the name, double-click in the table cell and type the new name.

If this NIC represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

IP Address
Displays one of the following values:

- For a NIC that provides access to the Secure Service Container web interface, the value is either a specific IPv4 or IPv6 address or, for IP address types of DHCP and Link Local, the word Automatic.
- For all other NICs, the value displayed is a dash (-).

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the NIC. The operating system to be installed on the partition will use this device number to access the NIC. When creating a new NIC for an OSA card or HiperSockets switch, DPM generates three consecutive device

numbers for the operating system to use for unit addresses, and displays only the first number in this field.

Change the device number if your company uses a specific numbering convention for its networks. To edit the device number, double-click in the table cell and type a new hexadecimal value. When you edit the device number for an OSA card or HiperSockets switch, DPM uses this new value as the first device number, and generates two consecutive device numbers based on the new value.

Notes:

- You cannot use a device number of 0000 for a PCI adapter, such as a RoCE adapter.
- The z/VM hypervisor does not support a device number of 0000 for an OSA card or HiperSockets switch.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port
Displays the adapter port value in decimal.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

VLAN ID & Type
Displays the identifier of the virtual local area network (VLAN) through which the network adapter sends and receives network traffic. This field also displays the type of VLAN configuration, such as VLAN Enforcement.

MAC Address
Displays the user-provided or system-generated unique media access control (MAC) address for this NIC.

Description
Displays the user-provided description, if any, of the network interface card. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Secure Service Container Web Interface Communication

The "Secure Service Container Web Interface Communication" section displays network settings for a Secure Service Container partition. Some of the displayed values depend on the IP address type of the NIC that provides access to the web interface. An asterisk (*) preceding the label indicates that a value is required. These fields are read-only until you click **RESET NETWORK**.

Host Name
Specifies the Linux host name of the appliance to run in the Secure Service Container partition. To access the Secure Service Container web interface, users need to specify a URL that contains either a host name or an IP address for the Secure Service Container partition. A host name can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (any case), and the following special characters: period (.), colon (:), and hyphen (-).

Default IPv4 Gateway
Specifies an IPv4 address for the default gateway. A default IPv4 gateway is required if you specified a Static IPv4 IP address type for the NIC.

Default IPv6 Gateway
Specifies an IPv6 address for the default gateway. A default IPv6 gateway is required if you specified a Static IPv6 IP address type for the NIC.

DNS Server 1
Specifies an IPv4 or IPv6 address for the primary domain name system (DNS) server. A DNS server definition is required if you specified a Dynamic Host Configuration Protocol (DHCP) IP address for the NIC.

DNS Server 2
Specifies an IPv4 or IPv6 address for a secondary DNS server.

RESET NETWORK
Click **RESET NETWORK** to remove any previously supplied values for fields in the "Secure Service Container Web Interface Communication" section, so you can supply new values. To save the new values and associate them with the NIC that provides access to the web interface, click **Apply**; otherwise, click **Cancel** to cancel the reset operation.

New Network Interface Card

Use the **New Network Interface Card** window to create a network interface card (NIC). On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Initially displays a system-generated name for the new NIC, which you can edit by double-clicking in the name field and typing a new name. The NIC name must be different from the name of any other NIC that you define for this new partition.

Description
Optionally, provide a description for this new NIC. The description can be up to 1024 characters in length.

Device Number
Optionally, provide a 4-digit hexadecimal device number in the range 0000 - ffff. If you do not provide a value, the system automatically generates a unique device number. When creating a new NIC for an OSA card or HiperSockets switch, DPM generates three consecutive device numbers for the operating system to use for unit addresses; if you supply a value, the system uses this value as the first device number.

For a NIC that is backed by a PCI-based adapter, DPM generates a unique identifier (UID) that is used as the PCI device number. The value is used only if the operating system supports PCI device numbers.

VLAN ID
For partitions with a type of **Linux** or **z/VM** only, optionally specify the identifier of the virtual local area network (VLAN) through which the network adapter is to send and receive network traffic for this partition and the operating system or hypervisor that it hosts.

- The valid range of VLAN IDs is 1 - 4094.
- You can specify a VLAN ID for this NIC only when you select an OSA-Express or HiperSockets adapter.

  This field is not displayed for partitions with a type of **Secure Service Container**, but you can specify a VLAN ID for that partition type by setting the **Use to access the web interface** switch to **YES**, and entering a value in the **VLAN ID** field displayed in the section under that switch.

VLAN Type
If you provide a VLAN ID, this field, which specifies the type of VLAN configuration, is displayed. The default value is VLAN Enforcement. To complete the setup for VLAN enforcement, you must specify the same VLAN ID in the network configuration files for the operating system or hypervisor.

MAC Address
Optionally, specify a unique media access control (MAC) address that is both locally administered and unicast. A MAC address consists of six groups of two lower-case hexadecimal digits, separated by colons; for example: `02:ff:12:34:56:78`

You can specify a MAC address for any type of partition, but only when you select an OSA-Express or HiperSockets adapter for the NIC. DPM checks the validity and uniqueness of the value that you supply, and issues a message if it finds an error. If you do not specify a value, DPM automatically generates a unique MAC address for the NIC.

Use to access the web interface
Only when the partition type of this partition is **Secure Service Container**, the display includes a switch to indicate whether you can configure this NIC to access the Secure Service Container web interface. If this NIC is the only NIC defined for this Secure Service Container partition, you cannot set this switch to **NO**. When the switch is set to **YES**, the display includes the following configuration settings, which Secure Service Container partitions require for access to the web interface. For a Secure Service Container partition, you can select only an OSA or HiperSockets adapter.

VLAN ID
Specify the virtual local area network (VLAN) if the link you are using is defined in TRUNK mode. The valid range of VLAN IDs is 1 - 4094. Note that DPM does not provide VLAN enforcement for Secure Service Container partitions.

IP Address Type
Select one of the following types:

- **DHCP** (Dynamic Host Configuration Protocol)
- **Link Local**
- **Static IPv4 Address**
- **Static IPv6 Address**

The selected type determines which of the remaining fields require values. An asterisk (*) preceding the label indicates that a value is required.

IP Address
Enter the IP address of the network adapter. This field is required only for IP addresses of type **Static IPv4 Address** and **Static IPv6 Address**.

Mask/Prefix
For an IPv4 address type, enter the mask/prefix in either bit notation (for example, `/24`) or mask notation (for example, `255.255.255.0`). For an IPv6 address type, enter the mask/prefix in bit notation only.

Adapter Ports and Switches table
Lists all of the configured ports or switches for all of the configured network adapters on this system. To successfully define a new NIC, you must select only one table entry.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. Select only one adapter port or switch for the new NIC.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port
Displays the adapter port value in decimal.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

Uplink Utilization
Indicates the average uplink utilization for the port or switch over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different port or switch on the same network. The utilization is shown in both a graphic progress bar and in numeric percentage. For OSA and RoCE adapters, the physical port utilization is displayed; for HiperSockets, the switch utilization is displayed.

Adapter NIC Allocation
Indicates the percentage of NICs that are currently allocated to the adapter for this port or switch. If the percentage is high (for example, 90%), consider selecting a different port or switch on the same network. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes NICs only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Each network adapter port or switch has enough allocation space to support a maximum number of NICs; the maximum number varies depending on the adapter type. If you select a port or switch on an adapter that does not have sufficient allocation space for this new NIC, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a port or switch on a different adapter.
- If the partition is stopped and you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the port or adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new NIC, click **OK** to create the NIC definition and close the **New Network Interface Card** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Storage

Use the Storage section to view, to modify, or to attach storage groups and tape links, or to create host bus adapters (HBAs) that enable the partition to access storage networks and hardware that is connected to the DPM-enabled system.

Depending on the version of DPM that is applied on the system, the Storage section contains a Storage Groups table, a Tape Links table, or an HBAs table with controls that you can use to attach storage groups and tape links, or to create HBAs. Follow the instructions that correspond to the type of table displayed on the page.

- "Viewing or modifying attached storage groups or tape links (DPM R3.1 or later)" on page 1224
- "Viewing or modifying HBAs for FCP storage access (DPM R3.0 or earlier)" on page 1226

Viewing or modifying attached storage groups or tape links (DPM R3.1 or later)

System administrators create storage groups and tape links to enable partitions (and the operating systems and applications that they host) to use physical storage hardware that is connected to the system. A *storage group* is a logical group of storage volumes that share certain attributes. A *tape link* defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN.

DPM supports the following types of storage groups and tape links.

- FICON storage groups, which consist of volumes that reside on external Fibre Connection (FICON) extended count key data (ECKD) direct-access storage devices (DASD). This type of storage group is available starting with DPM R3.1.
- FCP storage groups, which consist of volumes that reside on external Fibre Channel Protocol (FCP) Small Computer System Interface (SCSI) disk storage devices. This type of storage group is available starting with DPM R3.1.
- Non-Volatile Memory Express (NVMe) storage groups, which consist of solid state drives (SSDs) that are installed in carrier cards in the system I/O drawers. NVMe storage is available only when the system has one or more IBM Adapter for NVMe1.1 features. This type of storage group is available starting with DPM R4.2.
- FCP tape links, each of which defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN. These connection attributes include storage resources such as system adapters, world wide port names (WWPNs), and the number of partitions that can share the connection. Support for FCP tape links is available starting with DPM R4.3.

FICON and FCP storage groups can be shared by multiple partitions, and multiple storage groups can be attached to one partition. FCP tape links also can be shared by multiple partitions, and multiple tape links can be attached to one partition. In contrast, only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared. However, a partition that has attached NVMe storage groups can also have attached FICON and FCP storage groups, and FCP tape links.

To attach new storage groups or tape links to the partition, complete the following steps.

1. Select the plus icon in the table toolbar to open the **Attach Storage Groups** or **Attach Tape Links** window. (Note that you can use the minus icon in the table toolbar to detach a storage group or tape link from the partition.)
   - On the **Attach Storage Groups** window, select one or more storage groups listed in the Storage Groups table to attach to this partition.
     - The suggested practice is to select storage groups that are in the Complete fulfillment state, but you can select any storage group except for those with a fulfillment state of Incomplete, or those that are already attached to the maximum number of partitions. If you do select groups in states other than Complete, some storage might not be available for use when you start the partition.
     - Use the additional information in the Storage Groups table, as necessary, to decide which storage groups to attach. For descriptions of the columns in the Storage Groups table, see "Attach Storage Groups" on page 1229.

When you have finished selecting storage groups to attach, select **OK** to close the **Attach Storage Groups** window.

- On the **Attach Tape Links** window, select one or more tape links listed in the table to attach to this partition.
  - The suggested practice is to select tape links that are in the Complete fulfillment state, but you can select any tape link except for those with a fulfillment state of Incomplete, or those that are already attached to the maximum number of partitions. If you do select links in states other than Complete, some storage might not be available for use when you start the partition.
  - Use the additional information in the table, as necessary, to decide which tape links to attach. For descriptions of the columns in the table, see "Attach Tape Links" on page 1230.

  When you have finished selecting tape links to attach, select **OK** to close the **Attach Tape Links** window.

2. Check the entries for the storage groups or tape links that you selected, which are now displayed in the Storage Groups table or Tape Links table in the Storage section. If necessary, you can use the minus icon in the table toolbar to remove a storage group or tape link from the table.
   - For FICON storage groups only, you can change the volume device numbers only when the device number input field is active. The factors that determine whether you can change the device number include not only the current state of the partition, but also whether the storage group is shared or dedicated, and whether it is already attached to other partitions.
   - For FCP storage groups and FCP tape links only, you can expand the table entry to show the system-generated host bus adapters (HBAs) and their assigned adapters. You can change the device numbers that DPM automatically assigned to the HBAs when you selected the FCP storage group or FCP tape link. An error icon is displayed if you try to specify a device number that is already in use.
   - For FCP storage groups only, the expanded display also includes a link through which you can open the FCP adapter assignment window, and remove or replace the adapters that DPM automatically assigned to the HBAs.

   For more details, see the following topics.
   - "Host Bus Adapters (HBA) table for an FCP storage group or tape link" on page 1226
   - "FCP adapter assignment" on page 1231
3. When you have finished, review another section or click **OK** to save the partition definition.

   If the partition is running, or when you restart a stopped partition, you might need to enter Linux commands to make any newly attached storage groups available to the operating system that the partition hosts. NVMe storage groups are automatically detected by the operating system, so you do not need to enter Linux commands to make that type of storage group available to the operating system. Similarly, the tape devices that are available through attached tape links are automatically detected by the operating system, so you do not need to enter Linux commands for tape devices either. The actions required for FCP or FICON storage groups depend on the type and fulfillment state, and whether the storage group contained the boot volume for the operating system.

   When attaching a storage group in Complete state when the partition is stopped

   - For an FCP storage group:
     - If the storage group contained the boot volume, the operating system brings online all of the HBAs for this storage group, and all volumes in the storage group are available. No action is required unless you have attached other storage groups.
     - If the storage group does not contain the boot volume, and the operating system is not configured to bring HBAs online automatically, you need to issue the **chccwdev** command to bring online all of the HBAs.
   - For a FICON storage group, the operating system brings online only the boot volume. You need to issue the **chccwdev** command to bring online all of the remaining volumes in the storage group that contains the boot volume, as well as the volumes in any other storage groups that you attached.

When attaching a Complete storage group to a running partition, or attaching an unfulfilled storage group that becomes Complete as the partition is running

- For an FCP storage group:
  - If adapters were assigned to HBAs while the partition is running, you need to use the **chchp** command to activate the channel paths for those new adapters.
  - To access the volumes in the storage group, you need to issue the **chccwdev** command to bring online all of the HBAs.
- For a FICON storage group:
  - If the adapters connecting the storage group to the storage subsystem were assigned while the partition is running, use the **chchp** command to activate the channel paths for those new adapters.
  - All volumes are offline. You need to issue the **chccwdev** command to bring online all of the volumes in the storage group.

To find the IDs that you need to use for the Linux commands, use the following tasks.

- HBA device numbers are available in the Host Bus Adapters (HBA) table when you expand the storage group table entry in the Storage section of the **Partition Details** task.
- Channel path IDs for FCP adapters are shown in the Host Bus Adapters (HBA) table when you expand the storage group table entry in the Storage section of the **Partition Details** task.
- Channel path IDs for FICON adapters are shown on the **ADAPTERS** tab of the Storage Group details; open the **Configure Storage** task and select the storage group in the **Storage Overview** to open the Storage Group details page.
- FICON volume device numbers are shown on the **VOLUMES** tab of the Storage Group details page; open the **Configure Storage** task and select the storage group in the **Storage Overview** to open the Storage Group details page.

Host Bus Adapters (HBA) table for an FCP storage group or tape link

For FCP storage groups or tape links only, you can expand the Storage Groups or Tape Links table entry to show the Host Bus Adapters (HBA) table. The following list describes the columns in the table; depending on the fulfillment state of the storage group or tape link, some information might not be available.

Name
Displays the system-generated name of the HBA.

Device Number
Displays the system-generated hexadecimal device number for the HBA. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by typing a new value in the column field.

WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a port in a disk storage subsystem or tape library that is connected to the system.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Adapter ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

Assigned Adapter
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

Viewing or modifying HBAs for FCP storage access (DPM R3.0 or earlier)

Host bus adapters (HBAs) provide a partition with access to external storage area networks (SANs) and devices that are connected to a system. Each HBA represents a unique connection between the partition

and a physical FICON channel that is configured on the system. When you modify or create an HBA, you can select the adapter that you want to use from a list of all of the storage adapters that are currently configured on the system.

- For availability, select at least two storage adapters of the same type, and create an HBA for each one.
- If you are creating a Secure Service Container partition to install a software appliance, define at least one HBA to access the storage device on which the appliance installation image resides.

The following topics describe the HBAs table actions and elements.

- "The HBAs table toolbar" on page 1227
- "Columns in the HBAs table" on page 1227
- "Standard table functions" on page 1228

The HBAs table toolbar

The HBAs table contains an entry for each host bus adapter, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Host Bus Adapter** window, through which you can create a new host bus adapter (HBA). For more information, see "New Host Bus Adapter" on page 1232.

Details
Opens the **HBA Details** window. This action is enabled when only one HBA is selected in the table. The **HBA Details** window fields and controls are the same as those for the **New Host Bus Adapter** window, with the following exceptions:

- The name, description (if any), device number, and adapter port selection are displayed for the selected HBA.
- The read-only WWPN field displays the worldwide port name of the HBA. A WWPN is automatically assigned to an HBA when the HBA is created, and provides a unique identifier for it in the network.
- The Device number field is marked as a required field.

Delete
Opens the **Delete HBA** confirmation window through which you can delete one or more HBAs. This action is enabled when one or more HBAs are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected HBAs. The confirmation window closes, and the resulting HBAs table display does not contain any entries for the deleted HBAs. The HBAs are not actually deleted until you click **OK** or **Apply** on the main window of the **Partition Details** task.
- Click **Cancel** to close the confirmation window and return to the Storage section, without deleting any HBAs.

Adapter Details
Opens the **Adapter Details** task in a separate window. This action is enabled when one or more HBAs are selected in the table.

Columns in the HBAs table

The HBAs table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a host bus adapter (HBA). The name is a hyperlink through which you can open the **HBA Details** window. To edit the name, double-click in the table cell and type the new name.

If this HBA represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

WWPN
Displays the worldwide port name of the HBA. A WWPN is automatically assigned to an HBA when the HBA is created, and provides a unique identifier for it in the network.

Type
Indicates the HBA type, which matches the type of adapter port that is selected when the HBA is created. The valid value is FCP, which represents Fibre Channel Protocol mode.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the HBA. The operating system to be installed on the partition will use this device number to access the HBA. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by selecting the **Details** action and editing the HBA device number. To edit the device number, double-click in the table cell and type a new hexadecimal value.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Description
Displays the user-provided description, if any, of the host bus adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Attach Storage Groups
Use the **Attach Storage Groups** window to select one or more storage groups to attach to the partition. This window contains the Storage Groups table, which lists all storage groups that system administrators have defined for use by partitions on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The Storage Groups table contains the following information and controls.

Select
Use check boxes in the Select column to identify which storage groups you want to attach to the partition. If a check box is disabled, either the storage group is attached to the maximum number of partitions, or you do not have permission to access the storage group.

Name
Specifies the user-defined name of the storage group. The name is a link that opens to the Storage Group details page in the Configure Storage task.

Type
Specifies the type of storage group: FICON or FCP or NVMe.

Partitions
Specifies the number of partitions to which the storage group is attached.

Shareable
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

Total Capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Description
Specifies the user-provided description, if any, of this storage group.

Fulfillment state
Identifies the current state of the storage group. DPM runs a background check of storage resources for FCP storage groups and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours)..

Checking migration
This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

Conflicts
Specifies whether any device numbers will be duplicated in the configuration if you attach a FICON storage group. This column contains a warning icon and message when one or more of the following conditions are true.

- One or more of the base or alias volume device numbers used in a FICON storage group are the same as a device number that is in use for this partition for a network connection through an OSA card or HiperSockets switch.
- One or more of the base or alias volume device numbers used in a FICON storage group are the same as a device number that is in use for one of the currently attached FICON or FCP storage groups.

To determine which device numbers conflict, select the chevron (⌄) to expand the table entry and display the Conflicting Device Numbers tables. One table identifies the device numbers for the storage group volumes, and another table lists the device numbers of configured partition resources that are in conflict. This second table lists the device number, device name, resource type, and a link to the task or page through which you can resolve the conflict.

To resolve conflicts, you can either change the conflicting device numbers, or remove the storage group. In some cases, you can edit the device numbers directly in the Conflicting Device Numbers tables. The Device Number column fields in both tables are editable depending on the shareability of the FICON storage group, whether the storage group is already attached to the partition, and the current state of the partition.

OK
After you have selected one or more storage groups, click **OK** to return to the Storage section of the **Partition Details** task.

CANCEL
To close the window without saving any selections, click **CANCEL**.

Attach Tape Links
Use the **Attach Tape Links** window to select one or more tape links to attach to the partition. This window contains the a table listing all tape links that system administrators have defined for use by partitions on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The table contains the following information and controls.

☐
Use check boxes in each table row or in the table header to identify which tape links you want to attach to the partition. If a check box is disabled, either the storage group is attached to the maximum number of partitions, or you do not have permission to access the storage group.

Name
Specifies the user-defined name of the tape link. The name is a hyperlink that opens to the Tape Link details page in the **Configure Storage** task.

Type
Specifies the type of tape link: FCP.

Partitions
Specifies the number of partitions to which the tape link is attached.

Shareable
Specifies whether the tape link can be shared among partitions, or whether it is dedicated to only one partition.

Description
Specifies the user-provided description, if any, of this tape link. The description can be up to 200 characters in length.

Fulfillment state
Identifies the current state of the tape link. DPM runs a background check of storage resources for FCP tape links and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours).

Complete
All of the storage resources listed in a create or modify request are available, properly configured and zoned, and DPM detects only those resources.

Incomplete
One or more storage resources for the tape link are marked as incomplete because the resource is missing, or in an error or degraded condition. Because DPM periodically checks the availability of storage adapters, switches, and tape libraries that are in use for a tape link, resources that were functioning properly can become incomplete.

Pending
One or more requested storage resources are not yet available or zoned correctly, or the tape link is not yet attached to all partitions that were specified in the original create request or a modify request.

Pending with mismatches
DPM detects system adapters that do not match the original create request or a modify request. Either the number of system adapters does not match the number of connecting paths, or the detected adapters do not match specific adapters that were assigned to the tape link.

OK
After you have selected one or more tape links, click **OK** to return to the Storage section of the **New Partition** task.

CANCEL
To close the window without saving any selections, click **CANCEL**.

FCP adapter assignment
Use the **FCP adapter assignment** window to review the adapters assigned to a storage group and remove or replace them with other adapters that are available for use by a partition. This window is available only on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The **FCP adapter assignment** window displays two tables: Assigned Adapters and Adapter Candidates. Each table contains the same columns and has a footer that indicates the total number of adapters in the table. You might need to scroll to see all table entries, or use the Search field to filter the table entries. The search string applies to both tables. Note that any incomplete adapters are indicated by an incomplete icon ( ).

If an FCP adapter is configured while the storage group is attached to an active partition, DPM cannot detect and list the new adapter as available for use by any partition. To make sure that you can choose from a complete list of available adapters, stop all active partitions to which the storage group is attached, and select the **Connection Report** icon to start a background check of the available connections for this storage group. To view all partitions that are using the storage group, go to **Configure Storage** > **Storage Overview**, open the Storage Details page for the storage group, and select the **PARTITIONS** tab.

If you need to assign new adapters, the Assigned Adapters table contains a placeholder row for each required adapter. To fill those placeholders, use one of the following methods.

- Use the **Automatically assign** icon ( ) to have DPM automatically select redundant adapters across all fabrics. DPM selects the adapters with the lowest allocation percentage and the fastest card type.
- Use the buttons in the Action table column to manually change adapter assignments, one adapter at a time. The suggested practice is to assign at least two adapters from each fabric for redundancy.
  1. In the Assigned Adapters table, select **UNASSIGN** to remove individual adapters.
  2. In the Adapter Candidates table, select **ASSIGN** to assign different adapters. Newly assigned adapters are indicated by a blue dot next to the table row in the Assigned Adapters table.

If you need to change all of the currently assigned adapters, use the **Unassign all** icon ( ) to empty the Assigned Adapters table. Then use either the **Automatically assign** icon or the Action buttons to assign new adapters.

When you have finished, select **SAVE** to return to the Storage section of the **Partition Details** task.

The following list describes the columns that are displayed in both of the tables on the **FCP adapter assignment** window.

Adapter Name
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

Adapter ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

Location
Specifies the physical location of the adapter in the I/O drawer of the system.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Allocation
Indicates the percentage of host bus adapters (HBAs) that are currently allocated to this adapter, shown in a bar graph and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. If the percentage is high (for example, 90%), consider assigning a different adapter.

Action
Contains one of the following buttons.

- In the Assigned Adapters table, **UNASSIGN** removes the adapter in the table row and moves the table row into the Adapter Candidates table.
- In the Adapter Candidates table, **ASSIGN** assigns the adapter in the table row and moves the table row into the Assigned Adapters table.

New Host Bus Adapter

Use the **New Host Bus Adapter** window to create a new host bus adapter (HBA). On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Initially displays a system-generated name for the new HBA, which you can edit by double-clicking in the name field and typing a new name. The HBA name must be different from the name of any other HBA that you define for this new partition.

Description
Optionally, provide a description for this new HBA. The description can be up to 1024 characters in length.

Device number
Optionally, provide a 4-digit hexadecimal device number in the range 0000 - ffff. If you do not provide a value, the system automatically generates a unique device number.

Adapter Ports table
Lists all of the configured ports for all of the configured storage adapters on this system. To successfully define a new HBA, you must select only one table entry.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Adapter HBA Allocation
Indicates the percentage of HBAs that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter port. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Each storage adapter port has enough allocation space to support a maximum of 254 HBAs, but your system planner can change that maximum to a lower value. If you select an adapter port that does not have sufficient allocation space for this new HBA, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different adapter.
- If the partition is stopped and you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Location
Displays the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the port or adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new HBA, click **OK** to create the HBA definition and close the **New Host Bus Adapter** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Accelerators

An accelerator virtual function provides a partition with access to specific features, such as zEnterprise Data Compression (zEDC), that are installed on a system. Each virtual function represents a unique connection between the partition and a physical feature card that is configured on the system. This section is displayed only when a system that supports accelerators is managed through this HMC, and is enabled only for systems that support accelerators.

Use the Accelerators section to view, to modify, or to create virtual functions that enable the partition to access specific features installed on the DPM-enabled system. When you create a virtual function, you can select the adapter that you want to use from a list of all of the accelerator adapters that are currently configured on the system.

Accelerators are optional features and, therefore, might not be installed on the system. If none are installed, the Accelerators section is disabled.

The following topics describe the Accelerator Virtual Functions table actions and elements.

- “The Accelerator Virtual Functions table toolbar” on page 1234
- “Columns in the Accelerator Virtual Functions table” on page 1234
- “Standard table functions” on page 1235

The Accelerator Virtual Functions table toolbar

The Accelerator Virtual Functions table contains an entry for each virtual function, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Virtual Function** window to create a new virtual function. For more information, see "New Virtual Function" on page 1235.

Details
Opens the **Virtual Function Details** window. This action is enabled when only one virtual function is selected in the table. The **Virtual Function Details** window fields and controls are the same as those for the **New Virtual Function** window, with the following exceptions:

- The name, description (if any), device number, and adapter selection are displayed for the selected virtual function.
- The Device number field is marked as a required field.

Delete
Opens the **Delete Virtual Function** confirmation window through which you can delete one or more virtual functions. This action is enabled when one or more virtual functions are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected virtual functions. The confirmation window closes, and the resulting Accelerator Virtual Functions table display does not contain any entries for the deleted virtual functions. The virtual functions are not actually deleted until you click **OK** or **Apply** on the main window of the **Partition Details** task.
- Click **Cancel** to close the confirmation window and return to the Accelerators section, without deleting any virtual functions.

Adapter Details
Opens the **Adapter Details** task. This action is enabled when one or more virtual functions are selected in the table.

Columns in the Accelerator Virtual Functions table

The Accelerator Virtual Functions table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the virtual function. The name is a hyperlink through which you can open the **Virtual Function Details** window. To edit the name, double-click in the table cell and type the new name.

If this virtual function represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Type
Indicates the virtual function type, which matches the type of adapter that is selected when the virtual function is created. The valid value is zEDC, for the zEnterprise Data Compression (zEDC) feature, which provides hardware-based acceleration for data compression and decompression.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the virtual function. The operating system to be installed on the partition will use this device number to access the virtual function.

Change the device number if your company uses a specific numbering convention for its accelerators. To edit the device number, double-click in the table cell and type a new hexadecimal value. Note that you cannot use a device number of 0000 for accelerator adapters.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports.

Description
Displays the user-provided description, if any, of the virtual function. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

New Virtual Function

Use the **New Virtual Function** window to create a new virtual function. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Provide a name for the new virtual function. The virtual function name must be different from the name of any other virtual function that you define for this new partition.

Description
Optionally, provide a description for this new virtual function. The description can be up to 1024 characters in length.

Device Number
Optionally, provide a 4-digit hexadecimal device number in the range 0000 - ffff. If you do not provide a value, the system automatically generates a unique device number. The number is used only if the operating system supports device numbers.

Adapter table
Lists all of the configured accelerators on this system.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. Select only one adapter for the new virtual function.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports.

Utilization
Indicates the average utilization for the adapter over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different adapter. The utilization is shown in both a graphic progress bar and in numeric percentage.

Virtual Function Allocation
Indicates the percentage of virtual functions that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes virtual functions only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Up to 15 partitions can share a zEDC feature. If you select an adapter that does not have sufficient allocation space for this new virtual function, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different adapter.
- If the partition is stopped and you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new virtual function, click **OK** to create the virtual function definition and close the **New Virtual Function** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Cryptos

The term *cryptos* is a commonly used abbreviation for adapters that provide cryptographic processing functions. Use the Cryptos section to view or modify the cryptographic adapters and domains that are assigned to the partition, or to enable the partition to use the cryptographic adapters that it requires, to assign a usage domain and, optionally, to assign control domains. Usage domains provide access to cryptographic functions, and provide the ability to manage domains and keys. Control domains provide only the ability to manage domains and keys.

Crypto features are optional and, therefore, might not be installed on the system. If none are installed, the Cryptos section is disabled.

When crypto adapters are installed on a system, they are configured in either coprocessor or accelerator mode, depending on the type of cryptographic processing that is required by the applications that run on the system. Each coprocessor or accelerator contains a specific number of usage domains, identified by an index number, which contain an isolated set of master keys. When you create a new partition, you select only one usage domain index to assign to your partition, and that index assignment applies for each cryptographic adapter that your partition can access.

Depending on the type of crypto adapter that you select, you might also need to define one or more control domains.

Additionally, you can enable or disable the key import functions that are available through the CP Assist for Cryptographic Functions (CPACF) feature. CPACF supports clear and protected key encryption based on the Advanced Encryption Standard (AES) algorithm, and the Secure Hash Algorithm (SHA) with the Data Encryption Standard (DES) algorithm, and the Elliptic Curve Cryptography (ECC) algorithm. For operating systems and applications to take advantage of key encryption support, the partition in which they run must be configured to permit AES, or DES, or ECC protected key import functions.

The following topics describe the table actions and elements in the Cryptos section.

Fields for CPACF Key Management Operations

Review the options for the CPACF Key Management Operations that are, by default, selected for this partition. If necessary, click the check box to deselect one or all options. Note that you cannot deselect a key import permission while the partition is active.

Permit AES key import functions
When selected, this option enables applications that run in this partition to generate and manage AES protected keys through the CPACF feature.

Permit DES key import functions
When selected, this option enables applications that run in this partition to generate and manage DES protected keys through the CPACF feature.

Permit ECC key import functions
When selected, this option enables applications that run in this partition to generate and manage ECC protected keys through the CPACF feature. Note that only specific systems support the ECC algorithm; if this system does not support ECC, this key import selection is disabled.

The Adapters table toolbar

The Adapters table contains an entry for each cryptographic coprocessor or accelerator, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of

the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

Add
Opens the **Add Adapters** window through which you can add one or more crypto adapters to be used by the partition. For more information, see "Adding cryptographic adapters and domains" on page 1240.

Remove
Opens the **Remove Adapters** confirmation window through which you can remove one or more adapters from the partition definition. This action is enabled when one or more adapters are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Remove** to confirm that you want to remove the selected adapters. The confirmation window closes, and the resulting Adapters table display does not contain any entries for the deleted adapters.
- Click **Cancel** to close the confirmation window and return to the Cryptos section, without removing any adapters.

Adapter Details
Opens the **Adapter Details** task. This action is enabled when one or more adapters are selected in the table.

Columns in the Adapters table

The Adapters table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Crypto Number
Indicates the adjunct processor number that is assigned to this adapter. This number is associated with the use of the Adjunct Processor Extended Addressing (APXA) facility, which is only available on specific systems. This facility increases the number of usage domains that can be supported on one cryptographic adapter.

Conflicts
Displays a warning icon in the column, only if one or more domain conflicts exist for a specific adapter. To display additional information about the conflicts, click the warning icon to open the Crypto Conflicts window. For more details, see "Crypto Conflicts - adapter" on page 1242.

Type
Indicates the mode in which the cryptographic adapter is configured on this system.

CCA coprocessor
The adapter is configured as a Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

EP11 coprocessor
The adapter is configured as an Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.

Accelerator
The adapter is configured as an Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific Crypto Express adapter names.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

The Adapter Domains table toolbar

When you first use the **New Partition** task, the Cryptos display contains only an Adapters table; after you add crypto adapters, the display also includes an Adapter Domains table.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

Add Control Domains
Opens the **Add Control Domains** window through which you can add more control domains. For more information, see the Add Control Domains section in “Adding cryptographic adapters and domains” on page 1240.

Add Usage Domains
Opens the **Add Usage Domains** window through which you can add more usage domains. For more information, see the Add Usage Domains section in “Adding cryptographic adapters and domains” on page 1240.

Remove
Opens the **Remove Domains** confirmation window through which you can remove one or more domains from the partition definition. This action is enabled when one or more domains are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Remove** to confirm that you want to remove the selected domains. The confirmation window closes, and the resulting Adapter Domains table display does not contain any entries for the deleted domains.
- Click **Cancel** to close the confirmation window and return to the Cryptos section, without removing any domains.

Columns in the Adapter Domains table

The Adapter Domains table lists each selected usage or control domain in a table row, with a table column for each of the selected adapters that are associated with the domain. Depending on how many adapters you selected, you might need to use the horizontal scroll controls to see all of the table columns.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Displays the index number assigned to each of the usage domains or control domains added to the partition definition. A letter icon that precedes the index number indicates whether the domain is a usage domain (**U**) or a control domain (**C**).

Adapters
Each remaining column in the Adapter Domains table represents a selected adapter, with the adapter name shown as the column heading. For each domain listed in the table, the adapter column displays either a checkmark or a warning icon, to indicate whether any conflicts exist. To display additional information about the conflict, click the warning icon to display the Crypto Conflicts window. For more details, see "Crypto Conflicts - Usage Domain number" on page 1243.

Standard table functions

In addition to the customized action icons and the Actions list, the Adapters table and Adapter Domains table toolbars include the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Adding cryptographic adapters and domains

When you first select **Add** to add cryptographic adapters to the partition definition, DPM opens a dialog that consists of several windows through which you can select adapters and domains. On any window, you can click **Cancel** to close the dialog and return to the Cryptos section. Otherwise, make a selection and click **OK** to advance to the next window.

In contrast, when you subsequently access the dialog windows through selections in the **Actions** list of the Adapter Domains table, you can access the domain dialog windows separately; DPM opens the appropriate dialog window, based on your selection. Clicking **OK** or **Cancel** returns you to the Crypto section.

The following lists describe the contents of each dialog window, in the order in which DPM presents them. Each window contains a table through which you make your selections; each of these tables has a toolbar with standard table functions, such as filters.

Add Adapters
The **Add Adapters** window displays a table containing one entry for each available crypto adapter that is not already assigned to this new partition. Use the Select column to select one or more adapters for the new partition to use.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Crypto Number
Indicates the adjunct processor number that is assigned to this adapter. This number is associated with the use of the Adjunct Processor Extended Addressing (APXA) facility, which is only available on specific systems. This facility increases the number of usage domains that can be supported on one cryptographic adapter.

Conflicts
Displays a warning icon in the column, only if one or more domain conflicts exist for a specific adapter. To display additional information about the conflicts, click the warning icon to open the Crypto Conflicts window. For more details, see "Crypto Conflicts - adapter" on page 1242.

If you select an adapter that has domain conflicts, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different adapter.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because at least one other partition definition contains the same adapter and usage domain.

Type
Indicates the mode in which the cryptographic adapter is configured on this system.

CCA coprocessor
The adapter is configured as a Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

EP11 coprocessor
The adapter is configured as an Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.

Accelerator
The adapter is configured as an Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific Crypto Express adapter names.

Utilization
Indicates the average utilization for the adapter over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different adapter. The utilization is shown in both a graphic progress bar and in numeric percentage.

Usage Domain Allocation
Indicates the percentage of usage domains that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes usage domains only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions cannot exceed 100%.

Each adapter supports up to 16 usage domains, but that limit can be increased through the use of the adjunct processor extended addressing facility, depending on the machine type and configuration of the DPM-enabled system. If you select an adapter that does not have sufficient

allocation space, an error message is displayed above the table, indicating that the new partition might fail to start because this adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Add Usage Domains
The **Add Usage Domains** window displays a table containing one entry that represents each available usage domain and control domain, with usage domains listed first, by default. To limit the table entries to only those domains that are not defined to any partition on the system, select the **Hide usage domains defined to other partitions** check box. By default, the check box is checked.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Indicates the index number assigned to the usage domain or control domain. Each coprocessor or accelerator contains a specific number of usage domains, identified by an index number, which contain an isolated set of master keys. When you create a new partition, you select only one usage domain index to assign to your partition, and that index assignment applies for each cryptographic adapter that your partition can access. If you select a control domain, it is converted into a usage domain.

Conflicts
When the **Hide usage domains defined to other partitions** check box is unchecked, the Conflicts column is shown in the table. If a conflict exists for a specific domain, a warning icon is shown in the column. To display additional information about the conflict, click the warning icon to display the Crypto Conflicts window. For more details, see “Crypto Conflicts - Usage Domain number” on page 1243.

If you select a domain that has conflicts, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different usage domain.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because at least one other partition definition contains the usage domain for one or more of the same adapters.

Add Control Domains
The **Add Control Domain** window displays a table containing one entry that represents each available control domain.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Indicates the index number assigned to the control domain. Control domains provide only the ability to manage domains and keys. If the partition is configured as the TCP/IP host for the Trusted Key Entry (TKE) workstation, you need to assign control domain indexes to the partition. Otherwise, selecting a control domain is optional. You can select one or more control domains.

Crypto Conflicts - adapter

Use the Crypto Conflicts window to view details about domain conflicts for a specific adapter, the name of which is displayed in the window title. This window contains the Conflicting Partitions table, which contains an entry for each partition for which the definition includes the same cryptographic adapter and usage domains that you have selected for the new partition. The table contains the following columns.

Partition
Displays the name of a partition for which the definition contains one or more adapters or domains that match those you have selected for the new partition. The name is a hyperlink through which you can open the **Partition Details** task.

Active/Reserved
Indicates whether the existing partition is active or reserved. If the partition is either active or reserved, a checkmark is displayed.

Usage Domains
Specifies each of the domain index numbers that conflict with those index numbers you have selected for the new partition. If multiple index numbers are in conflict, each number is separated by a comma; if consecutive index numbers are in conflict, they are shown in ranges. For example: `0-3, 5, 8-10`

To close the window and return to the previous window, click **Close**.

Crypto Conflicts - Usage Domain number

Use the Crypto Conflicts window to view details about the conflicts for a specific usage domain, the index number of which is displayed in the window title. This window contains the Conflicting Partitions table, which contains an entry for each partition for which the definition includes the same usage domain for one or more cryptographic adapters that you have selected for the new partition. The table contains the following columns.

Partition
Displays the name of a partition for which the definition contains one or more adapters or domains that match those you have selected for the new partition. The name is a hyperlink through which you can open the **Partition Details** task.

Active/Reserved
Indicates whether the existing partition is active or reserved. If the partition is either active or reserved, a checkmark is displayed.

Adapters (Crypto Number)
Displays the name of each adapter that is associated with the usage domain. The name includes the crypto number, which is shown in parentheses. Each adapter name is a hyperlink through which you can open the **Adapter Details** task. If multiple adapters are listed for a specific partition, each adapter is shown on a separate line in the table.

To close the window and return to the previous window, click **Close**.

Boot

Partitions on a DPM-enabled system can host a single operating system or hypervisor. Use the Boot section to view the currently selected option, or to select the location of the executables for the hypervisor or operating system to be run in this partition, or to upload the required files to initialize the hypervisor or operating system when the partition itself is started. Some of these boot options require that you find and select an ISO image file, which is a collection of files and metadata for installing software, and an .INS file, which maps image components (for example, kernel, ramdisk, parameter file) to the appropriate storage addresses in main memory.

The Boot section contains the following fields.

Secure Boot
The **Secure Boot** option indicates whether you want to have DPM verify that the software signature matches the signature from the distributor. If the signature does not match, the boot process ends. This option is enabled only when:

- The partition has a partition type of Linux.
- The system that hosts the partition supports the Secure Boot for Linux function.
- You are booting the Linux operating system from a volume in an FCP or NVMe storage group.

Boot from

The "Boot from" menu lists the boot options that are available for the hypervisor or operating system. If an option in the list is disabled, hover your cursor over that option to display additional information for that option. If necessary, take appropriate action to make that selection available; for example, if you want to use the Storage device (SAN) option, return to the Storage page to attach a storage group with a boot volume. When you select a specific boot option, the display shows editable fields and other information related to the selected option. The following list describes each boot option, and provides instructions for providing any required information.

For the supported boot options and more detailed instructions for installing z/VM in a partition, see the *DPM Guide*, which is available through the Library link on IBM Resource Link.

None

Select this option if you want to start a partition without a hypervisor or operating system. Although the partition can be started, it is not in a usable state. This option is the default for partitions with a partition type of **Linux** and **z/VM**.

Secure Service Container

This boot option is the default for a Secure Service Container partition. The display includes the Boot in Installer Mode switch, which determines what processing is done when you start the partition.

YES

With the switch set to **YES**, the partition start process initializes the Secure Service Container Installer so you can install an appliance in the partition.

NO

With the switch set to **NO**, the partition start process effectively restarts an installed appliance. In this case, the Secure Service Container Installer is rebooted, and the installed appliance is restarted in the Secure Service Container partition on this and all subsequent reboots, until you change the switch setting.

Storage Group (SAN) or Storage device (SAN)

Select this option when the hypervisor or operating system executables reside on an internal or external storage device. This option is available only when storage groups or host bus adapters (HBAs) are defined for the partition.

When you select this option, the Boot section contains either a Storage Groups table or an HBA table. The Storage Groups table is displayed only when the DPM R3.1 storage management feature or a later DPM version is applied on the system. Follow the instructions that correspond to the type of table displayed on the page.

- “Boot from a boot volume in a storage group” on page 1244 (only for systems with the DPM R3.1 storage management feature or a later DPM version applied)
- “Boot from a boot volume accessed through an HBA” on page 1245

Boot from a boot volume in a storage group

The Storage Groups table displays the available storage groups that contain a boot volume. To view the available boot volumes, expand any table entry by selecting the storage group. The Storage Group table contains the following columns.

Select

Use a radio button in the Select column to identify the storage group that contains the boot volume for the operating system or hypervisor. Depending on the fulfillment state of the storage group and availability of a boot volume, the radio button might be disabled.

Name

Specifies the user-defined name of the storage group.

Type

Specifies the type of storage group: FICON or FCP or NVMe. The expanded table display contains a Boot Volume table that lists all available boot volumes that the storage group contains. The Boot Volume table content and Advanced Boot Volume Settings fields vary, depending on the storage group type. Note that, if you select an FCP storage group as the

boot source for Linux, you can select the Secure Boot option, only when the system that hosts the partition supports the Secure Boot for Linux function.

- For each boot volume in an FCP storage group, the Boot Volume table provides the universally unique identifier (UUID) and capacity of the volume, along with a user-supplied description, if any.
- For each boot volume in a FICON storage group, the Boot Volume table provides the name of the storage subsystem in which the volume resides, along with the volume ID, capacity, type, and device number. If a user-supplied description is available, it is also displayed in the table.
- For each boot volume in an NVMe storage group, the Boot Volume table provides the boot volume serial number and capacity, along with a user-supplied description, if any. When you select an NVMe volume, note that NVMe namespace management is not supported, so you can boot programs only from namespace ID=1.
- For descriptions of the optional fields in the Advanced Boot Volume Settings area, see Advanced (optional) boot settings.

Partitions
Specifies the number of partitions to which the storage group is attached.

Shareable
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

Total Capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Description
Specifies the user-provided description, if any, of this storage group.

Fulfillment state

Checking migration
This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

Boot from a boot volume accessed through an HBA

The HBA table displays the available host bus adapters. Select the HBA connected to the storage subsystem that hosts the boot volume, provide the 64-bit worldwide port number (WWPN) of the storage subsystem, and provide the 64-bit hexadecimal logical unit number (LUN) of the volume that contains the boot image. For example:

Target WWPN: 50:0a:09:85:87:09:68:ad or 500a0985870968 (hexadecimal)
Target LUN: 4021400000000000

Advanced (optional) boot settings

In addition, you can provide values for the following optional fields. The optional fields in the display vary, depending on whether you selected an HBA, an NVMe storage group, an FCP storage group, or a FICON storage group. If you selected a storage group, the optional fields are displayed under the list of boot volumes in the expanded table entry for the storage group.

Boot program selector (0-30)
The boot program selector is a single number that identifies a boot configuration on the SAN device, which can contain up to 31 (decimal 0 – 30) different configurations. Each configuration can be a Linux kernel, a kernel parameter file, or optionally a ram disk. Configurations are prepared through the Linux zipl tool.

Specifying a value is optional but useful for backup purposes. If you do not supply a value, DPM uses the default value of 0.

Boot record logical block address
The boot record logical block address identifies the entry or anchor point where the boot loader can find the hypervisor or operating system. For Linux operating systems, this address is the master boot record and is usually the first block on the IPL device. Through this optional setting, you can provide a different block address as the entry point. If you provide a value, specify the 64-bit load block address as a 16-digit hexadecimal string.

IPL load parameter
This optional field can contain initial program load (IPL) parameters to be passed to the operating system or hypervisor. You can specify a maximum of eight alphanumeric characters.

OS load parameters
Through this optional setting, you can provide operating system-specific parameters to be passed to the hypervisor or operating system during SCSI IPL (initial program load). The hypervisor or operating system has to support load parameters being passed during IPL.

For a Linux operating system, use this field to specify kernel parameters. During the boot process, these parameters are concatenated to the end of the existing kernel parameters that are used by your boot configuration.

- The specifications must contain ASCII characters only. If characters other than ASCII are present, the content of the field is ignored during IPL.
- If you specify the kernel parameters with a leading equal sign (=), the existing kernel parameters are ignored and replaced with the kernel parameters in this field.
- If you replace the existing kernel parameters, be sure not to omit any kernel parameters required by your boot configuration.

You can also specify load parameters to log in to the operating system or hypervisor through either the **Operating System Messages** task or the **Integrated 3270 Console** task:

- For the **Operating System Messages** task, type `sysc`
- For the **Integrated 3270 Console** task, type `sysg`

Network server (PXE)
Select this option when you want to use a preboot execution environment (PXE) on a network server. This option is available only if a network interface card (NIC) for either an OSA port or HiperSockets switch is defined for the partition.

When you select this option, the NIC table displays the available network interface cards. Select the NIC for the adapter that connects the partition to the network on which the network boot server resides.

FTP server
Select this option if you want to use FTP to boot an image that is located on a different system. Provide the following information:

Host name
Enter either the fully qualified domain name of the FTP server, or its IP address.

User name
Enter the user name on the target FTP server.

Password
Enter the password associated with the user name on the target FTP server.

INS file
Either click **Browse** to retrieve a list of INS files from the target FTP server and select one file, or enter the fully qualified name (relative to FTP root) of an INS file.

Depending on the size of the FTP site, browsing might require more time than manually entering the full path and name of the INS file. Also note that the browsing function returns INS files found in the user's home directory or its subdirectories. Because you cannot select a starting directory, or navigate to a directory above the user's home directory, manually entering the full path and name of the INS file might be more expedient.

If you click **Browse**, a separate window displays the user's home directory and its subdirectories. Select one INS file, and click **OK** to close the Browse FTP Server window.

FTPS server
Select this option if you want to use the FTP Secure (FTPS) protocol to boot an image that is located on a different system. FTPS uses the Secure Socket Layer (SSL) protocol to secure data. With this option, you need to supply a host name, user ID, password, and .INS file, as described for the **FTP server** boot option.

SFTP server
Select this option if you want to use the Secure File Transfer Protocol (SFTP) to boot an image that is located on a different system. SFTP uses the Secure Shell (SSH) protocol to secure data. With this option, you need to supply a host name, user ID, password, and .INS file, as described for the **FTP server** boot option.

Hardware Management Console removable media
Select this option if you want to use an INS file from a media drive that is connected to the HMC. The media drive must be installed in the HMC when you save the partition definition and when the partition is started. Possible drive selections are **CD/DVD drive** or **USB flash memory drive**, depending on what media drives are installed in the HMC. If an option is displayed but is not selectable, an inline message or tool tip explains why the selection is disabled.

If the partition is configured to boot from a CD/DVD drive and the HMC that you are using does not have a CD/DVD drive installed, you might be required to change the drive selection.

- If the **CD/DVD drive** selection was configured on a different HMC that is still available for managing partitions and still has a CD/DVD drive installed, you do not have to change this boot option. In this case, you can continue to boot the partition from the other HMC. However, if you do change the boot option, you cannot reselect the **CD/DVD drive** selection through this HMC.
- If the **CD/DVD drive** selection was configured on the HMC that you are currently using, and this HMC no longer has a CD/DVD drive installed, you must change the boot option for this partition.

When you select this option:

1. If more than one type of media drive is available on the HMC, select the radio button for the media drive on which the INS file resides. Otherwise, skip to the next step.
2. Either enter the fully qualified name (relative to the mount point) of an INS file, or complete the following steps.
    a. Select **Browse** to start a search on the target media drive to retrieve a list of INS files. Any INS files found are displayed in a separate window.

b. Select only one INS file and click **OK** to close the Browse Removable Media window.

ISO image
Select this option when you want to upload an ISO file that is located on your workstation file system. This option is available only when you are connecting to the HMC through a remote browser.

When you select this option:

1. Select **Browse** to find the ISO image file on your workstation file system. You cannot select an ISO image from an HMC media drive. As soon as you select an ISO image file, DPM starts to upload the file, and displays a progress indicator for the upload operation.
2. After the upload operation completes, click **Browse** to search the ISO image file for the INS file that you want to use. Any INS files found are displayed in a separate window. Select only one INS file and click **OK** to close the Browse ISO Image window.

Boot loader time-out (60-600s)
The boot loader time-out setting determines the maximum amount of time for the load operation to complete. By default, the time-out setting has a value of 60 seconds. For only the **Network server (PXE)** boot option, the default time-out setting is 600 seconds, to account for network traffic. If the boot loader takes longer than the time-out value to load the hypervisor or operating system executables, DPM cancels the operation and issues an error message.

Confirm Disruptive Action Dialog

Use the **Confirm Disruptive Action** dialog to confirm that you want to make the changes that you specified in a section of the **Partition Details** task, even though this partition is not stopped.

This dialog is displayed for one of the following requests:

- A request to change the device number, virtual LAN (VLAN) ID, or media access control (MAC) address of one or more network interface cards (NICs).
- A request to change the device number of one or more host bus adapters (HBAs) or virtual functions (VFs).
- A request to change the adapter or adapter port of one or more NICs, HBAs, or VFs.
- A request to delete one or more NICs, HBAs, or VFs.
- A request to remove one or more crypto adapters, usage domains, or control domains.
- A request to change the current login or network settings for a Secure Service Container partition.

Depending on the type of requested changes, you might be required to type in confirmation text or enter your password. On the **Confirm Disruptive Action** dialog, complete the following steps.

1. Review the Changes table to verify the disruptive changes that you requested. This table contains the following columns:

   Name
   Contains one of the following values:

   - The name of a NIC, HBA, or VF
   - The name of a crypto adapter
   - The number of the usage domain or control domain
   - Reset Login for a change to the master user ID or password for a Secure Service Container partition
   - Reset Network for a change to the values for the Secure Service Container Web Interface Communication

   Type
   Contains one of the following values:

   - NIC
   - HBA

- VF
- Crypto Adapter
- Crypto Usage Domain
- Crypto Control Domain
- Secure Service Container

Change
Contains additional text to describe the requested disruptive change.

2. Review the Partition table to determine whether you must type a confirmation value. This table contains the following columns:

   Name
   The name of the partition for which you are requesting disruptive changes.

   System
   The system that is associated with this partition. The system name is a hyperlink through which you can open the **System Details** task.

   Status
   The current status of this partition.

   OS Name
   The operating system name that is associated with this partition.

   Confirmation Text
   This column is displayed only if you are required to type in confirmation that the action will disrupt a partition's operations. To confirm, type either the value in the Name column, or the value in the OS Name column, exactly as it is displayed in this table.
3. If you are required to enter a password, this display includes a text box in which you need to type the password associated with your user ID.
4. Click **Save** to save the changes that you have requested, or click **Cancel** to close the window without saving any changes.

Perform a Console Repair Action

Accessing the Perform a Console Repair Action task

Note: You cannot perform this task remotely.

This task should be the starting point for all Hardware Management Console repairs. You can either repair an open problem or report a repair of a non-detected problem.

To start a console repair action:

1. Open the **Perform a Console Repair Action** task. The Perform a Console Repair Action window is displayed.
   - To start a repair or continue a repair of a previously reported problem, select **Repair an open problem**.
   - To report about repairing a problem that was not detected or reported by Problem Analysis, select **Report a repair of a non-detected problem**.
2. Click **OK** to start the repair.

Perform a Console Repair Action

Use this window to either:

- Repair an open problem
- Resume a delayed repair

- Report the repair of a problem that was not detected or reported by Problem Analysis.

Use this window to select the type of repair action you want to perform:

Manage open problems
To repair an open problem, or to resume a delayed repair, select **Repair an open problem**.

Report a repair of a non-detected problem
To report information about repairing a problem that was not detected or reported by Problem Analysis, select **Report a repair of a non-detected problem**.

Additional functions on this window include:

OK
To continue the task after selecting the type of repair action you want to take, click **OK**.

Cancel
To close this window and cancel the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform a Console Repair Action (select a problem/select the work)

Use this window to select a problem to work on and to select the work you want to do.

Select a problem to work on from the "Problem Report table" on page 1250, then select a choice from the menu bar.

Click **Manage problems** on the menu bar to select the following:

- Repair Selected Problem to start a repair procedure for the selected problem.
- **Exit** to close this window and return to the previous window.

Click **View** on the menu bar to select the following:

- Problem Summary to display additional information that further describes the selected problem, and lists actions performed to diagnose and correct the problem.
- **Problem Analysis Panels** to display again the panels Problem Analysis displayed to report the selected problem when it occurred.
- **Refresh** to update the list with recently opened problems.

Click **Sort** on the menu bar then select the following:

- **By Number** to list problems by order of problem numbers, from the highest number to the lowest number.
- **By Date** to list problems in order of the dates on which they occurred, from the most recent problem to the least recent problem.
- **By Reference Code** to list problems by alphanumeric order of reference codes.
- **By Status** to list problems by order of their priority for repair. Delayed problems are listed first, followed by open problems, followed by any remaining problems.

Problem Report table

Problems to work on are listed in this table. Select a problem, then use the menu bar choices to select the work you want to do.

Number
Displays the problem number assigned by Problem Analysis when the problem was detected, and used to identify and track the problem.

Date and Time
Displays the date and time the problem occurred.

Reference Code
Identifies the specific error condition associated with the problem.

Status
Indicates whether the problem is open, delayed, or otherwise worked on.

Additional functions on this window include:

Close
Click **Close** on the menu bar then select the following:

- **Selected Problem** to change the status of the selected problem to closed.
- **All Problems** to change the status of all problems to closed.

Note: Closing a problem removes it from the list of problem reports.

Help
To display help for the current window, click **Help**.

Repair Selected Problem

This window displays the location and part number or parts that you may need to replace to repair the problem.

The window also identifies the printed documentation you need to use to repair the problem.

Location
Displays the physical location of the part in the hardware configuration of this Hardware Management Console.

Part number
Displays the Custom Card Identification Number (CCIN) of the part.

Make note of any field replaceable units listed to refer to when using the printed documentation.

Additional functions on this window include:

OK
To confirm you have completed using printed documentation to repair the problem, click **OK**.

Delay Repair
To close this window while you use printed documentation to repair the problem, click **Delay Repair**.

View Service Panels
To display again the panels Problem Analysis displayed to report the selected problem when it occurred, click **View Service Panels**.

Cancel
To close this window and cancel the repair, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Perform a Console Repair Action (identify outcome not reported to problem analysis)

Use this window to identify the outcome of work you performed to repair a problem that was not detected or reported by Problem Analysis.

Select whether or not parts were exchanged as a result of the repair, then click **OK**.

Parts were exchanged
To indicate you exchanged parts to repair the problem, select **Parts were exchanged**.

Note: At least one of the exchanged parts must be in the hardware configuration of this Hardware Management Console.

No parts were exchanged
To indicate you did not exchange parts to repair the problem, select **No parts were exchanged**.

Note: Select this choice also if you exchanged parts, but all exchanged parts were outside the hardware configuration of this Hardware Management Console.

Additional functions on this window include:

OK
To continue the task after you make a selection, click **OK**.

Cancel
To close this window and cancel the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform a Console Repair Action (identify outcome with documentation)

Use this window to identify the outcome of work you performed using printed documentation to repair a problem.

Problem number
Displays the number of the problem you are working on.

It is the number assigned by Problem Analysis when the problem was detected, and used to identify and track the problem.

Select one choice for the repair action, then click **OK**.

Parts were exchanged
To indicate you exchanged parts to repair the problem, select **Parts were exchanged**.

Note: At least one of the exchanged parts must be in the hardware configuration of this Hardware Management Console.

No parts were exchanged
To indicate you did not exchange parts to repair the problem, select **No parts were exchanged**.

Note: Select this choice also if you exchanged parts, but all exchanged parts were outside the hardware configuration of this Hardware Management Console.

A new problem was detected
To indicate a new problem occurred while you were repairing the current problem, select **A new problem was detected**.

The status of current problem will become delayed. Repair the new problem before resuming repair of the delayed problem.

Additional functions on this window include:

OK
To continue the task after you make a selection, click **OK**.

Cancel
To close this window and cancel the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform a Console Repair Action (select the parts exchanged)

Use this window to select the parts you exchanged to repair a problem.

The list displays parts included in the hardware configuration of this Hardware Management Console only. You do not need to identify exchanged parts that are not in this configuration.

Note: If none of the parts you exchanged are listed, then click **Cancel** to return to the previous window, and then select **No parts were exchanged** instead.

Select the parts exchanged, then click **OK**.

Location
Displays the physical location of the part in the hardware configuration of this Hardware Management Console.

Additional functions on this window include:

OK
To continue the task after selecting the parts that were exchanged, click **OK**.

Cancel
To close this window and cancel the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform a Console Repair Action (was original problem repaired)

Use this window to indicate whether the original problem was repaired by work you performed.

Problem number
Displays the number of the problem you are working on.

It is the number assigned by Problem Analysis when the problem was detected, and used to identify and track the problem.

Status
Select a status, then click **OK** to continue.

Problem is repaired
To indicate the problem no longer exists after completing repairs, select **Problem is repaired**.

Problem is not repaired
To indicate the problem still exists after completing work to repair it, select **Problem is not repaired**.

Additional functions on this window include:

OK
To continue the task after selecting a status, click **OK**.

Cancel
To close this window without choosing a status, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform a Console Repair Action (description of work performed)

Use this window to specify a description of the work you performed to repair a problem.

Additional functions on this window include:

OK
To continue the task after specifying a description of the repair action, click **OK**.

Reset
To clear the description input field and enter another description, click **Reset**.

Cancel
To close this window and cancel the description, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Summary

This window displays additional information that describes the selected problem.

System name
Displays the name of the object on which the problem occurred

Machine type
Displays the machine type of the object

Machine model
Displays the model number of the object

Machine serial number
Displays the serial number of the object.

Machine management hardware (PHM) number
Displays the number assigned to the problem by the support system

Additional functions on this window include:

OK
To continue the task after you complete this window, click **OK**.

Help
To display help for the current window, click **Help**.

Perform a Console Repair Action (new part exchanged during repair)

Use this window to specify the information about a new part exchanged during a repair.

Note: This is one window in a sequence of one or more exchanged parts.

To close all windows in the sequence, select **Next Part** until the last window displays, then click **OK**.

Location
Displays the physical location of the part in the hardware configuration of this Hardware Management Console.

Original data
Displays the data associated with the original part.

Data that is different for the new part
Specify the information for the part that replaced the removed part.

Serial number
Specify the serial number of the part that replaced the removed part.

Part number
Specify the Custom Card Identification Number (CCIN) of the part that replaced the removed part.

Engineering change (EC) number
Specify the EC number of the part that replaced the removed part.

Additional functions on this window include:

OK
To update the vital product data for this Hardware Management Console with information about each new part, click **OK**.

This is available only when the last exchanged part in the sequence displays. Otherwise, it is unavailable.

Previous Part
To display the previous part in the sequence of exchanged parts, click **Previous Part**.

This is not available when the first exchanged part displays.

Next Part
To display the next part in the sequence of exchanged parts, click **Next Part**.

This is not available when the last exchanged part displays.

Cancel
To close all windows in the sequence of exchanged parts, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform a Console Repair Action (location/part number of parts to repair problem)

This window displays the location and part number of parts that you may need to replace to repair the problem.

The window also recommends getting assistance from your support structure to repair the problem.

Record the field replaceable units
Make note of any field replaceable units listed to refer to when using the printed documentation.

Documentation
Displays the printed documentation you need to use to repair the problem.

Additional functions on this window include:

OK
To confirm you have completed using printed documentation to repair the problem, click **OK**.

Display Repair
To close this window while you repair the problem, click **Delay Repair**. The status of the problem becomes delayed.

View Service Panels
To display again the panels Problem Analysis displayed to report the selected problem when it occurred.

Cancel
To close this window and cancel the repair, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform a Console Repair Action (send information about repair action)

Use this window to select whether to send information about the repair action you completed and to select whether to request the support system close the Problem Management Hardware (PMH) number it assigned to the problem you repaired.

Transmitting the data sends the information you provided on previous windows, and machine information that identifies this Hardware Management Console.

The information is sent to the support system via the Remote Support Facility (RSF).

The options to close or not to close the Problem Management Hardware (PMH) number that was assigned to the problem you repaired are available only when you select to transmit the repair data. Otherwise, they are unavailable.

Transmit the data
To send information about the repair action, select **Transmit the data**.

Transmitting the data sends the information you provided on previous windows, and machine information that identifies this Hardware Management Console.

The options to close or not to close the PMH number become available when you select this choice.

Do not transmit the data
To not send information about the repair action, select **Do not transmit the data**.

Close PMH number
To request the support system close the PMH number, select **Close PMH number**.

Do not close PMH number
To not change the status of the PMH number in the support system, select **Do not close PMH number**.

Additional functions on this window include:

OK
To continue the task after making your selections, click **OK**.

Cancel
To close this window and cancel any choices, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform Model Conversion

Accessing the Perform Model Conversion task

Use this task to add, remove, or update system hardware and features. Some system configuration tasks support performing system upgrades and model conversions. Follow your normal order process for ordering an upgrade or model conversion for your system.

Note: When the power save mode is active some upgrade options are not available for the **Perform Model Conversion** task. See the **Set Power Saving** task.

To add, remove, or update system hardware and features:

1. Open the **Perform Model Conversion** task.

   The Perform Model Conversion window lists the upgrades and features for your system.
2. Select the perform model conversion option you want to work with.

Feature on Demand
Select this option to display information on all installed features on your system and information on the features contained in the staged record on the system. You can apply all the features contained in the staged record or permanently remove the staged record from the system.

Features
Select this option to add or remove available features on your system.

Perform Model Conversion

Use this window to add, remove or update system hardware and features.

Is it recommended that if new hardware is associated with the model upgrade then it should be installed prior to executing selections from this window. It is required that this function be initiated after Standby power-on. It is also recommended (but not required) that this function be initiated prior to system power on.

“Feature on Demand” on page 1257
Select an option to retrieve and apply or not apply FoD data from media, installed features, and features contained in the staged record on your system.

Retrieve and Apply FoD data from media
Select this option to retrieve and apply FoD data from media.

Retrieve FoD data but do not apply
Select this option to retrieve FoD data from media but do not apply.

Manage
Select an option to manage installed or staged record features on your system:

Installed
Displays information on all the installed features on your system.

Staged
Displays information on the features contained in the staged record on the system.

“Features” on page 1258
Select an option to add or remove available features on your system.

“Add a Feature” on page 1258
Select this option to install features to your system from a removable media device. To install the features on your system, insert the removable media device into your Support Element and select the media you are using to install the features.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

"Remove a Feature" on page 1259
Select this option to display all features available for your system and the option to remove installed features.

Additional functions on this window include:

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Processor Assignments Panel

Use this window to view the system processor assignments that are generated during the processing of the Prepare for Enhanced Processor Drawer Availability option. The processor values that are displayed from this window are the processor configuration utilized during the Perform Enhanced Processor Drawer Availability processing.

Use this table to view the physical processor assignments in your system.

Processor Type
Displays the physical processors assigned to the logical partitions logical processors

Dedicated Count
Displays the number of dedicated processors in each logical partition's logical processor assignment.

Non-Dedicated Count
Displays the number of non-dedicated processors in each logical partition's logical processors assignment

Processor Totals
Displays the total amount of physical processors installed in your system.

LICCC Count
Displays the number of processors which licensed internal code has been applied.

Additional functions on this window include:

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Feature on Demand

The window displays the installed features on the system and features contained in the staged record.

- Installed displays information on all the installed features on your system. Review the information under **Installed**. Optionally, use the table icons or **Select Action** from the table tool bar to permanently remove features from your system.
- Staged displays information on the features contained in the staged record on the system. Review the information under **Staged**. Optionally, click **Apply Record** to apply ALL the features contained in the staged record to the system or click **Remove Record** to permanently remove the staged record from the system.

Additional functions are available from this window:

Cancel
To close this window and exit this option, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installed

This page displays the current installed features on your system and an option to permanently remove any installed features.

You can work with the table by using the table icons or **Select Action** from the table tool bar.

Remove Feature
Removes the selected installed feature permanently from your system.

If you place your cursor over an icon, the icon description appears. The icons perform the following functions:

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

Staged

The page displays the features contained in the staged record and an option to apply ALL the features in the staged record or permanently remove the record from the system. There can only be one record staged at any given time.

Apply Record
To apply ALL the features contained in the staged record to the system, click **Apply Record**.

Remove Record
To permanently remove the staged feature from the system, click **Remove Record**.

Features

This option allows you to add or remove features installed and supported for your.

- “Add a Feature” on page 1258 displays a list of one or more features you can install on your system.
- “Remove a Feature” on page 1259 displays all features supported on your system and allows you to remove installed features.

Additional functions are available from this window:

Cancel
To close this window and exit this option, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add a Feature

This window allows you to select one or more of the features you want to install on your system that were on the removable media device. Select the one or more of the listed features you want to install then click **OK**.

OK
To perform the operation, click **OK**.

Cancel
To close the window without making a selection, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove a Feature

This window displays all features supported for your system and allows you to remove installed features on your system. The features currently installed on your system are indicated by "Currently Active" next to them. Select the one or more of the listed features you want to remove then click **OK**.

OK
To perform the operation, click **OK**.

Help
To display help for the current window, click **Help**.

Perform Problem Analysis

Accessing the Perform Problem Analysis task

This task manually calls Problem Analysis, which analyzes stored data that is collected from various parts of a processor at the time of an error and determines the type of problem. Problem Analysis then informs the user of the steps that are necessary to resolve the problem.

Problems that are considered to be *hard* errors start Problem Analysis automatically. An example of a hard error is a processor card failure. Results from automatic Problem Analysis are stored under **Hardware Messages**.

The icon of the CPC that had the hard error and the icon of any group that contains the CPC icon will have a blue background indicating that Problem Analysis results were reported for that CPC.

Problems that can be considered to be *soft* errors require the operator to start Problem Analysis manually, usually after the operating system reports a problem. An example of a soft error is an interface control check (IFCC).

To perform a manual problem analysis:

1. Select one or more CPCs (servers).
2. Open the **Perform Problem Analysis** task. The Problem Analysis window is displayed. This window displays the last 50 IFCCs that occurred.
3. You can select a specific problem, then click **View Selected Errors...**. The Problem Analysis window is displayed listing a description of the errors for the problem you previously selected.
4. You can continue to analyze the problems or click **Cancel** to return to the previous window.

Accessing the View Service History task

This task displays a list of current problems for selected CPCs or a selected group of CPCs. The problems may be opened or closed and will be displayed with the most recent entry at the top of the list.

To display the service history:

1. Select one or more CPCs (servers).
2. Open the **View Service History** task. The Service History window is displayed.
3. From the menu bar you can:
   - Select **View** for the following choices:

     Problem Summary
     Displays detailed information about the selected problem including machine type, model, and serial number information.

     Problem Analysis Panels
     Redisplays the Problem Analysis (PA) windows that were created when the selected problem was originally reported.

     Repair Information
     Displays repair information for the selected problem.

Exit
Ends the task.

- Select **Close** for the following choices:

  Selected Problem
  Changes the current status of the selected problem to closed.

  All Problems
  Changes the current status of all open problems to closed.

- Select **Sort** for the following choices:

  By Date
  Lists problems in the order of the dates on which problems occurred, starting with the most recent problem.

  By System Name
  Lists problems by the alphabetical order of the names of the objects on which they occurred.

  By Status
  Lists all open problems, followed by all closed problems.

- Select **Help** to display additional task information.

4. When you have completed this task, select **View**, **Exit** to return to the Hardware Management Console workplace.

Accessing the View Console Service History task

This task displays the service history log for the Hardware Management Console. The service history is a record of problems occurring on the Hardware Management Console. Service history information is recorded by *Problem Analysis* that starts automatically and identifies the source of a Hardware Management Console problem. Service history entries are displayed with the most recent entry at the top of the record.

To view the console service history:

1. Open the **View Console Service History** task. The View Console Service History window is displayed.
2. A table is displayed that lists the problems. Select a problem, then use the options from the menu bar for additional information or sorting preferences.
3. Click **View**, **Exit** from the menu bar when you have completed this task.

Service History

Use this window to review or close problems discovered by Problem Analysis, or reported using Problem Analysis, for one or more objects.

A problem is *opened* when either:

- Problem Analysis determines service is required to correct a problem detected by the object
- A console operator uses the **Report a Problem** task to report a suspected problem not detected by the object.

Each record of a problem includes detailed information about the problem, and indicates whether the service required to correct the problem is still pending (an *opened* problem), or is already completed or no longer needed (a *closed* problem).

Collectively, the problem and service records are referred to as the *service history* of the object. Upon viewing the object's service history, you can:

- Redisplay the Problem Analysis windows that were displayed when a problem was originally reported.
- Display detailed information about a problem.
- Manually close open problems.

Click **View** on the menu bar, then select the following:

- **Problem Summary...** to display additional information that further describes the selected problem and the object it occurred on, and lists actions performed to diagnose and correct the problem.
- **Problem Analysis Panels...** to display Problem Analysis panels that were shown to report the selected problem when it occurred.
- **Repair Information...** to display the repair information for the selected problem.
- **Exit** to end this task and return to the console workplace.

Click **Close** on the menu bar, then select the following:

- **Selected Problem** to change the status of selected *open* problems to *closed*.
- **All Problems** to change the status of all *open* problems to *closed*.

Click **Sort** on the menu bar, then select the following:

- **By Date** to list problems in order of the dates on which they occurred, from the most recent problem to the oldest problem.
- **By System Name** to list problems in alphabetical order of the names of the objects on which they occurred.
- **By Status** to list all *open* problems, followed by all *closed* problems.

Click **Help** to display help for the current window.

Service History table

This list displays the most recent problems that were automatically detected by Problem Analysis, or reported manually using Problem Analysis, for all selected objects.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

System name
Displays the name of the object on which the problem occurred.

Problem Number
Displays the number assigned by Problem Analysis and used to identify and track the problem.

Status
Indicates whether the problem is *open* or *closed*.

Description
Displays a brief explanation of the problem.

Service History Problem State

This window displays information that identifies an object, describes a specific problem that occurred on it, and lists actions performed to diagnose and correct the problem.

System name
Displays the name of the object on which the problem occurred.

Machine type
Displays the machine type of the object.

Machine model
Displays the model number of the object.

Machine serial number
Displays the serial number of the object.

Problem management hardware (PMH) number
Displays the number assigned to the problem by the support system.

Problem number
Displays the number assigned to the problem by Problem Analysis.

Problem type
Identifies the type of problem reported to the support system by Problem Analysis, and indicates the type of service required to correct it.

Problem data
Displays additional information provided by Problem Analysis specifically for this problem.

The information may be part numbers of parts needed to repair the problem, or reference codes needed to perform additional problem determination.

Problem State table

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

"Problem States" on page 1262
Displays the problem state of the object on which the problem occurred.

Problem States

Descriptions of the problem states or their effects on the problem:

Additional problem information
Indicates a service representative, while performing a repair procedure, manually edited the service history log to further describe the problem or its repair.

Continued in printed information
Indicates a repair procedure instructed a service representative to continue the repair using a printed repair procedure.

Customer notified
Indicates Problem Analysis displayed a panel to report the problem.

Duplicate problem closed
Indicates Problem Analysis closed the problem because it was a duplicate of another open problem.

Inactive problem closed
Indicates Service History closed the problem because of inactivity.

Problem closed
Indicates Problem Analysis could no longer detect the problem after a service representative completed a repair procedure.

Problem closed by the user
Indicates the console operator used the Service History task to close the problem.

Problem detected
Indicates Problem Analysis detected the problem automatically.

Problem reopened
Indicates Problem Analysis detected the problem occurred again after it was repaired and closed.

Repair closed
Indicates a problem was closed when the repair was completed.

Repair ended
Indicates a service representative completed a repair procedure.

Repair resumed
Indicates a service representative started using a previously suspended repair procedure.

Repair started
Indicates a service representative began a repair procedure.

Repair suspended
Indicates a service representative temporarily stopped using a repair procedure before completing the repair.

Returned from printed information
Indicates a service representative resumed using a repair procedure to acknowledge completing a printed repair procedure.

Service authorization complete
Indicates Problem Analysis successfully transmitted problem information and requested service through a Remote Support Facility (RSF) connection to the support system.

Service authorization delayed
Indicates Problem Analysis reported the problem, but the console operator did not request service.

Service authorization failed
Indicates Problem Analysis could not successfully transmit problem information or request service through a Remote Support Facility (RSF) connection to the support system.

Service authorized electronically
Indicates Problem Analysis used the Remote Support Facility (RSF) to connect to the support system to transmit problem information and request service.

Service requested via telephone
Indicates Problem Analysis displayed problem information and instructed the console operator to call a service representative, describe the problem, and request service.

Additional functions are available from this window:

OK

To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Service History Part Replacement

This window displays part replacement information including part descriptions as well as how many parts were replaced.

Part Location
Displays the machine location of the object on which the problem occurred.

Part Number
Displays the actual part number of the object.

Serial Number
Displays the serial number of the object.

Fix description
The description from Service History of how to correct the problem.

OK

to return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem description)

This window displays the following information about a problem discovered by automatic Problem Analysis:

System name
Displays the name of the object on which the problem occurred.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

Depending on the information that was provided for a problem, the following information could also appear in this window:

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the Interface Control Code (IFCC) occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Use the following information to determine whether to request service, then take the appropriate action:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Impact of Repair
Describes what system resources will be affected.

Additional functions are available from this window:

Request Service...
To request service to correct the problem, click **Request Service...**.

I/O Trace...
To display Input/Output (I/O) trace information, click **I/O Trace...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Display Sense Data
To display additional specific problem failure information, click **Display Sense Data**.

Detail Problem Description...
To view a more detailed description of the problem, click **Detail Problem Description...**.

Delete
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Tag-in control lines

This field displays a two-digit, hexadecimal value that identifies the inbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-in is active.
- The value for a bit is 0 when its tag-in is not active.

Bit	Tag-In
0	Operational
1	Address
2	Status
3	Select
4	Request
5	Service or Data (see Note)
6	Data or Mark (see Note)
7	Disconnect

Note: The values for bits 5 and 6 indicate whether the following tags-in are active:

```
Bit 5    Bit 6          Data In       Service       Mark
-----    -----          -------       -------       ----
 1        1              On            Off           Off
 1        0              Off           On            Off
 0        1              Off           Off           On
 0        0              Off           Off           Off
```

For example, a tag-in value of 86 indicates that Operational In and Data In are both active.

Tag-out control lines

This field displays a two-digit, hexadecimal value that identifies the outbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.

- The value for a bit is 1 when its tag-out is active.
- The value for a bit is 0 when its tag-out is not active.

Bit	Tag-In
0	Operational
1	Address
2	Select/Hold
3	Data streaming
4	Service
5	Data
6	Suppress
7	Command

For example, a tag-out value of 84 indicates that Operational Out and Data Out are both active.

Problem Analysis (sense data details)

This window displays sense data details and additional problem failure information.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (operation/outcome)

This window displays information about an automatic Problem Analysis operation on an object. The information identifies the operation and describes its outcome.

Review the information, then take the appropriate action.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information)

This window displays information about a problem discovered by automatic Problem Analysis.

Use the information provided to determine whether to request service, then take the appropriate action.

System name
Displays the name of the object that had the channel path configured on when the IFCC occurred.

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the IFCC occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Additional functions are available from this window:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Request Service...
To request service to correct the problem, click **Request Service...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (contact)

Use this window to identify a person that can be contacted about the problem, and to specify how to service will be requested.

Provide the following information, then click **Request Service...**:

Customer name
Specify the name of the person that can be contacted about the problem.

Customer phone
Specify the telephone number of the person that can be contacted about the problem.

Transmission Type
Select how to request service, through automatic transmission or manually by telephone.

Select a transmission type, then click **Request Service...**.

Electronic transmission
To automatically transmit the service request and problem information, select **Electronic transmission**.

Voice transmission
To manually request service and report problem information by telephone, select **Voice transmission**.

Note: The telephone number and problem information are provided on a subsequent window.

Additional functions are available from this window:

Request Service...
To authorize service for this problem and initiate the transmission type by electronic or by voice, select click **Request Service...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information/contact)

This window displays information about a problem discovered by automatic Problem Analysis. Use this information to request service and describe the problem.

1. Be ready to provide the problem information when you call.
2. Dial the telephone number to speak with a service representative.
3. Request service.
4. Provide the problem information to the service representative.

Request service when:

- Service is required.
- Service may be required, and you have verified all possible causes of the problem do not exist.

It is recommended you do not request service when:

- Service is not required.
- Service may be required, but you have verified one or more possible causes of the problem exist, and you will attempt to correct the problem.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (action to take)

This window displays information about a problem discovered by automatic Problem Analysis.

Review the information, then take the appropriate action.

Problem Data
Provides specific information about the selected problem.

Parts List

- Part Location - the physical location of the part.
- Part Number - the number of the part.
- Fix Percentage - the percentage of accuracy for correcting the problem.
- Serial Number - the serial number of the part.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (channel path errors)

This window displays the unreported errors that occurred on a specific channel path of a Central Processor Complex (CPC).

Use this window to select an error when you want to display detailed information from Problem Analysis that describes the error.

Select one error from the list, then click **Analyze Error...** to display details about the error.

System name
Displays the name of the CPC that had the channel path configured on when the error occurred.

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Interface location
Identifies the physical location of the channel card and port that supports the channel path on which the error occurred.

Additional functions are available from this window:

Error table

Date
Displays the date the error occurred.

Time
Displays the time the error occurred.

Description
Displays a brief description of the error.

Analyze Error...
Select an error from the list, then click **Analyze Error...** to display details about the selected error.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (unreported errors)

This window summarizes the unreported errors that occurred on the selected Central Processor Complexes (CPCs). The summary identifies the problem areas where errors occurred, and displays the number of errors that occurred in each area.

Use this window to select a problem area when you want to display more information about the unreported errors that occurred in the area.

Problem areas for a CPC include the processors and its channels paths.

An unreported error is an error that is analyzed, but is not reported by Problem Analysis. Errors are not reported when automatic recovery operations succeed, and when service is not needed for the CPC to continue operating.

Select a problem area for a CPC from the list, then click **View Selected Errors...** to display a summary of unreported errors that occurred in that area.

Beginning time
Displays the time and date when the least recent unreported error occurred.

All unreported errors occurred at or after this time.

Ending time
Displays the time and date when the most recent unreported error occurred.

All unreported errors occurred before or at this time.

Error table

System Name
Displays the name of the CPC where the unreported errors occurred.

Problem Area
Indicates whether the unreported errors occurred on a processor in the CPC, or on a particular channel path.

Number of Errors
Indicates the number of unreported errors that occurred in the problem area during the time range.

View All Errors...
To view details about all errors shown in the list, click **View All Errors...**.

View Selected Errors...
To view details about one error in the list, click **View Selected Errors...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Perform Transfer Rate Test

Accessing the Perform Transfer Rate Test task

This task decides whether you want to perform the transfer rate test for a selected object to the primary Support Element or to the alternate Support Element.

To perform the transfer rate test:

1. Select a CPC (server).
2. Open the **Perform Transfer Rate Test** task. The Perform Transfer Rate Test message window is displayed.
3. Click **Primary** to test against the primary Support Element or click **Alternate** to test against the alternate Support Element.
4. Click **Cancel** to exit the task without performing the transfer rate test.

Power Off or Restart

Accessing the Power Off or Restart task

This task enables you to restart the application, restart the console, or power off the console if you are accessing the Hardware Management Console locally. If you are accessing the Hardware Management Console remotely, you can only restart the console if the **Remote restart or power off** service is enabled from the **Customize Console Services** task (see "Remote Power Off Setup and Execution for the HMC, SE, and HMA" on page 1272).

To power off or restart the console:

1. Open the **Power Off or Restart** task. The Power Off or Restart window is displayed.
2. You can select one of the following:
   - Restart application
   - Restart HMC console
   - Power off HMC console
   - Block HMC console power off and restart requests
3. Click **OK** to perform the selected action or click **Cancel** to return to the Hardware Management Console workplace.

   Note: If there are other users and tasks running, an additional message is displayed allowing you to send a message (initiates the **Console Messenger** task) to alert the user sessions that you intend to shutdown or restart the console.

Power Off or Restart

This window allows you to restart the application, restart the console, or power off the console if you are accessing the console locally.

If you are accessing the console remotely, you can only restart the console if the **Remote restart or power off** service was enabled from the **Customize Console Services** task (see "Remote Power Off Setup and Execution for the HMC, SE, and HMA" on page 1272).

Note: If this task cannot immediately perform the action that you have selected, a notification appears in a message window. You can wait for your action to complete or click **Cancel** in the message window to exit this task.

Restart application
To close the console and restart the application, select **Restart application**.

This option is only available if you are accessing the console locally.

Restart HMC console
To close the console and restart the console, select **Restart HMC console**.

This option is available if you are accessing the console locally or remotely. If you are accessing the console remotely the **Remote restart or power off** service must be enabled from the **Customize Console Services** task.

Power off HMC console
To close the console and power off the hardware, select **Power off HMC console**.

This option is only available if you are accessing the console locally.

Block HMC console power off or restart requests
To block requests for powering off or restarting the console, select **Block HMC power off or restart requests**.

Note: This option is only available if you have a SERVICE user ID or a user ID that is assigned service roles.

OK
To proceed with your selection, click **OK**.

The **Power Off or Restart** confirmation window is displayed. This window indicates the users and tasks that are currently accessing this console. If there are no users or tasks running, you can either:

- Click **Yes** to proceed with the power off or restart, or
- Click **No** to exit the task and not perform the power off or restart.

However, if there are users and tasks running you have the additional option of sending and alerting those user sessions a message that you intend to power off or restart the console. You can click **Console Messenger** to initiate the **Console Messenger** task.

Cancel
To exit this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remote Power Off Setup and Execution for the HMC, SE, and HMA

To enable remote power off at the Hardware Management Console (HMC), Support Element (SE), or Hardware Management Appliance (HMA), use the following steps for each console. Note, each console setup must be done locally and before remote power off is required. Users that have been assigned system programmer or service roles can perform these steps for remote users.

Remote power off setup

- For the HMC:
  1. Log in locally at the HMC, then open the **Customized Console Services** task. The Customize Console Services window is displayed.
  2. On the **Remote power off or restart** option, click **Change...**. The Change Remote Power Off and Restart Settings window is displayed.
  3. To enable the HMC to be powered off or restarted remotely, select **Power off and restart**, then click **OK**.
- For the SE:
  1. Log in locally at the Primary SE, then open the **Customized Console Services** task. The Customize Console Services window is displayed.
  2. On the **Remote power off or restart** option, click **Change...**. The Change Remote Power Off and Restart Settings window is displayed.

3. To enable the SE to be powered off or restarted remotely, select **Power off and restart**, then click **OK**.

- For the HMA, you need to configure both the HMC and SE settings locally at the HMA.
  - For the HMC:
    1. Log in locally at the HMC on each HMA, then open the **Customized Console Services** task. The Customize Console Services window is displayed.
    2. On the **Remote power off or restart** option, click **Change...**. The Change Remote Power Off and Restart Settings window is displayed.
    3. To enable the HMC to be powered off or restarted remotely, select **Power off and restart**, then click **OK**.
  - For the SE:
    1. Log in locally to the Primary SE on the HMA. Use the key sequence of right-click from the desktop to get flux box menu, then select **SE Console**. Single Object Operation cannot be used.
    2. When you are logged in to the SE, open the **Customize Console Services** task. The Customize Console Services window is displayed.
    3. On the **Remote power off or restart** option, click **Change...**. The Change Remote Power Off and Restart Settings window is displayed.
    4. To enable the SE to be powered off or restarted remotely, select **Power off and restart**, then click **OK**.

Remote power off execution

Once the consoles have been enabled to power off remotely, use the following steps to power off the HMC, SE, and HMA when it is required.

- For the HMC:
  1. Use a remote browser to log in to the HMC, then open the **Power Off or Restart** task. The Power off or Restart window is displayed.
  2. To power off the console, select **Power off HMC console**, then click **OK.**
- For the SE:
  1. Use a remote browser to log in to the HMC. Open the **Single Object Operation** task, select an SE, then click **OK**.
  2. Open the **Power Off or Restart** task. The Power off or Restart window is displayed.
  3. To power off the console, select **Power off SE console** and **Power Off both the primary and alternate SEs**, then click **OK.**
- For the HMA, you must first shut down the console on the SE. Then, power off the console for the HMC.

  Note: It must be done in that order.

  1. For the SE:
     a. Use a remote browser to log in to the HMC, which is on the HMA with the primary SE.
        1) Open the **Single Object Operation** task, select an SE, then click **OK**.
        2) Open the **Power Off or Restart** task. The Power off or Restart window is displayed.
        3) To power off the console, select **Power off SE console** and **Power Off both the primary and alternate SEs**, then click **OK.**

           Note: This cleanly shuts down both the Primary and Alternate SEs on both HMAs.
  2. For the HMC:
     a. Use a remote browser to log in to the HMC, which is on the HMA.
     b. Open the **Power Off or Restart** task. The Power off or Restart window is displayed.

c. To power off the console, select **Power off HMC console**, then click **OK.**

Note: Repeat the previous steps for the HMC on the second HMA.

Product Support Directed Changes

Accessing the Product Support Directed Changes task

Notes:

- You cannot perform this task remotely.
- Product Support Directed Changes is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task enables the service representative to receive temporary licensed internal code fixes when no formal changes are available. This task should be used only when product support directs you to do so. The following selections are available from the menu:

To receive temporary licensed internal code fixes:

1. Select one or more CPCs (servers).
2. Open the **Product Support Directed Changes** task. The Product Support Directed Changes window is displayed.
3. Select one of the following options:

   Retrieve all temporary internal code fixes
   Use this selection to retrieve an internal code fix from removable media. The fix is then stored on the Support Elements for the selected CPCs. The fix is also stored in a staging area on the Hardware Management Console hard drive.

   Note: A set of fixes is stored in the Hardware Management Console fixed drive staging area during a retrieve. This set of fixes is available there for other CPCs until a different set of fixes is retrieved. The fixes may also be placed in the staging area from a remote console.

   Activate all temporary internal code fixes
   Use this selection to replace the system's existing internal code with the retrieved internal code fixes when the system is activated. This changes the status on the Support Element Analyze Internal Code Changes window.

   Deactivate and delete all temporary internal code fixes
   Use this selection when a previously activated internal code fix is **not** to be used as a part of a CPC's internal code the next time the system is activated. This changes the status on the Support Element Analyze Internal Code Changes window.
4. Click **OK** to continue with the task or click **Cancel** to return to the Hardware Management Console workplace.

Product Support Directed Changes

Use this window to select an option for using Product Support directed management of temporary fixes to the system licensed internal code on selected Central Processor Complexes (CPCs).

Licensed internal code controls many of the operations available on the system and Support Element. Temporary internal code fixes may provide new operations, or correct or improve existing operations until a permanent internal code change is available.

Manage temporary internal code fixes options

Retrieve all temporary internal code fixes
To copy all internal code fixes from the source supplied by the support system to the staging area on the Hardware Management Console and the Support Element hard drive on selected CPCs.

To retrieve an internal code fix from either a removable media (USB flash memory drive) or a staging area on the Hardware Management Console fixed drive, select **Retrieve all temporary internal code fixes**. The fix is then stored on the support elements for the selected CPCs. If retrieved from removable media the fix is also stored in a staging area on the Hardware Management Console hard drive.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Activate all temporary internal code fixes

To place temporary fixes into an active state, or prepare the fix for activation, depending on the code affected by the fix.

To replace the system's existing internal code with the retrieved internal code fixes when the system is activated, select **Activate all temporary internal code fixes**. This changes the status on the Support Element Manage Internal Code Fixes window to **ACT** if no syntax errors are found or **ERR** if errors are found.

Deactivate and delete all temporary internal code fixes

To make all temporary internal code fixes changes not operational and erase them from the selected CPC hard drives or prepare the fix to be made not operational, depending on the code affected by the fix.

When a previously activated internal code fix is **not** to be used as a part of a CPC's internal code the next time the system is activated, select **Deactivate and delete all temporary internal code fixes**. This changes the status on the Support Element Manage Internal Code Fixes window to **PEND** until the system is activated again. After activation, internal code fixes are deleted from the Manage Internal Code Fixes window.

Note: A support system will provide all temporary internal code fixes and manage their use. For internal code changes already stored on the Support Element hard disk, manage these changes only under the supervision of a service representative or with the assistance of the support system.

Additional functions are available from this window:

OK

To continue the task with your selection, click **OK**.

Cancel

To cancel your request to manage temporary internal code fixes and close the window, click **Cancel**.

Help

To display help for the current window, click **Help**.

Confirm the Action - Retrieve

Use this window to confirm or cancel your request to retrieve temporary internal code fixes for the Central Processor Complexes (CPCs) listed.

Attention: Once the retrieval process is started, it cannot be stopped.

Retrieve

To confirm your request to retrieve internal code fixes, click **Retrieve**.

Cancel

To cancel your request to retrieve internal code fixes and return to the previous window, click **Cancel**.

Help

To display help for the current window, click **Help**.

Confirm the Action - Activate

Use this window to confirm or cancel your request to activate temporary internal code fixes for the Central Processor Complexes (CPCs) listed.

Activate
To confirm your request to activate internal code fixes, click **Activate**.

Cancel
To cancel your request to activate internal fixes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action - Deactivate and Delete

Use this window to confirm or cancel your request to deactivate and delete temporary internal code fixes for the Central Processor Complexes (CPCs) listed.

Attention: Deleting retrieved internal code fixes erases them from the Support Element hard disk.

Deactivate and Delete
To confirm your request to deactivate and delete internal code fixes, click **Deactivate and Delete**.

Cancel
To cancel your request to deactivate and delete internal code changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Retrieve All Temporary Internal Code Fixes

Use this window to copy temporary internal code fixes from the selected source to the Hardware Management Console staging area and to the Support Element hard drive on selected Central Processor Complexes (CPCs).

At least one of the following sources will be available for retrieving temporary internal code fixes:

- Retrieve internal code fixes from removable media
- Retrieve internal code fixes from the staging area.

Retrieving internal changes only copies them from the source to selected Support Element hard disks. Retrieved internal code fixes do not affect the operation of a system until they are activated.

Retrieve all temporary internal code fixes from removable media
When the temporary internal code fixes have been delivered on a USB flash memory drive, select **Retrieve all temporary internal code fixes from removable media**.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

Retrieve all temporary internal code fixes from the staging area
To copy temporary internal code fixes that are stored in the Hardware Management Console staging area to the hard drive on selected CPCs, select **Retrieve all temporary internal code fixes from the staging area**.

OK
To continue the task with your selection, click **OK**.

Cancel
To cancel your request to retrieve all temporary internal codes fixes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

PSW Restart

Accessing the PSW Restart task

Note: PSW Restart is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task performs a restart operation on the first available central processor(s) of the selected CPC images (except for a coupling facility image).

A restart interruption will store the current program status word (PSW) at real address 8 and fetch a new PSW from real address 0 in central storage.

PSW Restart can be used when the status of the selected object is:

- Operating
- Stopped

To restart a processor:

1. Select a CPC image.
2. Open the **PSW Restart** task. The PSW Restart Task Confirmation window is displayed.
3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
4. To continue with the restart, click **Yes**. The PSW Restart Progress window is displayed indicating the progress of the restart and the outcome.
5. Click **OK** to close the message when the restart completes successfully.

   Otherwise, if the restart does not complete successfully, follow the directions in the message to determine the problem and how to correct it.

Query Channel Crypto/Configure Off/On Pending

Accessing the Query Channel/Crypto Configure Off/On Pending task

Use this task to select a condition to either:

- Query channel/cryptos currently requiring a configure off/on action in order to perform a code load.
- Query channel/cryptos that will require a configure off/on action after the next install and activate of a channel/crypto in order to perform a code load.

To query channel/cryptos that are configure off/on pending:

1. Locate the **CPC** to work with.
2. Open the **Query Channel/Crypto Configure Off/On Pending** task.

   The Query Channel/Crypto Configure Off/On Pending window displays.
3. Click **Current conditions** to display a list of channel/cryptos that have configure off/on current conditions pending.
4. Click **Conditions in the next Inst/Act** to display a list of channel/cryptos that have configure off/on conditions pending in the next nondisruptive code load.
5. Click **OK** to return to the previous window.

Query Channel/Crypto Configure Off/On Pending

Use this window to select a condition to either:

- Query channel/cryptos currently requiring a configure off/on action in order to perform a code load

- Query channel/cryptos that will require a configure off/on action after the next install and activate of a channel/crypto in order to perform a code load.

Current conditions
To display a list of channel/cryptos that are currently pending a configure off/on action to perform a nondisruptive channel or crypto code load, click **Current conditions**.

Conditions in the next Inst/Act
To display a list of channel/cryptos that will require a configure off/on action in the next nondisruptive code load, click **Conditions in the next Inst/Act**.

Cancel
To close the window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Query Channel/Crypto Configure Off/On Pending -- current

Use this window to review a list of channel paths and/or cryptos with an assigned physical channel identifier (PCHID) that are currently pending a configure off/on action in order to complete a nondisruptive channel and/or crypto code load.

Channel/Crypto Information
The table lists the following information for the current active channels/cryptos that are pending a configure off/on action in order to perform a code load.

PCHID
Displays the four-digit physical channel identifier of each channel path or crypto.

CSS.CHPID or Crypto number
Displays a single-digit number that identifies the channel subsystem followed by a two-digit number that is a channel path identifier of each channel path, and the crypto number displays the number assigned to the Crypto X2.

Active EC/MCL
Displays the current active code in the PCHID.

Pending EC/MCL
Displays the pending code to be loaded into the PCHID after a configure off/on.

PCHID Type
Displays the channel or crypto type for the assigned PCHID.

CHPID or Crypto Type
Displays the CHPID type for the CSS.CHPID, and displays the crypto type for the crypto number.

OK
To close the window and return to the previous window, click **OK**

Cancel
To close the window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Query Channel/Crypto Configure Off/On Pending -- in the next Install/Activate

Use this window to review a list of active channel paths and/or cryptos with an assigned physical channel identifier (PCHID) that will be pending a configure off/on action in the next install and activate of a nondisruptive channel/crypto code load.

Channel/Crypto Information
The table lists the following information for the current active channels/cryptos that will be pending a configure off/on action to perform a code load.

PCHID
Displays the four-digit physical channel identifier of each channel path or crypto.

CSS.CHPID or Crypto number
Displays a single-digit number that identifies the channel subsystem followed by a two-digit number that is a channel path identifier of each channel path and the logical partition name, and the crypto number displays the number assigned to the Crypto X2.

PCHID Type
Displays the channel or crypto type for the assigned PCHID.

CHPID or Crypto Type
Displays the CHPID type for the CSS.CHPID, and displays the crypto type for the crypto number.

OK
To close the window and return to the previous window, click **OK**.

Cancel
To close the window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Query Coupling Facility Reactivations

Accessing the Query Coupling Facility Reactivations task

This task allows you to query what coupling facility current code level changes need to be deactivated and then reactivated in order to be applied to your CPC.

To query coupling facility reactivation:

1. Locate the **CPC** to work with.
2. Open the **Query Coupling Facility Reactivations** task.

   The Query Coupling Facility Reactivations window displays.
3. Review the list of coupling facility code level change to be reactivated.
4. Click **OK** to exit the window.

Reassign Hardware Management Console

Accessing the Reassign Hardware Management Console task

Note: You cannot perform this task remotely.

This task allows you to reassociate the Hardware Management Console with a different CPC. You will need to acquire the appropriate reassignment media from the support system prior to starting this task.

Reassign Hardware Management Console

Use this window to reassociate the Hardware Management Console with a different CPC. Appropriate reassignment media must be obtained from the support system before this operation can be performed.

You are prompted to insert the media into the console. The media is verified and if correct, the Vital Product Data (VPD) files are updated appropriately. The VPD is then transmitted to the support system and you are instructed to remove the media. A message is displayed indicating the success or failure of the operation.

OK
To continue with your request to reassociate the Hardware Management Console, click **OK**.

Cancel
To cancel your request to reassociate the Hardware Management Console and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Reassign I/O Path

Accessing the Reassign I/O Path task

Reassign is an I/O operation you can use to perform, at once, all the following steps necessary to reassign a reconfigurable input/output (I/O) path from its owning logical partition to another logical partition:

To reassign an I/O path:

1. Select a CPC (server).
2. Open the **Reassign I/O Path** task, the Reassign I/O Path window is displayed.
3. From the list, select the I/O path identifier that you want to reassign, then click **OK**. The Select a Partition window is displayed showing the ID and PCHID that is currently assigned, the owning partition, and a list of logical partitions from which you can select to reassign the I/O path.
4. Select the logical partition in the **Target Partition** list to which you want the I/O path reassigned, then click **OK**. The Confirm the Action window is displayed.
5. Click **OK** to confirm your request to reassign the selected I/O path to the target logical partition.

   Note: You may receive an additional warning that the I/O path will be released for reassignment if:

   - The partition isolation parameter is enabled.
   - The partition isolation parameter is disabled, but the logical partition to be reassigned was previously configured offline while the partition isolation parameter was enabled.

   Click **OK** to confirm the action.
6. After the I/O path is reassigned, click **OK** to close the window.

Reassign I/O Path

Use this window to select the logical partition to which you want to reassign the selected input/output (I/O) path.

Note: You can reassign only one I/O path at a time. If you have targeted more than one CPC (server) as you open this task, the Object Selection window is displayed. You can select an object name from the list, then click **OK**.

The logical partition to which the I/O path is currently assigned is referred to as the *owning logical partition*. The logical partition to which you want to reassign the I/O path is referred to as the *target logical partition*.

Reassigning an I/O path includes:

1. Configuring off the I/O path from the owning logical partition, if the I/O path is currently configured on.
2. Releasing the I/O path from the owning logical partition, if the I/O path is currently isolated.
3. Configuring the I/O path on to the target logical partition, if activated.

   Note: If the target logical partition is not activated, the I/O path is still configured on, but its status does not immediately become **Online**. The status does not remain **Standby**. It will be Online Pending and will go to **Online** when the logical partition is activated.

Identifier (ID) table

This table lists the I/O paths that can be reassigned including the following information:

ID

This can display a two-digit number followed by a decimal followed by a two-digit number. The number before the decimal is the Channel Subsystem (CSS) number and the number after the decimal is the CHPID number of the I/O path that will be reassigned.

This can also display a four-digit number that represents a function identifier (FID) for the channel.

PCHID
Displays a four-digit physical channel identifier (PCHID) of the channel.

Owner
Displays the name of the logical partition to which the channel path is currently assigned.

State
Displays **Online** when the target logical partition is activated, displays **Online Pending** until the target logical partition is activated, or displays **Standby** if the target logical partition is not activated.

Type
Specifies the name of the device.

OK
To reassign the selected I/O path to another logical partition, click **OK**.

Refresh
To discard the selections you made to the Reassign I/O Path window and display again the selections that displayed when you opened this task, click **Refresh**.

Cancel
To close this window without reassigning the I/O path, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select a Partition

Use this window to select a partition to which the I/O path should be reassigned.

Identifier (ID)
Displays a two-digit number followed by a decimal followed by a two-digit number. The number before the decimal is the Channel Subsystem (CSS) number. The number after the decimal is the CHPID number of the I/O path that will be reassigned. It can also display a four-digit number that is the function identifier (FID).

Physical channel identifier (PCHID)
Displays a four-digit physical channel identifier (PCHID) of the channel.

Owning partition
Displays the name of the logical partition to which the I/O path is currently assigned.

Target partition
Displays the name of the logical partition to which the I/O path will be reassigned.

OK
To reassign the selected I/O path to another logical partition, click **OK**.

Cancel
To close this window without reassigning the I/O path, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action

Use this window to confirm or cancel your request to reassign the selected I/O path from the owning logical partition to the target logical partition.

Review the information in the fields, then make a selection.

Identifier
Displays a two-digit number followed by a decimal followed by a two-digit number. The number before the decimal is the Channel Subsystem (CSS) number. The number after the decimal is the CHPID number of the I/O path that will be reassigned. It can also display a four-digit number that is the function identifier (FID).

Physical channel identifier (PCHID)
Displays a four-digit physical channel identifier (PCHID) of the channel that will be reassigned.

Owning partition
Displays the name of the logical partition to which the I/O path is currently assigned.

Target partition
Displays the name of the logical partition to which the I/O path will be reassigned.

OK
To confirm your request to reassign the I/O path from the owning logical partition to the target logical partition, click **OK**.

Cancel
To cancel your request and close this window without reassigning the I/O path, click **Cancel**.

Help
To display help for the current window, click **Help**.

Reboot Support Element

Accessing the Reboot Support Element task

This task allows you to reboot the Support Element of the selected server (CPC) without logging on at the actual Support Element console. Use this task if you are currently operating from a remote location and the Support Element is not easily accessible. An example of when you would want to reboot the Support Element from the Hardware Management Console is after a change has been made to the TCP/IP configuration of the Support Element.

To reboot the Support Element:

1. Select one or more CPCs (servers).
2. Open the **Reboot Support Element** task. The Reboot Support Element Task Confirmation window is displayed.
3. Click **Yes** to continue with this task, or click **No** to exit the task.

Rebuild Vital Product Data

Accessing the Rebuild Vital Product Data task

Note: Do not rebuild the Vital Product Data unless you have been directed by product support.

This task forces a rebuild of the Vital Product Data on the Hardware Management Console. Before a rebuild is done, the current version will be saved.

To rebuild the vital product data:

1. Open the **Rebuild Vital Product Data** task. The Rebuild Vital Product Data window is displayed.
2. **Click OK** to continue with this task.
3. After the vital product data is rebuilt, a message displays that the rebuild was successful.
4. Click **OK** to complete the task.

   Note: If a failure occurs, an error will be logged in the default system log.

Rebuild Vital Product Data

Do not rebuild the Vital Product Data (VPD) unless you have been directed by product support to do so.

The VPD for a Hardware Management Console contains the following data:

- The location, part number, and serial number of the console
- The locations, part numbers, and serial numbers of the installed parts and features

- Installed Engineering Changes (ECs)
- The level of licensed internal code.

If the rebuild of the VPD fails, the backup VPD data file (iqyvpd2b.dat) is not restored.

OK
To continue with your request to rebuild Vital Product Data, click **OK**.

Cancel
To cancel your request to rebuild Vital Product Data, click **Cancel**.

Help
To display help for the current window, click **Help**.

Redundant I/O Interconnect Status and Control

Accessing the Redundant I/O (RIO) Interconnect Status and Control task

This task allows you to check the state and status of the Redundant I/O (RIO) multiport and chain links for the InfiniBand and PCIe channel types. An option is also available to display details and search a specific PCHID/CSS.CHPID controlled by the selected channel.

To check RIO multiport status:

1. Locate the **CPC** to work with.
2. Open the **Redundant I/O Interconnect Status and Control** task.

   The Redundant I/O Interconnect Status and Control window displays.
3. Click **Display PCHID/CSS.CHPID** to display details for both sides of the RIO multiport.
4. Click **Search PCHID/CSS.CHPID** to search for a specific PCHID/CSS.CHPID.
5. Click **Cancel** to close the window.

Redundant I/O Interconnect Status and Control

Use this window to display the state and status of the Redundant I/O Interconnect (RIO) multiport and chain links. You can display details of a selected RIO multiport and associated PCHID/CSS.CHPID(s) controlled by that RIO multiport. A search option is available to locate a RIO multiport associated with specific PCHID/CSS.CHPID.

Redundant I/O Interconnect Status and Control table
The table displays information on specific RIO multiport and associated PCHID/CSS.CHPID.

Attention
Displays "> > >" when a status of something on the multiport link is not normal.

PBU Link 1 to Fanout Status-Speed-Width
Displays the PBU Link 1 fanout status-speed-width.

Fanout Link 1 to IO Status-Speed-Width
Displays the fanout Link 1 location to IO status-speed-width.

Multiport Link 1 Cage-Slot-Jack
Displays the location of the cage, slot, and jack location of the multiport link 1.

Multiport Link 1 I/O Cage-Slot
Displays the location of the cage, slot, and jack location of the multiport link 1.

Chain Link Status-Speed-Width
Displays the state of the chain link between the Multiport Link 1 and 2. The status can be Operational, Standby, or Unknown.

Multiport Link 2 I/O Cage-Slot
Displays the I/O cage and slot location of the multiport link 2.

Multiport Link 2 Cage-Slot-Jack
Displays the location of the cage, slot, and jack location of the multiport link 2.

Fanout Link 2 to IO Status-Speed-Width
Displays the fanout Link 1 location to IO status-speed-width.

PBU Link 2 to Fanout Status-Speed-Width
Displays the PBU Link 2 fanout status-speed-width.

Display PCHID/CSS.CHPID
To display the PCHID/CSS.CHPID Details for both sides of the RIO multiport on the selected RIO multiport row, click **Display PCHID/CSS.CHPID**.

Search PCHID/CSS.CHPID
To search for a specific PCHID/CSS.CHPID, click **Search PCHID/CSS.CHPID**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Redundant I/O Multiport PCHID/CSS.CHPID Details

Use this window to display Redundant I/O Multiport PCHID/CSS.CHPID Details for the selected RIO multiports. If the PCHID is not defined in the IOCDS, the CSS.CHPID fields are blank.

RIO multiport side 1
Displays the cage-slot location and possible associated PCHID/CSS.CHPID(s) for RIO multiport side 1.

RIO multiport side 2
Displays the cage-slot location and possible associated PCHID/CSS.CHPID(s) for RIO multiport side 2.

OK
To perform the selected operation, click **OK**.

Search for PCHID or CSS.CHPID

Use this window to enter a PCHID/CSS.CHPID and display the RIO multiport row that controls that PCHID/CSS.CHPID.

Enter the PCHID or the CSS.CHPID to search for
Enter the PCHID or the CSS.CHPID you want to search for.

OK
To perform the search operation, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Release I/O Path

Accessing the Release I/O Path task

Release is a CHPID operation you can use to free reconfigurable I/O paths from their assignment to isolated logical partitions.

The active input/output configuration data set (IOCDS) determines whether channel paths are reconfigurable, and which logical partition each I/O path is assigned to. Each logical partition's security settings determine whether it is isolated. A logical partition's initial security settings are set by the activation profile used to activate it. Afterwards, the **Change LPAR Security** task can be used to change the settings. For more information, see the **Change LPAR Security** task.

Reconfigurable I/O paths assigned to an isolated logical partition do not become available to other logical partitions when they are configured off. Releasing such I/O paths will make them available to other logical partitions.

I/O paths that are both reconfigurable and isolated are eligible for being released. The reconfigurable I/O path displays **Shared** or **Dedicated** and either **Isolated** or **Not isolated** to indicate whether it is assigned to an isolated logical partition.

To release I/O paths:

1. The central processor complex (CPC) must be power-on reset.
2. The I/O paths must be defined as reconfigurable in the active input/output (I/O) configuration.
3. The I/O paths must be assigned to isolated logical partitions.
4. The I/O paths must be configured off.
5. Locate the reconfigurable I/O paths you want to release.
6. Open the **Release I/O Path** task.
7. Click **OK** from the confirmation window to confirm your request to release the selected I/O paths.

   This releases the I/O paths.

Note: Upon configuring off and releasing reconfigurable I/O paths from isolated logical partitions, you must use operating system facilities to configure them on to other logical partitions.

Release I/O Path Confirmation

Use the Release I/O Path Confirmation window to confirm or cancel your request to release the selected reconfigurable I/O paths from the logical partitions to which they are currently assigned.

Releasing isolated reconfigurable I/O paths from the logical partitions to which they are currently assigned makes them available for being configured on to other logical partitions.

Note: Although you can also release reconfigurable I/O paths that are not isolated, it is not necessary, since they are already available for being configured on to other logical partitions.

Isolated
Reconfigurable I/O paths are referred to as *isolated* if they are assigned to a logical partition that is activated with logical partition isolation enabled.

Logical partition isolation is a setting in a logical partition's image profile that controls whether its reconfigurable I/O paths become available to other logical partitions when the I/O paths are configured off:

- When a logical partition is activated with logical partition isolation disabled, its reconfigurable I/O paths become available to other logical partitions when the I/O paths are configured off.
- When a logical partition is activated with logical partition isolation enabled, its reconfigurable I/O paths are isolated, and do not become available to other logical partitions when the I/O paths are configured off.

  Instead, after an isolated I/O path is configured off, it must also be *released* to make it available to other logical partitions.

Channel path identifier list
Displays a list of channel path identifiers (IDs) of the reconfigurable I/O paths you selected to release.

OK
To confirm your request to release the selected reconfigurable I/O paths from the logical partitions to which they are currently assigned, click **OK**.

Cancel
To cancel your request and close this window without releasing any I/O paths, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remote Hardware Management Console

Accessing the Remote Hardware Management Console task

Notes:

- You cannot perform this task remotely.
- You can only establish a remote session to another Hardware Management Console if the following conditions are met:
  - The Hardware Management Consoles are in the same domain. To verify the domain, use the **Domain Security** task.
  - Remote operation is enabled on the remote Hardware Management Console. To enable remote operation, use the **Customize Console Services** task.

This task allows the local Hardware Management Console user to open a browser session to another Hardware Management Console.

To establish a remote session:

1. Open the **Remote Hardware Management Console** task. The Remote Hardware Management Console Addressing Information window is displayed.
2. Specify the IPv4 or IPv6 TCP/IP address or host name of the remote Hardware Management Console you want to contact.
3. Click **OK** to complete the task or **Cancel** to exit.

Remote Hardware Management Console

Use this window to start a session to another Hardware Management Console.

Note: You can only establish a remote session to another Hardware Management Console if the following conditions are met:

- The Hardware Management Consoles are in the same domain. To verify the domain, use the **Domain Security** task.
- Remote operations is enabled on the remote Hardware Management Console. To enable remote operation, use the **Customize Console Services** task.

TCP/IP host name or address
Specify the IPv4 or IPv6 Transmission Control Protocol/Internet Protocol (TCP/IP) address or host name of the remote Hardware Management Console to be contacted.

The IPv4 address is written as four decimal numbers, representing the four bytes of the IP address, separated by periods (for example, `9.60.12.123`). The IPv6 address can be written as eight groups of four hexadecimal digits, separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

OK
To start a remote session to another Hardware Management Console, click **OK**.

Cancel
To exit this window without starting a remote session, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remote Service

Accessing the Remote Service task

This task allows you to enable or disable remote service for individual objects or a group of objects. When enabled, error information may be sent by a Hardware Management Console operator or automatically to the support system for analysis and for service call requests. When disabled, error information and requests for service must be done through voice communications.

Authorize automatic service call reporting will send error information and requests for service automatically to the support system without operator intervention.

To customize remote service settings:

1. Select one or more objects (servers).
2. Open the **Remote Service** task. The Customize Remote Service window is displayed.
   - Enable remote service by selecting **Enable remote service requests**. This option (a check mark is displayed) allows the Hardware Management Console to establish remote connections for the object or objects to your service provider's remote service support system.
   - Enable automatic service calling by selecting:
     - **Authorize automatic service call reporting** to set the console to automatically report problems and request service.
3. Verify the **Customer Service Center Telephone Number** is correct or provide a new one in the input area.
4. Click **OK** when you have completed the task.

Remote Service

Use this window to specify remote service settings for individual systems or a group of systems. Each targeted system is represented by a read-only tab that allows its current remote service settings to be viewed. In addition, an editable **Working Copy** tab provides remote service settings that can be updated and applied to all targeted systems.

Remote service is two-way communication between the console and the support system for the purpose of conducting automated service operations. Using remote service reduces the operator interaction needed to complete some service operations and provides some console tasks with another source or destination for sending or receiving service information.

The controls you will use to customize the console's remote service settings are determined by whether you want to enable or disable remote service.

Controls for enabling remote service

Enable remote service if you want to allow console connections to the support system.

Select “Enable remote service requests” on page 1289 to enable remote service. If it is not selected remote service is disabled.

After enabling remote service, customize how service calls are reported:

“Authorize automatic service call reporting” on page 1289
To set the console for authorization to automatically report problems that require service (referred to as *automatic service call reporting*), select **Authorize automatic service call reporting**.

“Customer Service Center Telephone Number” on page 1289
This field displays the telephone number the console's hardware messages will include as an option for reporting problems and requesting service if automatic service call reporting is disabled. You can change the telephone number whenever necessary.

If remote service is disabled, the console includes the customer service center telephone number in the hardware messages it issues to notify console operators of problems that require service. Such hardware messages typically instruct the console operator to call the customer service center to report the problem and request service.

The customer service center telephone number is required *even when remote service is enabled*. The console may not always be able to automatically report a problem that requires service, and will issue a hardware message to instruct the console operator to call the customer service center instead. For example:

- The console may fail to connect to the support system while making a service call.
- The console may not be authorized to automatically make service calls.

  Note: In this case, hardware messages for problems that require service provide two options: calling the customer service center or manually authorizing the console to make the service call.

About remote service

Remote service is two-way communication between the Hardware Management Console and the support system for the purpose of conducting automated service operations.

- *Enable* remote service if you want to allow console connections to the support system (a check mark appears).
- *Disable* remote service if you do *not* want to allow console connections to the support system (a check mark does not appear).

Using remote service reduces the operator interaction needed to complete some service operations and provides some console tasks with another source or destination for sending or receiving service information. For example, by using remote service:

- You can allow the Hardware Management Console automatically report problems and request service through the support system.
- You can use the support system as a source for retrieving internal code changes.
- You can use the support system as a destination for transmitting service data.

About automatic service call reporting

The console issues hardware messages to notify console operators of problems that require service. When automatic service call reporting is authorized, the console can automatically report problems and request service through console connections to the support system.

Otherwise, when automatic service call reporting is *not* authorized, a console operator must decide how to report problems and request service. A problem's hardware message provides two options:

- Calling the customer service center to speak to a service representative
- Or manually authorizing the console to make the service call through a console connection to the support system.

Additional functions available from this window.

Reset
To set the editable Working Copy remote service settings fields back to their original values, click **Reset**.

Use As Working Copy
To set the editable Working Copy remote service settings fields to the values of the selected system, click **Use As Working Copy**.

OK
To accept the settings of the remote service configuration, click **OK**.

Cancel
To exit this task without configuring for remote service, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Enable remote service requests

To enable remote service, select **Enable remote service requests**.

About remote service

Remote service is two-way communication between the Hardware Management Console and the support system for the purpose of conducting automated service operations.

- *Enable* remote service if you want to allow console connections to the support system (a check mark appears).
- *Disable* remote service if you do *not* want to allow console connections to the support system (a check mark does not appear).

Using remote service reduces the operator interaction needed to complete some service operations and provides some console tasks with another source or destination for sending or receiving service information. For example, by using remote service:

- You can allow the Hardware Management Console automatically report problems and request service through the support system.
- You can use the support system as a source for retrieving internal code changes.
- You can use the support system as a destination for transmitting service data.

Authorize automatic service call reporting

If remote service is enabled, select **Authorize automatic service call reporting** to set the Hardware Management Console for authorization to automatically report problems that require service (referred to as *automatic service call reporting*).

About automatic service call reporting

The console issues hardware messages to notify console operators of problems that require service. When automatic service call reporting is authorized, the console can automatically report problems and request service through console connections to the support system.

Otherwise, when automatic service call reporting is *not* authorized, a console operator must decide how to report problems and request service. A problem's hardware message provides two options:

- Calling the customer service center to speak to a service representative
- Or manually authorizing the console to make the service call through a console connection to the support system.

Customer Service Center Telephone Number

This field displays the telephone number of the customer service center. Hardware Management Console operators can call this number to speak to a service representative about product problems and service.

If remote service is disabled, the console includes the customer service center telephone number in the hardware messages it issues to notify console operators of problems that require service. Such hardware messages typically instruct the console operator to call the customer service center to report the problem and request service.

The customer service center telephone number is required *even when remote service is enabled*. The console may not always be able to automatically report a problem that requires service, and will issue a hardware message to instruct the console operator to call the customer service center instead. For example:

- The console may fail to connect to the support system while making a service call.
- The console may not be authorized to automatically make service calls.

  Note: In this case, hardware messages for problems that require service provide two options: calling the customer service center or manually authorizing the console to make the service call.

Removable Media or FTP Server

Removable Media or FTP Server

Use the removable media or FTP server window to copy data from the selected media.

/console/data
To copy console data, select **/console/data**.

USB media
To copy data from a USB flash memory drive, select **USB media**.

Then insert a USB flash memory drive into a USB port, and click **OK**.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP server
To copy data from an FTP server, select **FTP server**. Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the Manage SSH Keys task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To copy data from the selected media device or FTP server, click **OK**.

Cancel
To close this window without copying data from the selected media or FTP server, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove Object Definition

Accessing the Remove Object Definition task

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables you to remove a server (CPC) that is currently part of **Systems Management** in the navigation pane. During definition removal, the Remove Object Definition Task Confirmation window is displayed, if the option was set on the User Settings Confirmations page, to allow you to continue or quit the **Remove Object Definition** task.

After a CPC is removed from **Systems Management**, it is added to the **Unmanaged Systems** group. No further action will be possible on that server (CPC) from the Hardware Management Console that removed its definition, status will not be reported, and messages will not be available.

To remove an object:

1. Select an object.
2. Open the **Remove Object Definition** task. The Remove Object Definition Task Confirmation window is displayed.
3. Click **Yes** to continue with this task, or click **No** to exit the task.

Report a Problem (on an object)

Accessing the Report a Problem task

This task allows you to report a problem on the CPC. You should use this task only when there are no Problem Analysis results for the problem.

If Problem Analysis results do exist, report the problem by clicking the **Service** on the Hardware Messages window associated with the problem. If Problem Analysis was not invoked automatically, use the **Perform Problem Analysis** task to attempt to resolve the problem without a request for service.

You can also use this task to test problem reporting.

To report a problem on a CPC:

1. Select a CPC (server).
2. Open the **Report a Problem** task. The Report a Problem window is displayed.
3. Select the type of problem from the list provided and enter a brief description of your problem in the **Problem Description** input field, then click **Request Service**.
4. Click **Request Service**.

To test whether problems can be reported you can perform the following:

1. Select **Test automatic problem reporting** from the Report a Problem window and enter **This is just a test** in the **Problem Description** input field.
2. Click **Request Service**. The Report Problem message window is displayed.
3. Click **OK** to complete the task.

Report a Problem

Use this window to either:

- Report a problem that occurred on the selected system, and to request service to repair it.
- Or test whether problems can be reported for the system (if testing is supported by the system's Support Element).

Problems are reported to the service provider for the selected system. Reporting a problem sends to the service provider the information you provide on this window, and machine information that identifies the system.

Ordinarily, Problem Analysis automatically detects error conditions, and reports to you any problem that requires service to repair it.

However, if you notice a problem occurred or you suspect a problem is affecting the system, but Problem Analysis has not reported it to you, then use this window to report the problem to the service provider.

Problem Type

Use this section of the window to either:

- Select the problem type that best describes where the problem occurred or what the problem affected on the selected system.
- Or test whether problems can be reported for the system (if testing is supported by the system's Support Element).

Possible problem types include:

Power
To report a problem with the power subsystem of the selected system, select **Power**.

CPC
To report a problem with hardware in the processor subsystem of the selected system, select **CPC**.

LAN
To report a problem with the local area network (LAN) that attaches the selected system, select **LAN**.

Software
To report a problem with an operating system or other software loaded on the selected system, select **Software**.

I/O
To report a problem with hardware in the input/output (I/O) configuration of the selected system, select **I/O**.

Type V Viewable PMH(PMV)
To report problems that do not call home automatically for the selected system, select **Type V Viewable PMH(PMV)**.

Health Check
To report the state of the system before applying a maintenance action (such as: driver upgrades, MCLs, MES adds), select **Health Check**.

Other
To report a problem with the selected system that is not adequately described by any other problem type, select **Other**.

Test automatic problem reporting
To test whether problems can be reported for the selected system, select **Test automatic problem reporting**.

Note: This option is displayed only if testing problem reporting is supported by the Support Element of the selected system.

Problem Description

Specify an explanation of the problem that occurred on the selected system.

Your comments will assist the service provider for the system with correctly determining the cause of the problem.

Additional functions are available from this window:

Request Service
To report the problem and request service to repair it, click **Request Service**.

Problems are reported to the service provider for the selected system. Reporting a problem sends to the support system the information you provide on this window, and machine information that identifies the system.

If this console is customized to use the Remote Support Facility (RSF) and is authorized to automatically call for service, the problem information and service request are sent to the support system automatically.

Otherwise, additional windows will be displayed to request you authorize an automatic service call, or to provide you with the instructions and information you need to manually contact the support system, request service, and describe the problem.

After the support system receives the service request, a service representative can be sent to the repair site, and can be prepared to repair the problem upon arriving.

Cancel
To exit this task without reporting a problem, click **Cancel**.

Help
To display help for the current window, click **Help**.

Test automatic problem reporting

To test whether problems can be reported for the selected system, select **Test automatic problem reporting**.

To report problems for the system:

- Remote service must be enabled for the system.
- The system must have at least one call-home server.

If the system is configured correctly for reporting problems, testing it will open a Type 1 problem. You should specify a description in the **Problem description** field to indicate it is only a test. Then click **Request Service** to start the test.

Notes:

- This option is displayed only if testing problem reporting is supported by the Support Element of the selected system.
- Problem reporting typically is tested during system installation.
- Use the **Remote Service** task to enable remote service and customize remote service settings for the system.
- The system's call-home servers can include this Hardware Management Console, other Hardware Management Consoles, and the systems's Support Element console if it is stand-alone Support Element. To configure **this** console as a call-home server for the system:
  1. Use the **Change Object Definition** task to identify the console as a call-home server for the system.
  2. Use the **Customize Outbound Connectivity** task to enable and access the console's call-home server service.

Report a Problem (on the HMC)

Accessing the Report a Problem task

This task reports problems that occurred on your Hardware Management Console to the support system (for example, the mouse does not work) or lets you test problem reporting.

Submitting a problem is dependent upon whether you have enabled authorized automatic service call reporting. You can do this by using the **Customize Remote Service** task and selecting **Authorize automatic service call reporting**. If it is enabled and you have a call-home server available, it will automatically send the problem to the support system.

If **Authorized automatic service call report** is not enabled, the problem will be logged in the Hardware Messages. You can subsequently send the problem to the support system by selecting the Hardware Management Console, access **Hardware Messages**, select the messages you want information on, click **Details...** in the Hardware Messages window. You will get the Problem Analysis window where you will click **Request Service...**.

To report a problem on your Hardware Management Console:

1. Open the **Report a Problem** task. The Report a Problem window is displayed.
2. Select a problem type then enter a brief description of your problem in the **Problem Description** input field.
3. Click **Request Service**.

To test problem reporting from the Report a Problem window:

1. Select **Test automatic problem reporting** and enter *This is just a test* in the **Problem Description** input field.
2. Click **Request Service**.

Report a Problem

Use this window to either:

- Report a problem that occurred on the Hardware Management Console, and to request service to repair it.

  Or

- Test whether problems can be reported for the console.

Problems are reported to the support system for the Hardware Management Console. Reporting a problem sends to the support system the information you provide on this window, and machine information that identifies the console.

Ordinarily, Problem Analysis automatically detects error conditions, and reports to you any problem that requires service to repair it.

However, if you notice a problem occurred or you suspect a problem is affecting the Hardware Management Console, but Problem Analysis has not reported it to you, use this window to report the problem to the support system.

Use the window's controls to identify and describe the problem, then click **Request Service** to report it.

Test automatic problem reporting

To indicate whether you want to test problem reporting for the Hardware Management Console, select **Test automatic problem reporting**.

To report problems for the console:

- Remote service must be enabled for the console.
- The console must have at least one call-home server.

If the console is configured correctly for reporting problems, testing it will open a Type 1 problem. You should specify a description in the **Problem Description** field to indicate it is only a test. Then click **Request Service** to start the test.

Notes:

- Problem reporting typically is tested during Hardware Management Console installation.
- Use the **Customize Remote Service** task to ensure remote service is enabled for the console.
- This console's call-home servers can include itself and other discovered Hardware Management Consoles. Use the **Customize Outbound Connectivity** task to enable this console as a call-home server.

Type V Viewable PMH(PMV)
To report problems that do not call home automatically, select **Type V Viewable PMH(PMV)**. The content for the **Problem Description** should come from the direction of the support system.

HMC problem
To report a problem that occurred on the Hardware Management Console (HMC), select **HMC problem**. Include a description of the problem in the **Problem Description** area.

Health Check
To report the state of the HMC before applying a maintenance action (such as: driver upgrades, MCLs, MES adds), select **Health Check**.

Problem Description
Specify an explanation of the problem that occurred on the Hardware Management Console.

Your comments will assist the support system for the console with correctly determining the cause of the problem.

Request Service
To report the problem and request service to repair it, click **Request Service**.

Problems are reported to the support system for the Hardware Management Console. Reporting a problem sends to the support system the information you provide on this window, and machine information that identifies the console.

If this Hardware Management Console is customized to use the Remote Support Facility (RSF) (**Customize Remote Service** task) and is authorized to automatically call for service, the problem information and service request are sent to the support system automatically.

Otherwise, additional windows will be displayed to request you authorize an automatic service call, or to provide you with the instructions and information you need to manually contact the support system, request service, and describe the problem.

After the support system receives the service request, a service representative can be sent to the repair site, and can be prepared to repair the problem upon arriving.

Cancel
To exit this task without reporting a problem, click **Cancel**.

Help
To display help for the current window, click **Help**.

Reset Clear

Accessing the Reset Clear task

Notes:

- This task is supported only for CPC image objects or groups of CPC images.
- Reset Clear is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task terminates any current operations and clears any interruption conditions in a CPC image (except for a coupling facility image). A reset clear clears main storage and all registers during initialization.

To perform a reset:

1. Select a CPC image.
2. Open the **Reset Clear** task. The Reset Clear Task Confirmation window is displayed.
3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
4. To continue with the reset, click **Yes**. The Reset Clear Progress window is displayed indicating the progress of the reset and the outcome.
5. Click **OK** to close the window when the reset completes successfully.

Otherwise, if the reset does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Reset Error Thresholds

Reset Error Thresholds

This window displays a list of selected PCHIDs that you want to reset the threshold that was used to stop reporting Interface Control Checks (IFCCs) and Bit Errors (BERs).

PCHID table
Lists the PCHIDs that require a reset error threshold.

OK
To reset the error threshold for the list of PCHIDs, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Reset Normal

Accessing the Reset Normal task

Notes:

- This task is supported only for CPC image objects or groups of CPC images.
- Reset Normal is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task terminates any current operations and clears any interruption conditions in a CPC image (except for a coupling facility image). A reset normal does not clear main storage during initialization.

To perform a Reset Normal:

1. Select one or more CPC images.
2. Open the **Reset Normal** task. The Reset Normal Task Confirmation window is displayed.
3. Review the information on the window to verify that the object(s) you will reset is the correct one.

   If the information is correct, click **Yes**. The Reset Normal Progress window displays indicating the progress of the reset and the outcome.
4. Click **OK** to close the window when the reset completes successfully.

   Otherwise, if the reset does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Restart z/VM Management Guest

Accessing the Restart z/VM Management Guest task

Use this task to issue a restart request of the target z/VM management guest machine. This task can be used to recover from situations where the z/VM management guest is not operating correctly.

Additionally, this task resets the automatic restart threshold for the automatic restart of the z/VM management guest by the SE.

Perform the following steps to restart a z/VM management guest:

1. Select a z/VM hypervisor.

2. From the **Service** task group, open the **Restart z/VM Management Guest** task. The Reboot Confirmation window is displayed.
3. If you want to continue this task, click **Yes**. If you want to end this task, click **No**.
4. Click **OK** to close the window.

Retrieve Backup or Upgrade Data

Accessing the Retrieve Backup or Upgrade Data task

Use this task when you want to retrieve backup or upgrade files that are located on an external server.

To retrieve the files:

1. Select a CPC (server).
2. Open the **Retrieve Backup or Upgrade Data** task. The Retrieve Backup or Upgrade File from FTP window is displayed.
3. Select the type of file (**Backup file** or **Upgrade file**) that you want to retrieve from an FTP server.
4. Click **Retrieve** to proceed or **Cancel** to end the task.
5. If you chose to retrieve either the backup file or upgrade file, the Retrieve Backup or Upgrade File from FTP window is displayed.
6. Provide the required FTP site, user ID, and password information if it is not already provided, then click **OK** to proceed.
7. If you chose the backup file, the Backup Files in the FTP Server window is displayed. Select a backup file, then click **OK**.

   If you chose the upgrade file, the Retrieve Backup or Upgrade File from FTP window is displayed. Select an upgrade file, then click **OK**.

Retrieve Internal Code

Accessing the Retrieve Internal Code task

Note: You can perform this task remotely **only** when you are retrieving data from the support system to a selected system.

This task copies internal code changes from the selected source to a Hardware Management Console work space and distributes updates to the Support Elements of systems defined to the Hardware Management Console. This task is to be used when you are working with internal code changes for the Support Elements. Changes to the Hardware Management Console internal code are controlled using the **Change Console Internal Code** task.

To retrieve internal code changes:

1. Select one or more systems.
2. Open the **Retrieve Internal Code** task. The Retrieve Internal Code Changes window is displayed.
3. Choose to work with all systems or selected systems:

   Selected systems
   Distributes code changes only to selected systems.

   All systems
   Distributes code changes to all defined systems.

   The Retrieve Internal Code Changes window is displayed.
4. You can retrieve changes from the following sources and to the following targets.

Retrieve code changes from removable media to the selected objects
Select this when the internal code changes have been delivered to you on removable media for a system.

Retrieve code changes from FTP site to the selected objects
Select this when internal code changes are available to you from an FTP site for a system. You also have the option to enable a secure data transfer.

Retrieve code changes from support system to the selected objects
Select this when you have been notified you that new internal code changes are available through the support system and you want to retrieve the changes to the selected system.

Retrieve code changes to all Hardware Management Consoles also
Select this option to distribute code changes to the hard disk of all known Hardware Management Consoles, at Licensed Internal Code Version 2.9.2 or later, that are connected to the same LAN network as the selected systems.

Note: A service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on your hard disk, it is recommended that you manage these changes only under the supervision of a service representative or with the assistance of your support system.

Retrieving internal code changes only copies them from the source to the Support Element hard disk. Retrieved internal code changes do not affect the operation of your processor cluster until you install and activate them using the controls under the **Change Internal Code** task.

5. Click **OK** to proceed through the task windows.

Retrieve Internal Code Changes (from the source to the selected object)

Use this window to copy internal code changes from their source to the selected objects.

Retrieve options

Select one of the following options, then click **OK** to begin:

Retrieve code changes from removable media to the selected objects
To copy internal code changes from removable media to the selected objects, select **Retrieve code changes from removable media to the selected objects**.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times (if an internal speaker is available and is not muted) and a message may display indicating the drive was not added and that you should remove the device and try again.

Then click **OK** to continue.

Use this option when you have removable media that has internal code changes stored on it. For example, use this option when either:

- The internal code changes have been delivered to you on removable media.
- You used another console to copy internal code changes from the support system to removable media.

Retrieve code changes from the support system to the selected objects
To copy internal code changes from the support system to the selected objects, select **Retrieve code changes from the support system to the selected objects**.

Then click **OK** to continue.

Use this option when:

- This console is configured and enabled for communicating with the support system.
- And after the support system has notified you that new internal code changes are available from the support system.

Retrieve code changes from FTP site to the selected objects

To copy internal code changes from an FTP site to the selected objects, select **Retrieve code changes from FTP site to the selected objects**.

Then click **OK** to continue.

Use this option when you have an FTP site that has internal code changes stored on it.

Note: This option is only available for objects at version 2.14.0.

In addition to choosing an option to perform, you can also choose to distribute code changes to the hard disk of all known Hardware Management Consoles, at Licensed Internal Code Version 2.9.2 or later that are connected to the same LAN network as the selected systems, by selecting **Retrieve code changes to all Hardware Management Consoles also** (a check mark appears).

Retrieving internal code changes

Retrieve internal code changes to copy them from their source to the selected objects. Following are some examples of the options with step-by-step instructions.

Important: Instructions for retrieving internal code changes will vary with their source and the set of changes you want to retrieve. Each example below provides instructions for a particular situation. Your situation may be different; refer to the instructions for general guidance. Then, while performing the task, request help for any window while it displays for more information about using it to complete the task.

Example 1

The following example shows the steps for:

- Using removable media as the source of internal code changes.
- Retrieving **all** internal code changes available from that source to selected systems.

From the **Hardware Management Console Workplace**:

1. Start the task: **Retrieve Internal Code**.

   This opens the **Retrieve Internal Code Changes** window. From the **Retrieve Internal Code Changes** selection window:
2. Click either **Selected systems** or **All systems**.

   This opens the **Retrieve Internal Code Changes** window. From the **Retrieve Internal Code Changes** window:
3. Select **Retrieve code changes from removable media to the selected objects**, then click **OK**.

   This opens the **Insert Removable Media** window. From the **Insert Removable Media** window:
4. Insert a System Update Level (SUL) media, then click **OK**.

   This opens the **Select Media Device** window. From the **Select Media Device** window:
5. Select the device you are going to be retrieving changes to, then click **OK**.

   This opens the **Select Internal Code Changes** window. From the **Select Internal Code Changes** window:
6. Select **All internal code changes**, then click **OK**.

   This opens the **Confirm the Action** window. From the **Confirm the Action** window:
7. Select **Retrieve** to begin the process.

   This opens the **Retrieve Internal Code Progress** window. From the **Retrieve Internal Code Progress** window:
8. Wait until the Status field of the table indicates the request has completed, then click **OK** to close the window.

   This completes the task.

Example 2

The following example shows the steps for:

- Using the **support system** as the source of internal code changes.
- Retrieving **one specific** internal code change from that source to selected systems.

From the **Hardware Management Console Workplace**:

1. Start the task: **Retrieve Internal Code**.

   This opens the **Retrieve Internal Code Changes** window. From the **Retrieve Internal Code Changes** selection window:
2. Click either **Selected systems** or **All systems**.

   This opens the **Retrieve Internal Code Changes** window. From the **Retrieve Internal Code Changes** window:
3. Select **Retrieve code changes from support system to the selected objects**, then click **OK**.

   This opens the **Select Internal Code Changes** window. From the **Select Internal Code Changes** window:
4. Select **Specific internal code changes**, then click **OK**.

   This opens the **Specify Internal Code Changes** window. From the **Specify Internal Code Changes** window:
5. If necessary, contact your support system to determine the Engineering Change (EC) number and change level of the internal code change you want to retrieve.
6. Specify the Engineering Change (EC) number in the first **EC Number** field.
7. Specify the change level in the adjacent **Change level** field.
8. Click **OK**.

   This opens the **Confirm the Action** window. From the **Confirm the Action** window:
9. Select **Retrieve** to queue a request for establishing a remote connection to the support system.

   This opens the **Retrieve Internal Code Progress** window. From the **Retrieve Internal Code Progress** window:
10. Wait until the Status field of the table indicates the request has completed, then click **OK** to close the window.

    This completes the task.

    Note: The internal code change will be retrieved when the queued request is processed, and a remote connection to the support system is established. Processing the request depends on the availability of the telephone line for the console modem, and on the priority of other requests in the queue.

The following options are also available from this window:

OK
To start the task that you have selected, click **OK**.

Object List
To display a list of the objects you have selected, click **Object List**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Retrieve Internal Code Changes (for selected objects or all defined objects)

Use this window to retrieve internal code changes for only selected objects or for all defined objects.

Selected systems
To retrieve internal code changes to selected systems only, click **Selected systems**.

All systems
To retrieve internal code changes to all defined systems, click **All systems**.

Help
To display help for the current window, click **Help**.

Request Selection

Use this window to proceed with your request to retrieve all internal code changes for the selected systems.

Selected systems
Use this list to verify that the systems displayed are the correct objects you wish to retrieve all internal code changes for.

OK
To confirm your request to retrieve all internal code changes for the systems displayed, click **OK**.

Help
To display help for the current window, click **Help**.

Confirm the Action

Use this window to confirm or cancel your request to retrieve internal code changes from their source to the selected objects.

Retrieving internal code changes makes them available for being installed and activated.

At this point in the task, **internal code changes** are:

- All changes available from the source you selected.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Internal code change process

The window displays a summary of the recommended internal code change process. Retrieving internal code changes is the third step (step **C**) of the process. Review the process before continuing.

Note: You should cancel your request to retrieve internal code changes in these cases:

- If you have not completed the last step of the process for **previous** internal code changes. That is, if you have not yet installed and activated all **previously** retrieved internal code changes.
- If you did not perform the first or second steps (steps **A** or **B**) of the process upon receiving the new internal code changes. That is:
  - If you have not yet performed a backup of critical data of the selected objects.
  - Or if you have not yet accepted all **previously** installed and activated internal code changes.

You should confirm your request to retrieve new internal code changes only after completing the recommended steps described above.

The following functions are also available from this window:

Retrieve
To confirm your request to retrieve internal code changes from their source to the console, click **Retrieve**.

Object List
To display the selected objects that you requested to retrieve all internal code changes for, click **Object List**.

Cancel
To cancel your request and close the window without retrieving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Specify Internal Code Changes

Use this window to identify the specific internal code changes you want the task you selected to apply to.

Identify the changes by their Engineering Change (EC) numbers and change levels.

Note: You will need the assistance of your support system to identify a specific internal code change by its EC number and change level.

Engineering Change Table
Complete one row of fields for each internal code change you want to apply the task to, then click **OK** to continue the task.

Note: Fields are initialized with default entries for EC numbers and change levels derived from previous entries, if any. If you do not want to use the default entries, click **Clear** to discard them. All entry fields will be cleared to allow typing other EC numbers and change levels.

EC Number
Specify the EC number of the internal code change you want the task you selected to apply to.

Then use the applicable fields in the same row to identify the change levels of the internal code change you want the task to apply to.

Change level
Specify the number of the last change level you want the task you selected to apply to. Or specify **ALL** to apply the selected task to all applicable change levels.

The task will be applied to applicable change levels of the internal code change, identified by the adjacent EC number, from the current applicable change level to the change level you specify.

Note: This field does **not** display if you selected to retrieve internal code changes to a removable medium.

Identify a specific internal code change
A specific internal code change is identified by an Engineering Change (EC) number and a change level.

One unit of internal code is called an **Engineering Change (EC)**. An EC is referred to also as a **stream**.

An **Engineering Change (EC) number** is assigned to an EC by product support. The number identifies the purpose of the internal code in the EC.

An **internal code change** for an EC changes all or part of the internal code in it. Both an EC and its internal code changes are identified by the same EC number.

But the EC number of an internal code change is qualified by another number, called an **internal code change level**, to distinguish it from the EC it changes.

The internal code change level, referred to also as a **change level**, also distinguishes an internal code change from previous and subsequent changes for the same EC.

For example, a unit of internal code, or EC, initially stored on the Hardware Management Console during manufacturing is assigned the EC number: E01234.

After the console is delivered and installed, it may be necessary to change EC E01234 to add new functions, improve existing functions, or correct problems. To do that, an internal code change is provided for the EC.

The EC number of the first internal code change would be E01234, while its change level would be 001. The change level would be increased by 1 for each subsequent internal code change for EC E01234.

Change level
Specify the number of the last change level you want the task you selected to apply to. Or specify **ALL** to apply the selected task to all applicable change levels.

The task will be applied to applicable change levels of the internal code change, identified by the adjacent Engineering Change (EC) number, from the current applicable change level to the change level you specify.

The applicable change levels and their range depends on the task you selected:

Accept
Applies to installed and activated change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Accept
Applies to installed and activated change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Install
Applies to retrieved change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Remove
Applies to installed change levels in the range from the highest change level down to and including the change level you specify.

Delete
Applies to retrieved and removed change levels in the range from the highest change level down to and including the change level you specify.

Install
Applies to retrieved change levels in the range from the lowest change level up to and including the change level you specify.

Remove
Applies to installed change levels in the range from the highest change level down to and including the change level you specify.

Retrieve
Applies to change levels available from the source in the range from the lowest change level up to and including the change level you specify.

Note: You will need the assistance of your support system to identify a specific internal code change by its EC number and change level.

OK
To continue the selected task and apply it to the specific internal code changes identified by the EC numbers and change levels, click **OK**.

Clear
To remove the information from all entry fields on the window, by discarding the EC numbers and change levels specified the last time the window was used, click **Clear**.

Cancel
To close the window, and return to the window from which you selected the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save Upgrade Data

Accessing the Save Upgrade Data task

This task saves all of the upgrade data for your console to the hard drive, USB flash memory drive, or FTP server before performing an Engineering Change (EC) upgrade.

To save the console upgrade data to the hard drive:

1. Open the **Save Upgrade Data** task. The Save Upgrade Data window is displayed.
2. Select **Hard drive**. It takes from one to five minutes to save the data.
3. When the data is saved, the Save Upgrade Data Completed window is displayed.
4. Click **OK** to end the task.

Save Upgrade Data

Use this window only while following an Engineering Change (EC) upgrade procedure that instructs you to save the console's upgrade data.

The console's *upgrade data* is information on its hard disk that is unique to it. Upgrading the console requires saving its upgrade data *before* installing new ECs, then restoring the upgrade data afterwards.

Some EC upgrade procedures save and restore the console's upgrade data automatically, and there is no need to use this task. Otherwise, if you are following an EC upgrade procedure that instructs you to save the console's upgrade data, you must use this task to save it manually.

Hard drive
To save the console's upgrade data to the hard drive, select **Save to hard drive**.

USB flash memory drive
To save the console's upgrade data to the USB flash memory drive, select **Save to USB flash memory drive**.

The USB flash memory drive for the Save Upgrade Data task must be formatted with a value label of **ACTUPG**, using the **Format Media** task.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP server
To save the console's upgrade data to an FTP server, select **FTP server**.

OK

To save the upgrade data to the selected location, click **OK**.

When you select **USB flash memory drive**, the **Select Media Device** window is displayed. From this window you can choose the media you want to send the data to. You can click **OK** to continue with the task, click **Refresh** to redisplay your media selections, or click **Cancel** to return to the previous window.

Refresh
To redisplay the list of available media, click **Refresh**. Use this option if you did not insert your media before this point in the task.

Cancel
To cancel this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save Upgrade Data (on an object)

Accessing the Save Upgrade Data task

This task allows you to save upgrade data of a remote element that is to be restored during an upgrade.

To save upgrade data:

1. Select a CPC (server).
2. Open the **Save Upgrade Data** task. The FTP Server Information window is displayed.

3. Provide the FTP server information where your data will be saved.
4. Click **OK** to apply the information.

Save/Restore Customizable Console Data

Accessing the Save/Restore Customizable Console Data task

Notes:

- If you want to save the data to a USB flash memory drive, you cannot perform this task remotely.
- If **Customizable Data Replication** is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see **Configure Data Replication** task.

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables you to save the following customizable Hardware Management Console data:

Associated Activation Profiles
Any activation profiles associated with CPC and CPC image objects.

Remote Service Data
Whether or not you have enabled remote service to allow automatic console connections to the support system.

Acceptable Status Settings
Any status settings that are considered acceptable for all types of managed objects.

Monitor System Events Data
Data for the **Monitor System Events** task including:

- The SMTP server and port settings
- The setting for the minimum time between emails
- The event monitors.

Outbound Connectivity Data
Configuration data that is specified in the **Customize Outbound Connectivity** task for making outbound connections. This data type also includes configuration data specified in the **Configure IDAA Call Home** task for host names or IP addresses of IDAA consoles that are allowed to use this Hardware Management Console (HMC) as a call-home proxy.

Remote Syslog Server Data
Configuration data specified in the **Manage Syslog Servers** task for the syslog servers that the Hardware Management Console sends audit and event information to, including which data types are sent.

User Profile Data
User identifications, authentication mode and roles, password rules, user pattern definitions, user template definitions, user settings that were created and retained, in addition to LDAP servers and optional LDAP user IDs.

Last User Logon Data
Restoring the enterprise wide data of the newest logon information, replicating automatically from the replica to the primary.

User Interface Customization Data
Restoring the user interface customizations.

Customer Information Data
Data for a CPC or a group of CPCs which includes administrator, system, and account information about the system being installed.

Domain Security Data
Security definitions (domain name and password) for your Hardware Management Consoles and CPC Support Elements in your processor complex.

Object Locking Data
Whether to automatically lock all managed objects or whether to relock after a task runs.

Group Data
All user-defined group definitions.

SNMP API Settings
SNMP API configuration information.

To save or restore customizable console data:

1. Open the **Save/Restore Customizable Console Data** task. The Save/Restore Customizable Console Data window is displayed.
2. Select one or more data types you want to save or restore.
3. Use the default file name to save the data to or restore the data from or specify your own in the **File name** input field.
4. Click **Save** to save data to USB flash memory drive or FTP sever, or click **Restore** to restore data from USB flash memory drive or FTP server.
5. Proceed with the your selection of USB flash memory drive or FTP server, or click **Cancel** to go back to the previous window without saving or restoring the data.

After saving this data, you can restore it to the same Hardware Management Console or to another Hardware Management Console.

Save/Restore Customizable Console Data

Use this window to distribute the same customizable console data among multiple consoles.

Customizable console data is data that is customized by users to set up how the console works. By saving and restoring customizable console data, you can easily tailor multiple consoles to have, for example, the same user IDs, user groups, domain, and look and feel.

Use this window first to save the customized data for a console that is customized the way that you want it. Then, restore that console's customizable data at each other console you want to work the same way.

Note: If Customizable Data Replication is enabled on the Hardware Management Console, the data that is specified in this task may change depending on automatic replication from other Hardware Management Consoles configured on your network.

To configure **Customizable Data Replication**:

1. Open the **Configure Data Replication** task, the **Configure Customizable Data Replication** window is displayed.
2. Select **Enable** in the **Configure Data Replication** box, the **Configure Customizable Data Replication** window is displayed.

You can save or restore one or more of the following types of customizable console data for a console:

- Associated Activation Profiles
- Remote Service Data
- Acceptable Status Settings
- Monitor System Events Data
- Outbound Connectivity Data
- Remote Syslog Server Data
- User Profile Data
- Last User Logon Data
- User Interface Customization Data
- Customer Information Data
- Domain Security Data

- Object Locking Data
- Group Data
- SNMP API Settings

Customizable Data Types

Use this window to save or restore customizable data for the console. The types of customizable data that can be saved or restored are:

Associated Activation Profiles
Any activation profiles that are associated with CPC and CPC image objects.

Remote Service Data
Whether or not you have enabled remote service to allow automatic console connections to the support system.

Acceptable Status Settings
Any status settings that are considered acceptable for all types of managed objects.

Monitor System Events Data
Data for the **Monitor System Events** task includes:

- SMTP server and port settings
- Minimum time between emails setting
- Event monitors.

Outbound Connectivity Data
Configuration data that is specified in the **Customize Outbound Connectivity** task for making outbound connections. This data type also includes configuration data specified in the **Configure IDAA Call Home** task for host names or IP addresses of IDAA consoles that are allowed to use this Hardware Management Console (HMC) as a call-home proxy.

Remote Syslog Server Data
Configuration data specified in the **Manage Syslog Servers** task for the syslog servers that the Hardware Management Console sends audit and event information to, including which data types are sent.

User Profile Data
User identifications, authentication mode and roles, password rules, user pattern and user template definitions, user settings that were created and retained for template user identifications, in addition to LDAP servers and optional LDAP user IDs.

Last User Logon Data
Restoring the enterprise-wide data of the newest logon information, replicating automatically from the replica to the primary.

User Interface Customization Data
Restoring the user interface customizations. For example: Masthead favorites and Home tab settings which include Work Pane Table sorts and filters, and Custom Table views. Replicating this data in a peer-to-peer setup allows the user interface to be replicated between all consoles.

Customer Information Data
Data for a CPC or a group of CPCs, which includes administrator, system, and account information about the system being installed.

Domain Security Data
Security definitions (domain name and password) for your Hardware Management Consoles and CPC support elements in your processor complex.

Object Locking Data
Whether to automatically lock all managed objects or whether to relock after a task runs.

Group Data
All user-defined group definitions.

SNMP API Settings
SNMP API configuration information.

By saving and then restoring one or more of these types of data, multiple consoles can easily be tailored to work and look the same.

USB flash memory drive

To save the console's customizable data to the USB flash memory drive, select **USB flash memory drive**. The USB flash memory drive for this task must be formatted with a value label of **ACTUPG**, using the **Format Media** task.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP server

To save the console's customizable data to an FTP server, select **FTP server**.

File name

Use this entry field to specify the file name to use for saving or restoring customizable console data. You can save it to or restore it from a USB flash memory drive.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

The file name will be a fully-qualified file name. The default name is **ccdata.dat**, which appears in the input field, and is appended to a fully qualified name once you have selected your media device.

You can also specify your own file name. For example, you can specify **myfile.dat** in the input field. If you selected a USB flash memory drive as your media device, then the fully qualified name is **/media/xxxx/myfile.data**, where **xxxx** is the unique ID of the USB in use.

Additional functions are available from this window:

Save
To save the specified customizable console data, click **Save**.

When a file name is specified, the **Select Media Device** message window is displayed. From the **Select Media Device** message window, select the type of media you want to save the data to. Then, either, click **OK** to save the data, click **Refresh** to refresh the list of available media, or click **Cancel** to go back to the previous window before saving to media.

Restore
To restore the specified customizable console data, click **Restore**.

When a file name is specified, the **Select Media Device** message window is displayed. From the **Select Media Device** message window, select the type of media you want to restore the data from. Then, either, click **OK** to restore the data, click **Refresh** to refresh the list of available media, or click **Cancel** to go back to the previous window before restoring from media.

Cancel
To end this task without saving or restoring data, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Media Device

Use this window to select the device to which the files will be saved to or restored from.

OK
To continue the task with the selected media, click **OK**.

Refresh
To update the device list, click **Refresh**.

Cancel
To exit this window without making any changes and to return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

File Transfer Information

Use this window to configure FTP settings when you use an external server to save or restore your files.

Host name
Specify the host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To apply this information, click **OK**.

Clear
To remove all information from the input fields, click **Clear**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Service On/Off

Accessing the Service On/Off task

Service on and *Service off* are channel operations you can use to control whether channels, identified with physical channel identifiers (PCHIDs) are on standby in, or reserved from, the active input/output (I/O) configuration:

- A channel is on *standby* while service is set off. It is in the active I/O configuration but it cannot be used until it is configured on. It will remain in the active I/O configuration until service is set on.
- A channel is *reserved* while service is on. It is not in the active I/O configuration and cannot be used. It will remain out of the active I/O configuration until service is set off.

Setting service on for a channel, which removes it from the active I/O configuration, allows running diagnostic tests on the channel without disturbing other channels being used by the system. Setting service on for a channel can be used also to remove failing channels from the I/O configuration so subsequent power-on resets will not attempt to initialize the failing channels.

If you have experience using other systems, setting service on or off for channels may have been referred to as taking channels in and out of single channel service (SCS), for which you may have used an SCS command with IN and OUT parameters.

To set service on and off for a channel:

1. Open the **Service On/Off** task.
2. Initially, each channel's current state and target state are the same. Use the Service On/Off window controls to change the target states of the channel that you want to set the service state on or off:
   - If the current state of a channel is **Reserved**, toggle its target state to **Standby** if you want to set service off for the channel.
   - If the current state of a channel is **Standby**, toggle its target state to **Reserved** if you want to set service on for the channel.

   If you attempt to change the target state of a channel that cannot have service set on or off, a message is displayed in the **Messages** list column to indicate changing the channel's state is not allowed. Double-click on the message for more information about why the channel state cannot be changed.
3. When you finish changing the target states of the channels for which you want to set service on or off, click **Apply** to make each channel's new target state its current state.
4. When you finish changing the target states of the object you want to service on or off, click **OK** to make each channel's new target state its current state.

Service On/Off

Use this window to set service on or off for channel paths. Set service on and off to control whether the channel paths are on standby in, or reserved from, the active input/output (I/O) configuration:

Important: Do not use this window to set service on or off unless you have been directed to do so.

- A channel path is on *Standby* or *Reserved* while service is set off. It is in the active I/O configuration but it cannot be used until it is configured on. It will remain in the active I/O configuration until service is set on.
- A channel path is *Reserved - Service* while service is set on. It is not in the active I/O configuration and cannot be used. It will remain out of the active I/O configuration until service is set off.
- A channel path is *Reserved* while service is set off. It is not in the active I/O configuration. A PCHID can be in a reserved state if it is not defined in the active IOCDS.

Setting service on for a channel path, which removes it from the active I/O configuration, allows running diagnostic tests on the channel path without disturbing other channel paths being used by the system. Setting service on for a channel path can be used also to remove failing channel paths from the I/O configuration so subsequent power-on resets will not attempt to initialize the filing channel paths.

To use the **Service On/Off** task the CPC must be power-on reset.

The window lists the following information for each channel path you selected to start the task. The information displayed depends on what object is selected. Selecting a crypto shows the Cryptographic number in the first column. Selecting a channel path shows the CSS and CHPID values in the first column. Select one or more channel paths or cryptos, then select **Toggle** from the drop down box to toggle their target states.

PCHID
Displays a four-digit physical channel identifier (PCHID) of each channel path.

"Current State" on page 1311
Indicates the current state of each channel path.

Desired State
Indicates the target state of each channel path.

Messages
If you attempt to change the target state of a channel path that cannot have service set on or off, this column displays the message "Not Allowed" for the channel path to indicate that changing its state is not allowed.

Current State

This window lists the current state and target of each channel path you selected to start the task. Use the window actions to *toggle* the target states of the channel paths you want to set service on or off.

- If the current state of a channel path is **Reserved - Service** toggle its target state to **Standby** or **Reserved** if you want to set service off for the channel path.
- If the current state of a channel path is **Standby,** or **Reserved** toggle its target state to **Reserved - Service** if you want to set service on for the channel path.

Online
Indicates the channel path is configured on. It is in the active Input/Output (I/O) configuration and it can be used. Service cannot be set on for the channel path until it is configured off.

Online pending
When the Central Processor Complex (CPC) is activated, this state indicates the channel path was configured on while assigned to an inactive logical partition. The channel path will be online when the logical partition is activated. Service cannot be set on for the channel path until it is configured off.

Reserved - Service
Indicates the channel path has service set on. It is not in the active I/O configuration, cannot be configured on, and cannot be used. It will remain out of the active I/O configuration until service is set off.

Reserved
Indicates the channel path has service set off. A PCHID can be in the reserved state if it is not defined in the active IOCDS.

Standby
Indicates the channel path has service set off. It is in the active I/O configuration but it cannot be used until it is configured on. It remains in the active I/O configuration until service is set on.

Additional functions on this window include:

OK

When you finish toggling the target states of the channel path, crypto, or FID you want to configure on or off, click **OK** to allow the new target states to take effect.

Cancel

To close the Service On/Off window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Service Required State Query

Service Required State Query

Use **Service Required State Query** to determine the reason for the Service Required State. If a pop up window indicates you are **not** in Service Required State at this time, the system is operating under normal conditions.

The list of reasons for the Service Required State displays only in a Service Required State.

Reasons

The **Service Required State** indicates that the next disruption will result in the system operating in a degraded capacity or will fail.

This window lists reasons that the Support Element is in the Service Required State:

Additional functions are available from this window:

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

Service Status

Accessing the Service Status task

This task sets a system to Service Status allowing a service representative to perform service tasks on the system or Support Element. Many of the system service tasks require that the system is first placed in Service Status. Repair and Verify, for example, cannot be run on a system until that system is placed in Service Status.

Service Status should be enabled for systems that are to be serviced. When in Service Status, the system status displayed on its Details window will be Service and no other status will be reported by the system until Service Status is disabled. During a service action, status changes (for example, No Power) that would normally cause an exception due to an unacceptable status will not cause an exception when the status is Service. System images will not be displayed on the Hardware Management Console when Service Status is enabled for the system.

Service status also prevents messages indicating the loss of communication to the Support Element from displaying while the Support Element is powered off or during licensed internal code (LIC) load.

To set the service status:

1. Select one or more systems.
2. Open the **Service Status** task. The Service Status window is displayed.
3. Select one or more objects from the table to change the status (check marks will appear).
4. Point to **Options** from the menu bar and then click **Enable service status**, **Disable service status**, or **Display error message** to enable or disable service status or display error messages, respectively.
5. Click **Save** to save your changes.
6. When you are asked if you are sure you want to save your changes, click **Yes**.

Service Status

Use this window to set the service status of one or more systems. You can also display error messages about the service status of the systems.

The service status of a system determines whether tasks that disrupt system operations can be performed in the service user mode of the system console or a Hardware Management Console.

Ordinarily, the service status for a system is disabled. This prevents the use of disruptive operations in the service user mode.

A service representative will request you temporarily enable the service status for a system. The service representative will need service status enabled to complete service procedures that may require performing disruptive operations.

To set the service status or to view error messages for a system, select the system or systems from the list, then click **Options** and select an action from the drop-down menu.

Note: The service status settings you change take affect only if you save them. Click **Save** to save changed settings.

Status Table

Object Name
Displays the names of the systems in the group selected.

Service Status
Indicates whether service status for the system is currently enabled or disabled, or if there is a service status error.

Options

Enable service status
To set the service status setting for the selected system to enabled, select **Enable service status**. The setting takes affect when you click **Save**. This setting permits the use of console operations in the service user mode that disrupt system operations.

Disable service status
To set the service status setting for the selected system to disabled, select **Disable service status**. The setting takes affect when you click **Save**. This setting prevents the use of console operations in the service user mode that disrupt system operations.

Display error message
To display a more detailed error message about the service status of the selected system, select **Display error message**.

Additional functions are available from this window:

Save
To save the settings currently displayed for service status, click **Save**.

The **Service Status** column displays the service status settings that will be saved.

Note: You must save changed service status settings to make them take affect.

Reset
To undo changes made to the service status settings and display again the settings most recently saved, click **Reset**.

Note: Click **Cancel** to undo changes made to the service status settings and to exit the task.

Cancel
To undo changes made to the service status settings, and to exit the task and return to the Hardware Management Console Workplace, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Service User Mode

Provides tasks and operations for problem determination and repair. Its intended users are the service representatives of the service provider for a system.

A service user mode is available at any system console or any Hardware Management Console. The access administrator for a console controls the user identifications and passwords that can be used to log in with the SERVICE default user ID or a user ID with service roles.

Enable service status

To enable the service status for one or more systems:

1. Select a system or systems from the names in the table (a checkmark appears in the **Select** column).
2. From the **Options** drop-down menu, select **Enable service status**.

   The **Service Status** column in the table displays **Enabled** to indicate that the service status is enabled for the selected system or systems.
3. To save the settings currently displayed in the list, click **Save**.

   A message panel is displayed verifying you want the setting to be changed.
4. Click **Yes** to save the change, **No** to keep the original setting.

   The **Service Status** window is displayed again.
5. To return to the Hardware Management Console Workplace, click **Cancel**.

Disable service status

To disable the service status for one or more systems:

1. Select a system or systems from the names in the table (a checkmark appears in the **Select** column).
2. From the **Options** drop-down menu, select **Disable service status**.

   The **Service Status** column in the list displays **Disabled** to indicate that the service status is disabled for the selected system or systems.
3. To save the settings currently displayed in the list, click **Save**.

   A message panel is displayed verifying you want the setting to be changed.
4. Click **Yes** to save the change, **No** to keep the original setting.

   The **Service Status** window is displayed again.
5. To return to the Hardware Management Console Workplace, click **Cancel**.

Display error message

To display a more detailed error message about the service status for a systems:

1. Select a system or systems from the names in the table that indicates an error message (a checkmark appears in the **Select** column).
2. From the **Options** drop-down menu, select **Display error message**.

   The **Failure Details** window displays a detailed explanation of the error and what steps should be taken to correct it.
3. Click **OK**.

   The **Service Status** window displays again.
4. To return to the Hardware Management Console Workplace, click **Cancel**.

Set Power Cap

Accessing the Set Power Cap task

This task allows you to limit the peak power consumption of a system resource or group of resources. You can closely manage power allocations within the physical limits of your data center.

The actions you can perform on the system resources from this task include:

- Selecting the Power Capping setting
- Setting the Cap Value
- Viewing power capping details on default and hidden columns

To set the power cap:

1. Select a system.
2. Open the **Set Power Cap** task. The Set Power Cap window is displayed. The window lists the current power capping settings and power cap values for the object.
3. Select the power capping setting from the **Power Capping** drop-down list.
4. Specify the power cap in the **Cap Value (Watts)** field.
5. Click **OK** to complete the task.

Set Power Cap

Use this task to limit the peak power consumption of a system component or group of components. You can closely manage power allocations within the physical limits of your data center.

You can work with the table by using the table icons or **Select Action** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The icons and list actions perform the following functions:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want. Click **OK** when you have defined your filter. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns. When you have completed the configuration and you want to save the settings, click **OK**. Otherwise, click **Cancel** and your changes will not be saved.

This window displays all components of the system. However, only components that support power capping are enabled. The same window is displayed regardless of how you launch the task. The actions you can perform on the system components include:

- Selecting the Power Capping setting
- Setting the **Cap Value**
- Viewing power capping details on default and hidden columns

The following information is available from the power capping table:

Name
Specifies the name of the object.

Type
Specifies the object type. The types available for power capping depend on your system configuration.

Power Capping
Select the power capping setting for the object from the drop-down list.

Note: This field is disabled and will default to **Not Supported** if power capping is not supported for this object.

Cap Value (Watts)
Enter the current cap value for the object in watts (W). The current cap value indicates the power budget for the selected object and must be within the **Cap Value Range**. This field may be automatically set, if under group capping control. See Group Capping for more information.

Note: This field is disabled if power capping is not supported for this object.

Cap Value Range (Watts)
Specifies the minimum and maximum values for the **Cap Value** in watts (W). This defines the set of acceptable values for setting the power cap. There are special considerations for group capping. See Group Capping for more information.

Last Power Capping
Specifies the current **Power Capping** setting for the object.

Note: This column is hidden by default. Use **Column Configuration** to display this column.

Last Cap Value (Watts)
Specifies the current **Cap Value** for the object in watts (W). The **Last Cap Value** indicates the active power budget for the selected object. When the task is initially opened, this is the same as the **Cap Value**.

Note: This column is hidden by default. Use **Column Configuration** to display this column.

Location
Specifies the location of the object.

Serial
Specifies the serial number of the object.

MTM
Specifies the machine type and model number of the object.

Note: If you are not entitled to access the **Set Power Capping** task, all rows of the table will be disabled.

Additional functions from this window include:

OK
To save the power capping settings for this system, click **OK**.

Apply
To save the power capping settings for this system and continue customization, click **Apply**.

Note: This option is grayed out until a change is made within this window.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Power Capping

Select the power capping setting from the **Power Capping** drop-down list. The possible settings include:

Disabled
The power cap of the object is not set, and the peak power consumption is not limited.

Enabled
The peak power consumption of the object is limited to the current **Cap Value**. When this setting is selected for system objects, all components of the object available for power capping are capped to limit the peak power consumption. Use this setting to enable group capping.

Custom
You can individually configure the components of the object for power capping. You can also use this setting to disable power capping for a system but retain the individual **Power Capping** setting and **Cap Value** for the objects within the system.

Note: This setting is available only for system objects.

For more information on group capping, see Group Capping.

Note: This field is disabled and will default to **Not Supported** if power capping is not supported for this object.

Last Power Capping

Specifies the current power capping setting of the object. When the task is initially opened, this is the same as the **Power Capping** setting. The possible settings include:

Disabled
The power cap of the object is not set, and the peak power consumption is not limited.

Enabled
The peak power consumption of the object is limited to the current **Cap Value**. For system objects, all components of the object available for power capping are capped to limit the peak power consumption.

Custom
You can individually configure the components of the system for power capping.

Note: This setting is available only for system objects.

For more information on group capping, see Group Capping.

Note: This column is hidden by default. Use **Column Configuration** to display this column.

Group Capping

A group is composed of an object that contains another object and the object or objects it contains. For example, a group might be a CPC that contains a zCPC. The following are important concepts regarding group power capping:

- Group caps replace individual object caps--that is, the **Cap Value** of a group supersedes the power cap of any object contained within the group.
- You can enable group capping by setting the **Power Capping** setting of the group to **Enabled**.
- You can change individual **Cap Value**s if the object is under group capping control. Customizing the individual **Cap Value** within a group, will automatically change the **Power Capping** setting to **Custom** for the group.
- If a group contains an object that does not support power capping, the **Power Rating** is used in calculating the minimum power cap value for the group. The **Power Rating** can be found on the details window for an object.
- The maximum **Cap Value** for a group is the sum of the **Power Rating** of all group objects.
- When a group component is powered off or removed, the group cap is redistributed to the remaining group components.
- To disable group capping without changing the individual power caps of the group members, change the **Power Capping** setting of the group to **Custom**.

Set Power Saving

Accessing the Set Power Saving task

This task allows you to reduce the average energy consumption of a system component or group of components. You can closely manage power allocations within the physical limits of your data center.

Note: When the power save mode is active some upgrade options are not available for the **Perform Model Conversion** task.

To set power saving:

1. Select a system.
2. Open the **Set Power Saving** task. The Set Power Saving window is displayed. The window lists the current power saving settings for the object.
3. Specify the power saving setting for the systems resources in the **Power Saving** list
4. Click **OK** to complete the task.

Note: You can set the power saving setting of the zCPC to **Low power** only one time per calendar day. This field is disabled and set to **Not Supported** if the current zCPC power saving setting is **High performance** but the zCPC has already entered **Low power** once within the calendar day.

Set Power Saving

Use this task to reduce the average energy consumption of a system component or group of components. You can closely manage power allocations within the physical limits of your data center.

This window displays all components of the system. However, only components that support power saving are enabled. The same window is displayed regardless of how you launch the task.

The following information is available from the power saving table:

Name
Specifies the name of the object.

Type
Specifies the object type. The types available for power saving depend on your system configuration.

Power Saving
Select the power saving setting for the object.

Note: This field is disabled and will default to **Not Supported** if power saving is not supported for this object.

Last Power Saving
Specifies the last power saving setting for the object. When the task is initially opened, this is the same as the **Power Saving** setting.

Note: This column is hidden by default. Use **Column Configuration** to display this column.

Location
Specifies the location of the object.

Serial
Specifies the serial number of the object.

MTM
Specifies the machine type and model number of the object.

Note: If you are not entitled for the **Set Power Saving** task, all rows of the table will be disabled.

Additional functions are available from this window:

OK
To save the power saving settings for this system, click **OK**.

Apply
To save the power saving settings for this system and continue customization, click **Apply**.

Note: This button is grayed out until a change is made within this window.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Power Saving

Select the power saving setting from the **Power Saving** list. Power saving reduces the energy consumption of a system. The possible settings include:

High performance
The power consumption and performance of the object are not reduced. This is the default setting.

Low power
The performance of the object is reduced to allow for low power consumption. When this setting is selected for system objects, all components of the object enabled for power saving have reduced performance to allow for low power consumption. Use this setting to enable group power saving.

Note: When configuring the power saving setting for systems cooled by forced-air, you can only set the power saving setting of the zCPC to **Low power** one time per calendar day. This field will be disabled and set to **Not Supported** if the current zCPC power saving setting is **High performance** but the zCPC has already entered **Low power** once within the calendar day.

Custom
Use **Custom** to disable group power saving and individually configure the components of the object for power saving.

Note: This setting is available only for system objects.

For more information on group power saving, see Group Power Saving

Note: This field is disabled and set to **Not Supported** for objects that do not support power saving.

Group Power Saving

A group is composed of an object that contains another object and the object or objects it contains. For example, a group might be a CPC that contains a zCPC . The following are important concepts regarding group power saving:

- Group power saving settings replace individual object settings--that is, the **Power Saving** setting of a system supersede the **Power Saving** setting of any object contained within the system.
- You can enable group power saving by setting the **Power Saving** setting of the system to **Low power** or **High performance**.
- You can change individual **Power Saving** settings if the object is under group power saving control. Customizing the individual **Power Saving** settings within a system, will automatically change the **Power Saving** setting to **Custom** for the system.
- To disable group power saving without changing the individual **Power Saving** settings of the group members, change the **Power Saving** setting of the system to **Custom**.

Show LED

Accessing the Show LED task

Show LED is a channel operation you can use to find the location of the jack and card slot in a cage. The light emitting diode (LED) is located below each card slot and near each jack in the cages that support attachment hardware. You can use this task for channel problem determination.

To set the show LED on:

1. Locate the **Channel** or **Channel path** that you want the LED on for.
2. Open the **Show LED** task.

   The Show LED window displays the PCHID for the LED that is on.
3. Click **OK** to turn the LED off.

Single Object Operations

Accessing the Single Object Operations task

- The following steps are used when trying to determine the correct authorization level used for the Single Object Operations session:
  - If a user ID is created on a Hardware Management Console Version 2.15.0 and that user ID is not on the targeted Support Element Version 2.15.0, then a new user ID is created dynamically for the Support Element. The Support Element user ID, that is created, is based on the HMC user ID (including the HMC name) and similar permissions as the user ID on the Hardware Management Console. Thus, the naming convention that is previously used in the following table does not apply to Support Element Version 2.15.0. The user ID does not persist after the single object operation and it does not appear in tasks such as **User Management**. Also, since the user settings for these users are initially created from the Hardware Management Console **User Settings** task, this task is only available on the Hardware Management Console for these users and is not available on the Support Element.
  - If the HMC user ID is defined on the target object with the same user name, then the authorization level for that target object user is used.
  - Otherwise, the authorization level of the user ID on the target object that corresponds to the "most powerful" task role that is associated with the HMC user ID is used. Or, if the HMC user ID matches a user pattern that is defined on the target object, then the authorization level for that user pattern will be used. (See “User Management” on page 1389 for more information on defining user patterns.) The "most powerful" task role is determined by comparing any predefined roles that the user has and predefined roles set in the "associated system defined user role" property of any custom roles that the user has.

    See Table 17 on page 1320 for the relationship between the "most powerful" Hardware Management Console task roles and the corresponding target object user IDs.

Table 17. Association between Hardware Management Console task roles and Support Element Version 2.14.1 and prior target object user IDs

Hardware Management Console Task Roles (descending order of "most powerful")	**Support Element Version 2.14.1 and prior target object user IDs** **Note: These user IDs cannot be modified.**
Access Administrator Tasks	SooAcsadmin
Service Tasks	SooService
System Programmer Tasks	SooSysprog
Advanced Operator Tasks	SooAdvanced
None of the above	SooOperator

- Only one direct connection, through this task, can be initiated at a time, and a maximum of four can be active at any one time. Only one Single Object Operations session can be active for any Support Element.

- If your Hardware Management Console (Version 2.10.0 or later) does not have a diskette drive, then any Support Element (Version 2.9.2 or earlier) task that tries to access the Hardware Management Console diskette drive will be redirected to access a USB flash memory drive.

This task creates a direct connection to a single object Support Element. You may need to connect to an individual Support Element to investigate and resolve exception situations. After a Single Object Operations session has been established, you can control the input to the Support Element or monitor the output of the Support Element by using the **Session** pull-down on the window.

Note: For all Support Elements, all change internal code function must be performed from the Hardware Management Console using the **Change Internal Code** task.

To establish a Support Element session from the Hardware Management Console:

1. Select a CPC (server).
2. Open the **Single Object Operations** task. The Single Object Operations Task Confirmation window is displayed.
3. Click **Yes** to proceed or **No** to go back to the Hardware Management Console workplace.
4. If you click **Yes**, the Support Element workplace is displayed and you can proceed with the appropriate tasks.

   Note: If the Support Element you attempt to connect to is already established, a message is displayed. You have the option to click **Close** and return to the Hardware Management Console workplace or you can click **Chat** to open the **Console Messenger** task and initiate a chat session with the user session on the Support Element.

   If the HMC and the target object are at Version 2.14.1, and another HMC has an established Single Object Operations session to the target object, then you have an additional option to **Disconnect remote userid**. When you select this option, the Confirm Forced Disconnect window is displayed. The HMC user must confirm to disconnect the specified user ID by clicking **Disconnect remote userid**. This disconnects the user ID but does not log it off.
5. Click the red **X** in the upper right corner of the workplace to end the session and go back to the Hardware Management Console workplace.

Single Step Console Internal Code

Accessing the Single Step Console Internal Code task

This task allows you to retrieve and apply, apply only or remove internal code on the Hardware Management Console.

To retrieve and apply, apply only or remove internal code on the Hardware Management Console:

1. Open the **Single Step Console Internal Code** task. The Single Step Console Internal Code window is displayed.
2. Select the Single Step Internal Code Change option that you want to perform and the backup location, if applicable, then click **OK**.

Single Step Console Internal Code

Use the Single Step Console Internal Code task to retrieve and apply, apply only or remove internal code on the Hardware Management Console (HMC).

The purpose of the Single Step Console Internal Code procedure is to:

- Determine whether to only apply internal code changes or to retrieve and apply internal code changes.
- Verify the system environment.
- Process a Backup Critical Data function.
- Accept all previously activated internal code changes (optional).
- Exclude the operational internal code changes from becoming permanent.

- Retrieve internal code changes from the support system, if retrieve and apply is the selected operation.
- Connect to the support system and verify the current status of all downloaded internal code changes.
- Install and activate the internal code changes.

The Single Step Console Internal Code function is also used to remove internal code changes as follows:

- Verify the machine environment.
- Remove and activate the accepted internal code change levels.

Select an action:

Retrieve and apply internal code changes
To back up critical hard disk information, accept the internal code changes (optional), retrieve internal code changes from the support system, and apply internal code changes, select **Retrieve and apply internal code changes**.

Apply internal code changes only
To back up critical hard disk information, accept internal code changes (optional), and apply pending internal code changes, select **Apply internal code changes only**.

Remove internal code changes
To remove internal code changes to resolve problems, select **Remove internal code changes**.

Do not accept activated code changes.
Single step accepts the currently activated internal code changes which makes the previous internal code changes permanent and clears up disk space that allows backups to run quicker. However, in the future, if you might want to remove some of the currently activated code changes, select **Do not accept activated code changes** so you can do a remove and activate to internal code levels that were previously activated.

If you selected to retrieve and apply or apply only the internal code on the HMC, select a backup location:

HMC USB media
To backup the HMC critical data to the HMC's USB flash memory drive, select **HMC USB media**. This is the default if a location is not selected.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP server
To store the backup data on an FTP server that is configured, select **FTP server**.

If you need to configure the FTP server, click **Configure FTP Server**. The Configure Backup Settings window is displayed. Provide the appropriate information, then click **OK**. You can proceed with this task by selecting the **FTP server** location.

Proceed with the following options to continue or cancel this task:

OK
To continue the task after you make your selections, click **OK**.

Cancel
To close the window without making any selections, click **Cancel**.

Help
To display help for the current window, click **Help**.

Single Step Internal Code Changes

Accessing the Single Step Internal Code Changes task

Notes:

- Before starting this task, make sure you have a formatted USB flash memory drive (with volume label of **ACTBKP**) available for backing up critical data.
- Single Step Internal Code Changes is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task allows you to retrieve and apply, apply only or remove internal code for one or more objects.

You can do any of the following:

- Choose to only apply internal code changes or to retrieve and apply internal code changes.
- Determine if pending internal code changes are disruptive. If so, you can choose to activate the changes concurrently or disruptively.
- Verify the system environment. In the case of a Support Element, it verifies that the most recent Alternate Support Element mirroring operation was successful and that a Service Required state does not exist.
- Perform a Backup Critical Data function.
- Accept all previously activated internal code changes (optional).
- Retrieve internal code changes from the support system.
- Connect to the support system and download any internal code change ***hold*** status for pending internal code changes.
- Connect to the support system to see if the status of any existing internal code changes has changed from non-disruptive to disruptive.
- Install and activate the internal code changes. You can apply this to all applicable internal code changes, a subset of its applicable internal code changes, or specify a bundle level number for internal code changes.
- Choose to retrieve and apply (or clone) internal code changes to match a saved clonable level.
- Choose to receive all code changes for your system regardless of the requirements for installing the next Engineering Change (EC) level.
- Trigger the Alternate Support Element mirroring operation.
- Transmit system availability data to the remote support system.

Certain internal code changes may require the MRU to shut down during the activation of the change. This is normal for these changes. This could cause a slight degradation in system performance during the time the MRU is shut down. After activation is complete, the MRU will be turned on again, and normal performance will be resumed.

To retrieve, apply or remove internal code:

1. Select one or more CPCs (servers).
2. Open the **Single Step Internal Code Changes** task. The Apply Single Step Internal Code Changes window is displayed.
3. Verify the objects that are listed and review the **Single Step Code Change Overview** information. If you want to proceed with the actions/defaults described in that window, click **Retrieve and Install...** to start the operation. Otherwise, if you have additional options that you want to perform for this task, click **Advanced...**.
4. Follow the instructions on the subsequent windows to complete the task, or click **Cancel** to end the task.

This task also allows you to retrieve and apply a previous saved level of internal code (clonable) from the support system. Before continuing with this task, you must have a saved level of internal code stored in the support system. For more information for creating a clonable level of internal code, see the **Define Clonable Internal Code Levels** task on the Support Element.

To retrieve and apply internal code changes to a Support Element to match a saved clonable level:

1. Select a CPC (server).
2. Open the **Single Step Internal Code Changes** task. The Apply Single Step Internal Code Changes window is displayed.
3. To access additional options, click **Advanced...**, the Apply Single Step Internal Code Changes window is displayed which includes additional options.
4. Select **Retrieve and apply (Clone) internal code changes to match a saved clonable level**, then click **OK**. The Retrieve Clonable Level Data window is displayed.
5. Specify the *serial number* of the Support Element where the internal code was saved from in the **Machine Serial Number** input field.
6. Specify the *name* that you gave to the clonable level of internal code in the **Clonable Level Name** input field.
7. Specify the *password* that you defined for this clonable level of internal code in the **Clonable Level Password** input field, then select **Retrieve Clonable Level Data**. The Single Step Internal Code Changes Apply Busy window is displayed while the system is retrieving the data from the support system.
8. Select **Apply Concurrent Internal Code Changes**. The Single Step Internal Code Changes Progress window is displayed. Wait for the task to complete; otherwise, follow the instructions on the subsequent windows.

Apply Single Step Internal Code Changes

This task is used to retrieve and apply, apply only or remove internal code for one or more objects.

Use this window to verify the objects and review the **Overview** information. The **Overview** information describes the actions (defaults) that will be applied to the objects when you click **Retrieve and Install...**.

You can also apply additional options by clicking **Advanced...**. At this point, you can either:

- Select the additional options you want applied to the objects and click **OK** to proceed, or
- Click **Cancel** to return to the main window and proceed with the actions (defaults) as described.

Objects
Lists the objects that will be affected by applying internal code changes.

Single Step Internal Code Change Overview
This portion of the window describes the functions of this task and what processes occur when it is executed.

To start the operation, click **Retrieve and Install...**. If you have additional options that you want to perform with this task, click **Advanced...**.

Retrieve and Install...
To proceed with this task using the current defaults, click **Retrieve and Install...**.

Using this option allows you to:

- Obtain any new internal code changes from the support system.
- Install all applicable changes to the selected systems.
- Determine if pending internal code changes are disruptive. If so, you can choose to activate the changes concurrently or disruptively.
- Verify the system environment. In the case of a Support Element, it verifies that the alternate Support Element mirroring operation was successful and that a Service Required state does not exit
- Perform a Backup Critical Data operation.
- Accept all previously activated internal code changes.
- Retrieve internal code changes from the support system.
- Install and activate the internal code changes.
- Trigger the alternate Support Element mirroring operation.

Advanced...
To display all the options available for this task, click **Advanced...**.

Using this option allows you to:

- Determine whether to only apply internal code changes or to retrieve and apply internal code changes.
- Determine if pending internal code changes are disruptive. If so, you can choose to activate the changes concurrently or disruptively.
- Verify the system environment. In the case of a Support Element, it verifies that the alternate Support Element mirroring operation was successful and that a Service Required state does not exist.
- Perform a Backup Critical Data operation.
- Accept all previously activated internal code changes (optional).
- Exclude the operational internal code changes from becoming permanent.
- Retrieve internal code changes from the support system.
- Connect to support system and download any internal code change Hold status for pending internal code changes.
- Connect to the support system to see if the status of any existing internal code changes has changed from nondisruptive to disruptive.
- Install and activate the internal code changes.
- Retrieve and apply (or clone) internal code changes to match a save clonable level.
- Receive all code changes for your system regardless of the requirements for installing the next Engineering Change (EC) level.
- Transmit system availability data to the remote support system.
- Trigger the Alternate Support Element Mirroring operation.

This option is also used to remove internal code changes as follows:

- Determine if removing internal code changes is disruptive. If so, you can choose to activate the changes concurrently or disruptively.
- Verify the machine environment. In the case of a Support Element, it verifies that the alternate Support Element mirroring operation was successful and that a Service Required state does not exist.
- Remove and activate internal code change levels. The object will then be running at the accepted internal code change level.
- Trigger the alternate Support Element mirroring operation.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Apply Single Step Internal Code Changes - Advanced options

Use this window to choose whether you want to retrieve and apply, apply only or remove internal code for one or more objects.

When the object is the Support Element, this window identifies the Support Elements on which to apply or remove internal code changes.

Objects
Lists the objects that will be affected by applying or removing internal code changes.

Retrieve and apply internal code changes
To back up critical hard disk information, accept the internal code changes (optional), retrieve internal code changes from support system and apply them to your object, and in the case of the Support Element object, trigger the alternate Support Element mirroring operation, select **Retrieve and apply internal code changes**.

Retrieve and apply (Clone) internal code changes to match a saved clonable level
(This selection appears if the target of the operation is a single Support Element and it supports the operation.)

To back up critical hard disk information and retrieve a previously saved clonable level of internal code changes from support system and apply them to your object, select **Retrieve and apply (Clone) internal code changes to match a saved clonable level**.

Apply internal code changes only
To back up critical hard disk information, accept internal code changes (optional), apply pending internal code changes, and in the case of the Support Element object, trigger the alternate Support Element mirroring operation, select **Apply internal code changes only**.

Remove internal code changes
To remove internal code changes, and in the case of the Support Element object, trigger the alternate Support Element mirroring operation, select **Remove internal code changes**.

Accept execution phase to be excluded
To *not* make the operational internal code changes permanent, select **Accept execution phase to be excluded**. Otherwise, the previously applied internal code changes are accepted and permanent.

Include internal code changes...
To receive all code changes for your system regardless of the requirements for installing the next Engineering Change (EC) level, select **Include internal code changes which will inhibit the Concurrent Upgrade Engineering Changes (EC) task from being used to apply the next Licensed Internal Code EC level**.

OK
After you select one of the Single Step Internal Code Change options, click **OK**.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Retrieve Clonable Level Data

Use this window to provide the required information to retrieve any clone data saved for the processor from which you wish to clone.

CPC serial number
Specify the permanent identifier of the machine from which the clonable level of code changes was saved. This serial number is 12 characters long and much be filled in completely.

Clonable level name
Specify the name assigned to a previously saved clonable level of code changes. The name is restricted to the alphanumeric set of characters.

Clonable level password
Specify a 12-character alphanumeric password, which, when entered, displays "*"s for each character that you specified.

Retrieve Clonable Level Data
To retrieve clonable level data after specifying the appropriate information, click **Retrieve Clonable Level Data**. A busy window displays while the system sends a Get Clonable Level transaction to the support system.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Apply Single Step Internal Code Changes - Concurrent

Use this window to activate the changes concurrently. *Concurrent* code changes can be activated without disrupting system activity on the selected objects.

Objects
Lists the objects to which internal code changes will be applied after retrieval.

Apply Concurrent Internal Code Changes
To apply the concurrent internal code changes, click **Apply Concurrent Internal Code Changes**.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Apply Single Step Internal Code Changes - Disruptive

Use this window to choose to activate the changes disruptively. Activating *disruptive* internal code changes will disrupt operating system activity on the Central Processor Complex (CPC).

Objects to shut down
Lists the objects that should be shut down before applying disruptive code changes.

Objects to change
Lists the objects to which disruptive code changes will be applied.

Apply Disruptive Internal Code Changes
To apply disruptive internal code changes, click **Apply Disruptive Internal Code Changes**.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Single Step Internal Code Changes Apply

Use this window to confirm or cancel your request to apply disruptive internal code changes.

Objects
Lists the objects to which disruptive internal code changes will apply.

Apply concurrent internal code changes only
Applies only concurrent internal code changes, not disruptive internal code changes.

Apply both concurrent and disruptive internal code changes
Applies both concurrent and disruptive internal code changes, not simply concurrent internal code changes.

OK
To confirm your request to apply internal code changes (which may include disruptive changes), click **OK**.

Cancel
To close this window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove Single Step Internal Code Changes - Concurrent

Use this window to confirm or cancel your request to remove concurrent code changes.

Confirm your request to remove concurrent internal code changes only if it is necessary to resolve a problem that occurred after installing and activating the current changes.

Objects
Lists the objects from which internal code changes will be removed.

Remove Concurrent Internal Code Changes
To remove concurrent internal code changes, click **Remove Concurrent Internal Code Changes**.

Cancel
To close this window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove Single Step Internal Code Changes - Disruptive

Use this window to confirm or cancel your request to remove disruptive code changes.

Confirm your request to remove disruptive internal code changes only if it is necessary to resolve a problem that occurred after installing and activating the current changes.

Objects to shut down
Lists the objects that should be shut down before removing disruptive internal code changes.

Objects to change
Lists the objects from which disruptive internal code changes will be removed.

Remove Disruptive Internal Code Changes
To remove disruptive internal code changes, click **Remove Disruptive Internal Code Changes**.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Single Step Internal Code Changes Remove

Use this window to confirm or cancel your request to remove disruptive internal code changes.

Objects
Lists the objects to which disruptive internal code changes will be applied.

Remove concurrent internal code changes only
Removes only concurrent internal code changes, not disruptive internal code changes.

Remove both concurrent and disruptive internal code changes
Removes both concurrent and disruptive internal code changes, not simply concurrent internal code changes.

OK
To confirm your request to remove internal code changes (which may include disruptive changes), click **OK**.

Cancel
To close this window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Special Code Load

Accessing the Special Code Load task

Notes:

- You cannot perform this task remotely.

- Special Code Load is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task is used when you want to preload a new CPC internal code level on the alternate Support Element while the remainder of the system is running.

To upgrade to Version Code 1.6.0 or later:

1. Select one or more CPCs (servers).
2. Open the **Special Code Load** task. The Confirm the Action window is displayed.
3. Install the Support Element microcode (CD-ROM) in the Hardware Management Console CD-ROM drive and click **OK**. Follow the rest of the directions shipped with your upgrade package.

Start (DPM)

Accessing the Start task

This task starts a stopped system or partition on which Dynamic Partition Manager (DPM) is enabled.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

To start a stopped DPM system or partition:

1. Select a stopped DPM system, or one or more stopped partitions.

   Note: You cannot mix your selection of systems and partitions.
2. Open the **Start** task.

   If the DPM R3.1 storage management feature or a later DPM version has been applied to the system, and one or more of the partitions to be started have attached storage groups that are being configured or modified, a warning message is displayed. The warning message includes the name of the affected partitions. The Start task does not continue until you make a selection.

   - Select **YES** to allow the affected partitions to be started.
   - Select **NO** to cancel the start operation for only the affected partitions.

   The Start window contains the following controls and information.

   Progress bar
   The overall total progress bar shows an aggregated status of all targeted partitions or the progress of the targeted system for this task instance.

   Note: The total system progress bar should be equal to the **Progress** column of the system in the table.

   Table
   Displays a tree-table for a targeted system followed by all the partitions configured to be started automatically with the system, displaying their individual progress. It can also display a list of targeted partitions with the associated system and individual progress. The Actions menu and row menu contain the following items for managing the table:

   Actions menu or toolbar icon
   Use the Actions menu or select an icon on the toolbar for your options.

   Partition Details
   To display the Partition Details window for each selected target, select **Partition Details**. This selection is enabled when one or more rows are selected.

   System Details
   To display the System Details window for the targeted system or each selected target's system (one per CPC), select **System Details**. This selection is enabled when one or more rows are selected.

Open Console
To open the **Open ASCII Console** task in a new window for the selected targets, select **Open Console** or click the toolbar icon. This selection is enabled when one or more rows are selected.

OS Messages
To open the **Operating System Messages** task in a new window for the selected targets, select **OS Messages**. This selection is enabled when one or more rows are selected.

Retry
To restart this function on the selected targets, which resets the progress, select **Retry** or click the toolbar icon. This selection is enabled when one or more targets that are in a failure state are selected.

Cancel
To cancel this function on the selected targets, removing their progress, select **Cancel** or click the toolbar icon. Initially, **Cancelling** is displayed in the Details column. When the function completes, **Cancelled** is displayed in the Details column. If the cancel fails, then an error message is displayed. This selection is enabled when one or more targets in a cancelable state are selected.

Monitor System
To monitor the system, select **Monitor System** or click the toolbar icon. This option brings the main user interface (UI) to the foreground, select the targets' system from the Navigation area and then select the **Monitor** tab in the work area. **Monitor System** is enabled when one or more targets are selected for the same system, and is disabled if partitions from different systems are selected.

Table columns
A description of the table columns for the systems or partitions follows.

Select
You can select one or more table entries.

Target
Displays the system or partition name as a hyperlink. To open **System Details** or **Partition Details** in a new task window, click the appropriate link.

Partition
Displays the partition name as a hyperlink. To open **Partition Details** in a new task window, click this link.

System
Displays the system name on which the partition resides as a hyperlink. To open **System Details** in a new task window, click this link.

Progress
Displays a progress bar identifying the percentage of progress for partitions waiting to start, partitions in the process of starting, and partitions that have started. The percentage is based on the amount of steps performed on the function and not on the amount of time.

Details
Displays the name of the step currently being performed, or content that describes the outcome of the operation. If the DPM R3.1 storage management feature or a later DPM version has been applied to the system, the Details column contains messages that indicate the outcome. Otherwise, the Details column contains one of the following icons and labels, with a clickable **Details** link that identifies the failed partitions and provides a message that explains the failure.

- **Success** indicates partitions that have started.
- **Failed** indicates partitions that failed to start.
- **Cancelled** indicates partitions for which the start operation was canceled.

Depending on the outcome of the start operation for a partition, additional messages might be displayed in the Details column.

- The **Open Console** link opens the console task through which you can log in to the operating system that is running on the partition.
- The Secure Service Container Web Interface Communication link opens a web browser, using the host name or IP address that is specified for a partition with the type Secure Service Container.
- Only when an administrator has created one or more network interface cards (NICs) with associated VLAN IDs for a new or modified partition, the Details column includes a list of those network devices. The list includes each NIC device number and the associated VLAN ID to be used when configuring the device on the operating system that the partition hosts.
- If the message Maximum Number of Partitions is displayed, the storage groups that are attached to the started partition are already in use by the maximum number of active partitions. This message means that storage is not available for the partition to use. In this case, go to the Storage section of the **Partition Details** task, and attach more storage groups to the partition.
- If the message No Boot Volume is displayed, an operating system or hypervisor cannot be started on this partition. In this case, go to the Storage section of the **Partition Details** task, and attach a storage group that contains a boot volume on which the executables for the operating system or hypervisor reside.

Close

When the task is complete, click **Close**. This option is not enabled until all the targets reach their final state of this function, which is either a failure, canceled, or 100% completed.

Note: In the case of a retry on a failed target, the close option is disabled again if it became enabled. If you click the task window's red X, the window either reopens to its current state if it is not completed or closes the task if it is completed.

3. When you complete this task, click **Close**.

Start All Processors

Accessing the Start All Processors task

Note: Start All Processors is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task ends instruction stop state for selected CPC images (except for a coupling facility image) that were previously stopped. This causes instruction processing to begin.

To start CPC images:

1. Select a CPC image.
2. Open the **Start All Processors** task. The Start All Processors Task Confirmation window is displayed.
3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
4. To continue with the start, click **Yes**. The Start All Processors Task Progress window is displayed indicating the progress of the start and the outcome.
5. Click **OK** to close the window when the start completes successfully.

   Otherwise, if the stop does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Stop (DPM)

Accessing the Stop task

This task stops a started system (or partitions) on which Dynamic Partition Manager (DPM) is enabled.

Notes:

- This task is available only when one or more managed systems have DPM enabled.
- Stop is considered a disruptive task. If the target is locked, you must unlock it before continuing.

To stop a started DPM system or partition:

1. Select a started DPM system, or one or more started partitions.

   Note: You cannot mix your selection of systems and partitions.

2. Open the **Stop** task. The "Confirm Disruptive Action" on page 1333 window is displayed. When you have agreed to continue with the task, the Stop window is displayed. The details of the window include the following information:

   Progress bar
   The overall total progress bar shows an aggregated status of all targeted partitions or the progress of the targeted system for this task instance.

   Note: The total system progress bar should be equal to the **Progress** column of the system in the table.

   Table
   Displays a tree-table for a targeted system followed by all the partitions configured to be started automatically with the system, displaying their individual progress. It can also display a list of targeted partitions with the associated system and individual progress. The Actions menu and row menu contain the following items for managing the table:

   Actions menu or toolbar icon
   Use the Actions menu or select an icon on the toolbar for your options.

   Partition Details
   To display the Partition Details window for each selected target, select **Partition Details**. This selection is enabled when one or more rows are selected.

   System Details
   To display the System Details window for the targeted system or each selected target's system (one per CPC), select **System Details**. This selection is enabled when one or more rows are selected.

   Cancel
   To cancel this function on the selected targets, removing their progress, select **Cancel** or click the toolbar icon. Initially, **Cancelling** is displayed in the Details column. When the function completes, **Cancelled** is displayed in the Details column. If the cancel fails, then an error message is displayed. This selection is enabled when one or more targets in a cancelable state are selected.

   Monitor System
   To monitor the system, select **Monitor System** or click the toolbar icon. This option brings the main user interface (UI) to the foreground, select the targets' system from the Navigation area and then select the **Monitor** tab in the work area. **Monitor System** is enabled when one or more targets are selected for the same system, and is disabled if partitions from different systems are selected.

   Table columns
   A description of the table columns for the systems or partitions follows.

   Select
   You can select one or more table entries.

   Target
   Displays the system or partition name as a hyperlink. To open **System Details** or **Partition Details** in a new task window, click the appropriate link.

   Partition
   Displays the partition name as a hyperlink. To open **Partition Details** in a new task window, click this link.

System
Displays the system name on which the partition resides as a hyperlink. To open **System Details** in a new task window, click this link.

Progress
Displays a progress bar identifying the percentage of progress for partitions waiting to stop, partitions in the process of stopping, and partitions that have stopped. The percentage is based on the amount of steps performed on the function and not on the amount of time.

Details
Displays the name of the step currently being performed, or content that describes the outcome of the operation. If the DPM R3.1 storage management feature or a later DPM version has been applied to the system, the Details column contains messages that indicate the outcome. Otherwise, the Details column contains one of the following icons and labels, with a clickable **Details** link that identifies the failed partitions and provides a message that explains the failure.

- **Success** indicates partitions that have stopped.
- **Failed** indicates partitions that failed to stop.
- **Cancelled** indicates partitions for which the stop operation was canceled.

Close
When the task is complete, click **Close**. This option is not enabled until all the targets reach their final state of this function, which is either a failure, canceled, or 100% completed.

Note: In the case of a retry on a failed target, the close option is disabled again if it became enabled. If you click the task window's red X, the window either reopens to its current state if it is not completed or closes the task if it is completed.

3. When you complete this task, click **Close**.

Confirm Disruptive Action

This window is used to confirm that you want to stop a started system or partition. If a system is targeted, this window displays any partitions on the system that are not stopped; otherwise, this window displays the targeted partitions.

Note: If necessary, you might be required to provide confirmation text input for each object and you might also be required to provide your password. These additional requirements ensure that you want to continue with the disruptive task.

The following information is provided in this table:

Name
Specifies the name of the system or partition that is being disrupted by the **Stop** task that is being executed. This name is displayed as a hyperlink. You can click the name to open the Partition Details window.

System
Specifies the system that is associated with the disrupted partition. This name is displayed as a hyperlink. You can click the system to open the System Details window.

Status
Specifies the status of the disrupted partition.

OS Name
Specifies the associated operating system name that is associated with the disrupted partition.

Confirmation Text
Provide the operating system name (**OS Name**) (preferred, if available) or the **Name** as input to the **Confirmation Text** fields. You can type the name in the field or copy the name from the table and paste it into the input area. If the confirmation text requirement is disabled for your user ID, then this field is not displayed.

Password confirmation input
Use this input field to specify your user ID password to continue with the disruptive task.

Note: If your user ID does not require a password to continue with the disruptive task, then this input field is not available.

Proceeding with a disruptive task can have severe effects. You are required to confirm the execution of the task by specifying your user ID password in this input field. When you provide the correct password, then **Stop System** or **Stop Partitions** is enabled and you can proceed with the disruptive task.

Some additional functions on this window include:

Stop System (or Partitions)
To proceed with this disruptive action, click **Stop System** or **Stop Partitions**.

Cancel

- To close the window without saving any changes and cancel the stop operation, click **Cancel**.
- If the changes you made did not get saved, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Stop All Processors

Accessing the Stop All Processors task

Note: Stop All Processors is considered a disruptive task. If the object is locked, you must unlock it before continuing.

This task places all selected CPC images (except for a coupling facility image) in an instruction stop state. This changes the operational status to **Stopped**.

To stop CPC images:

1. Select a CPC image.
2. Open the **Stop All Processors** task. The Stop All Processors Task Confirmation window is displayed.
3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
4. To continue with the stop, click **Yes**. The Stop All Processors Task Progress window is displayed indicating the progress of the stop and the outcome.
5. Click **OK** to close the window when the stop completes successfully.

   Otherwise, if the stop does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Storage Information

Accessing the Storage Information task

The model of your system determines the minimum, standard, and maximum storage capacity of the central processor complex (CPC).

Total Installed storage is part of the CPC's hardware configuration; it is provided by one or more storage cards physically installed in the CPC. *Allocated storage* is installed storage that is in use for a specific purpose:

- The *Customer Storage* is storage amount that is available to your system.
- The *Hardware System Area (HSA)* is storage only the CPC can use. It stores the CPC's licensed internal code and input/output (I/O) definition while the CPC is activated.
- *Virtual Flash Memory* is main memory.

- *Central Storage* includes main storage and internal disk subsystem cache. Operating systems and applications can use main storage; only the CPC can use the cache.

Storage is allocated to a CPC when it is activated.

When the CPC is activated, much of the storage allocated to the CPC can be allocated to the logical partitions activated on it:

- The central storage allocated to the CPC is the central storage initially available to logical partitions.
- The virtual flash storage allocated to the CPC is the virtual storage initially available to logical partitions.

Like the CPC, storage is allocated to a logical partition when it is activated. So to allocate storage to the CPC or a logical partition, you must customize the activation profile you use to activate it.

To review the current storage allocations:

1. Open the **Storage Information** task.
   - Page tabs along the top of the window identify its pages. Select a page tab to display that page.
   - The first page of the window displays information about storage installed and allocated for the CPC. Its page tab is labeled: Base System Storage Allocation.
   - If the CPC is activated, the window includes a second tab that displays information about storage allocated for logical partitions currently activated on the CPC. Its page tab is labeled: Logical Partition Storage Allocation.

Storage Information

This window displays:

- Information about storage installed and allocated for the base system.
- Information about central storage and virtual flash memory storage allocated for logical partitions currently activated on the base system.

Information about storage installed and allocated for the base system and central storage allocated for activated logical partitions is displayed in the tabbed views.

Base system storage allocation
Displays information about storage installed and allocated for the base system.

Logical partition storage allocation
Displays information about central storage and virtual flash memory allocated for logical partitions currently activate on the base system.

Additional functions on this window include:

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Base System Storage Allocation

Use this window to view the storage configuration information for the central processor complex (CPC). This storage information reflects what is currently allocated.

Total Installed Storage

Displays the amount of storage, in megabytes, that is installed. The installed storage is the total of central storage plus customer storage.

Customer Storage
Displays the amount of storage, in megabytes, allocated for main storage..

Hardware System Area (HSA)
Displays the amount of memory reserved for the base hardware system area (HSA).

Virtual Flash Memory (VFM)

Entitled
Displays the amount of Virtual Flash Memory that is allowed for your system. Entitled Virtual Flash Memory is the amount of Virtual Flash Memory that is licensed for use, which might be less than the total amount that is installed on the system.

Allocated
Displays the amount of Virtual Flash Memory that is allocated, which is the total Virtual Flash Memory assigned to all active and reserved partitions on the system.

Customer Storage Details

Storage Type

Central Storage
Displays the amount of storage, in megabytes and percentage, allocated for main storage and the hardware system area.

Available Storage

Available Storage is the amount of storage initially available to logical partitions. When the CPC is activated, available storage is the amount of storage allocated to the CPC *excluding* the amount allocated for the CPC's hardware system area (HSA). Afterward, the amount of available storage:

- Decreases whenever an inactive logical partition is activated.
- Decreases whenever unused storage is dynamically reconfigured *ON* to a logical partition for which the storage was reserved.
- Increases whenever unused storage is dynamically reconfigured *OFF* from a logical partition for which the storage was reserved.
- Increases whenever an active logical partition is deactivated.

Logical Partition Storage Allocation

This page displays information about central storage and Virtual Flash Memory allocated for logical partitions currently activated on the base system.

The *Base System* is the central processor complex (CPC). When the CPC is activated in LPAR mode, the input/output configuration data set (IOCDS) used to define the CPC's input/output (I/O) definition also identifies the logical partitions that can be activated on the CPC.

When logical partitions are activated, their central storage and Virtual Flash Memory are allocated from the CPC's available storage.

Available Storage is the amount of storage initially available to logical partitions. When the CPC is activated, available storage is the amount of storage allocated to the CPC *excluding* the amount allocated for the CPC's hardware system area (HSA). Afterward, the amount of available storage:

- Decreases whenever an inactive logical partition is activated.
- Decreases whenever unused storage is dynamically reconfigured *ON* to a logical partition for which the storage was reserved.
- Increases whenever unused storage is dynamically reconfigured *OFF* from a logical partition for which the storage was reserved.
- Increases whenever an active logical partition is deactivated.

Input/Output configuration data set (IOCDS)
Displays the identifier and name of the IOCDS used during power-on reset to define the CPC's I/O definition and to identify the logical partitions that can be activated on the CPC.

Central Storage Allocation (MB)

Displays information about how addressable central storage is used for storage allocated to logical partitions currently activated on the central processor complex (CPC). All storage amounts are displayed in megabytes (MB).

Central storage is main storage that operating systems or applications can use. The central storage allocated to a logical partition upon activation is its *initial central storage*. If a logical partition supports dynamic storage reconfiguration, additional central storage reserved for it upon activation is its *reserved storage*. Afterward, if the reserved central storage is not already being used by another logical partition, it can be dynamically reconfigured to the logical partition.

The amounts of initial and reserved central storage are set in the activation profiles used to activate the logical partitions. The storage is also arranged according to information in the activation profiles.

The central storage allocation changes with each activation and deactivation of a logical partition, and whenever unused storage is dynamically reconfigured.

Name
Displays the logical partition's name.

Origin
Displays the offset, from the beginning of central storage addressability, at which central storage for the logical partition begins.

Note: The origin is an offset, *not* an address. So a central storage origin of 2048 MB, for example, indicates the logical partition's central storage addressability begins 512 megabytes from the beginning of central storage addressability.

Initial
Displays the amount of central storage allocated to the logical partition during the most recent activation.

Current
Displays the amount of central storage currently allocated to the logical partition.

If the logical partition supports dynamic storage reconfiguration, this amount is the sum of its initial central storage and any amounts dynamically reconfigured to it from its reserved storage.

Otherwise, this amount is always the same as the initial storage amount.

Maximum
Displays the maximum amount of central storage that can be allocated to the logical partition.

If the logical partition supports dynamic storage reconfiguration, this amount is the sum of the initial central storage and reserved central storage allocated to the logical partition during the most recent power-on reset.

Otherwise, this amount is the same as the initial central storage amount.

Gap
Displays the amount of unused central storage addressability between the end of the central storage addressability for one logical partition and the beginning of the central storage addressability for the next logical partition.

The unused storage may end either at the beginning of central storage allocated to another logical partition, or at the end of central storage.

Virtual Flash Memory (GB)

Name
Displays the logical partition's name.

Initial
Displays the amount of Virtual Flash Memory allocated to the logical partition during the most recent activation.

Current
Displays the amount of Virtual Flash Memory currently allocated to the logical partition element.

Maximum
Displays the maximum amount of Virtual Flash Memory currently allowed for the logical partition.

System Details

Accessing the System Details task

Use this task to view or modify the properties of a system.

Perform the following steps to display and optionally modify the System details:

1. Select the system, and then open the **System Details** task. The System Details window is displayed.
2. Modify the editable fields as you want.
3. Click **Apply** to save the changes.

System Details

This window displays the following information for the selected central processor complex (CPC):

- Instance Information includes the current status of the CPC and other information about the operating conditions, characteristics, and settings of the CPC.

  Review the information under **Instance information**. Optionally, click **Change Options...** to change the activation profile used for activating the CPC from the group specified in the Group field.
- Acceptable Status settings determine which CPC statuses are acceptable. The Hardware Management Console reports when the CPC status becomes unacceptable.

  Review the settings on the **Acceptable Status** page. Optionally, make setting selections, and click **Apply** to change the acceptable status settings.
- Product Information is assigned to machines and CPCs when they are manufactured, primarily for the purpose of identifying them.
- Network Information includes SNA, node ID, primary, alternate, and network mask addresses for the CPC.
- STP Information displays the Server Time Protocol (STP) information for the CPC.

  Note: This tab is available only when STP is enabled and the selected CPC is in an operating state.
- Degrade Reasons indicates the CPC has a degraded status.

  Note: This tab is available only when an object is in a degraded state.
- Busy Status specifies the reason the CPC object is busy.

  Note: This tab is available only when an object is busy.
- “Energy Management” on page 1345 specifies power and thermal monitoring information.

  Note: Certain information on this tab is available only when the appropriate feature is installed.
- Security (“System BCPii Permissions” on page 1348) to enable BCPii permission settings for the system.

This window also displays product information about the CPC and the machine in which it is located. A *machine* is a particular configuration of hardware designed to provide particular operational capabilities and characteristics.

Additional functions on this window include:

OK
To save changes you made to the acceptable status settings of the system and close the window, click **OK**.

Apply
To save changes you made to the acceptable status settings of the system, click **Apply**.

Change Options...
To change the activation profile used for activating this instance of the CPC from the selected group, click **Change Options**. You can have different activation profiles set for a single system by opening the **System Details** task from different system defined or user-defined custom groups containing the object and selecting **Change Options...**.

The **Change Options...** button is not available if the **System Details** task is invoked from Tasks Index. It is also not available if the user does not have permission to the **Change Object Options** task. Your access administrator can grant permission to the **Change Object Options** task by using the **User Management** task.

Cancel
To close the window without saving changes you made to the acceptable status settings of the system, click **Cancel**.

Help
To display help for the current window, click **Help**.

Instance Information

This page displays the current instance information for the central processor complex (CPC).

Instance Information includes the current status of the CPC and other information about the operating conditions, characteristics, and settings of the CPC.

Status
Displays a combined current status of the CPC objects. If any objects of the CPC are unacceptable, then the overall current status is unacceptable.

Group
Displays the name of the group that contains the instance of the CPC to which the instance information applies.

More than one group can contain a unique instance of the same CPC; this situation allows assigning different activation profiles to different instances of the CPC.

Note: The Group field is blank if the **System Details** task is invoked from the Tasks Index.

Activation profile
More than one group can contain a unique instance of the same CPC; this situation allows assigning different activation profiles to different instances of the CPC.

Note: The Group field is blank if the **System Details** task is invoked from the Tasks Index.

Last used profile
Identifies the activation profile used for the most recent CPC activation.

Manually defined
Indicates whether the CPC was manually identified and defined (using the **System Manual Definition** template with the **Add Object Definition** task).

Yes
Indicates the CPC was manually identified and defined.

No
Indicates:

- The Hardware Management Console automatically identified the CPC.
- The console automatically created a unique object to represent the CPC.
- The object (referred to as an *undefined CPC*) was used to define the CPC.

Note: Tasks and objects used to define CPCs are available only with an Access Administrator and Service Representative default user IDs or user IDs with those roles.

Task name
Displays the name of the task most recently performed on the CPC.

Task status
Displays the status of the task most recently performed on the CPC.

CP Assist for Crypto functions
Displays whether the Cryptographic CP Assist feature is installed.

Note: If the CP Assist feature is not installed, some functions of the Integrated Cryptographic Service Facility (ICFS) might fail. See the *ICSF Application Programmer's Guide* or the *ICSF System Programmer's Guide* for complete information.

Secure Execution for Linux
Indicates whether the IBM Secure Execution for Linux feature is enabled on the system.

This indicator is also available on the **Systems** tab on the HMC Systems Management view, but the Secure Execution column on that tab is not displayed in the predefined default table view. To display the Secure Execution column, select the **Manage Views** icon in the work pane table toolbar to customize the table view.

Click **Manage** to import the required global key or host key bundle,view the hashes for the existing global key or host bundle, or clear the secondary global key or host key bundle. You can only import one key bundle at a time from a file system or from an FTP server. For the FTP server option, you need to supply a host name, user name, password, and protocol FTP, FTPS, or SFTP.

Note: This function is only available in the SERVICE user ID or an ID with equivalent permissions. The SYSPROG user ID or an ID with equivalent permissions can only view the hashes for the existing key bundles or clear the secondary key bundles.

"Lock out disruptive tasks" on page 1340
Sets the disruptive task lockout for the CPC.

Primary Licensed Internal Code security mode
Displays the Licensed Internal Code security mode for the Primary Support Element (starting on Version 2.14.0). The mode was set using the **Customize Console Services** task.

Alternate Licensed Internal Code security mode
Displays Licensed Internal Code security mode for the Alternate Support Element (starting on Version on 2.14.0). The mode was set using the **Customize Console Services** task.

You can find more detailed help on the following elements of this page:

Lock out disruptive tasks

Sets the disruptive task lockout for the CPC:

Yes
Locks the CPC to prevent the Hardware Management Console from performing disruptive tasks on the CPC.

No
Unlocks the CPC to allow the Hardware Management Console to perform disruptive tasks on the CPC.

After making your selection, click **Apply** to make the new settings take effect.

About disruptive tasks and the disruptive task lockout

Some Hardware Management Console tasks can be *disruptive*. Performing a disruptive task on the central processor complex (CPC) or an image can disrupt its operations. For example, activating the CPC and loading an image can be disruptive.

Setting **Lock out disruptive tasks** controls whether you can perform disruptive tasks on an object. You can lock an object to prevent accidentally performing disruptive tasks on it and then unlock the object only when you want to perform a disruptive task on it.

Note: When you use the Hardware Management Console to set an object's disruptive task lockout, the setting affects only disruptive tasks that are started manually by console operators using the Hardware Management Console (locally or remotely) or Web server sessions. The setting does *not* affect disruptive tasks started automatically or from other sources. For example, the setting does not affect tasks started by scheduled operations, by Operations Management commands, or by console operators using the Support Element console of the CPC.

Product Information

This page displays product information about the central processor complex (CPC), the machine in which it is located, and the software model capacity identifiers.

A *machine* is a particular configuration of hardware designed to provide particular operational capabilities and characteristics.

Product Information is assigned to machines and CPCs when they are manufactured, primarily for the purpose of identifying them.

CPC serial
Displays the serial number of the CPC

CPC location

Displays the 4-character device location of the central processor complex (CPC). It identifies the CPC's frame and its location (in EIA units) within the frame.

A CPC location consists of:

- A 1-character frame label.
- A 2-character EIA unit label for the location of the CPC from the bottom of the frame.
- A 1-character EIA unit label for the location of the CPC from the left side of the frame.

For example, CPC location A18A indicates the CPC is located:

- In frame A (**A**18A)
- At the 18th EIA unit from the bottom of the frame. (A**18**A)
- At the first EIA unit from the left side of the frame. (A18**A**)

CPC identifier

Displays the 2-digit hexadecimal number mapped to the device location of the central processor complex (CPC).

Note: The **CPC location** field displays the device location of the CPC.

Machine type - model
Displays the machine type and model number.

Machine serial
Displays the serial number of the machine.

Machine sequence
Displays the sequence number of the machine.

Plant of manufacture
Displays the identifier of the plant where the machine was made.

Product of
Displays the identifier of the manufacturer of the machine.

Model-Capacity identifier
Identifies the software model based on all permanent and all temporary active processors on the system.

Model-Temporary-Capacity identifier
Identifies the software model based on the permanent processor capacity plus only the active temporary capacity-based record.

Model-Permanent-Capacity identifier
Identifies the software model based on only the capacity in the permanent processor record

Acceptable Status

This page displays the current acceptable status settings for the central processor complex (CPC). **Acceptable Status** settings determine which CPC statuses are acceptable and which statuses are unacceptable. Use the check boxes to change the settings:

- A check mark in a check box indicates an acceptable status.
- An empty check box indicates an unacceptable status.
- To change one setting to the other, clear or select the check box.

The Hardware Management Console continuously monitors the status of the CPC and compares it to the acceptable status settings of the CPC.

You can find the status for CPCs in the **Status** column of the work pane table.

Setting the acceptable status settings of the CPC controls which statuses are reported as exceptions:

- Acceptable statuses, indicated by check marks in their check boxes, are *not* reported as exceptions.
- Unacceptable statuses, indicated by empty check boxes, are reported as exceptions.

Operating

To indicate that a state in which all CPs are in operating status is an acceptable status for the CPC, select **Operating**.

Service

To indicate that a state where CPs are in service status is an acceptable status for the CPC, select **Service**.

A console operator enabled service status for the CPC (ordinarily done at the request of a service representative to allow providing service for the CPC).

Not operating

To indicate if a power-on reset has not been performed: CPC power is on, but its CPs cannot operate until a power-on reset of the CPC is performed is an acceptable status for the CPC, select **Not operating**.

If a power-on reset was performed: no CPs are operating, but the exact status of the CPs vary.

The following CP statuses are summarized as not operating:

- Check stopped
- Loading
- Recovering
- Reset active
- Stepping
- Stopped

Communication not active
To indicate that the Support Element of the CPC is not communicating with this Hardware Management Console is an acceptable status for the CPC, select **Communication not active**.

Exceptions

To indicate that at least one Central Processor (CP) is operating, but at least one CP is not operating is an acceptable status for the CPC, select **Exceptions**.

Service required

To indicate that the CPC is still operating but is using the last redundant part of a particular type is an acceptable status for the CPC, select **Service required**.

Your CPC is shipped with more than the required number of parts to operate the CPC. You now have only the required number of parts to keep the CPC running. This is a reminder to you and your service representative to make repairs at the earliest possible time before additional parts fail that would make your CPC nonoperational.

No power

To indicate that the CPC power is off is an acceptable status for the CPC, select **No power**.

Degraded

To indicate that a degraded status where the CPC is operating but some hardware is not available is an acceptable status for the CPC, select **Degraded**.

Status check

To indicate that loss of communication with its Support Element is an acceptable status for the CPC, select **Status check**.

Save as Default

To change the acceptable status for all of the current objects defined with the same status type, select **Save as default**. After you click **Apply**, a message window is displayed confirming that you want to proceed with this operation.

Network Information

This page displays the current network information for the central processor complex (CPC).

The TCP/IP settings of a CPC are commonly considered to uniquely identify the CPC in a network. But if the CPC can be connected to more than one network, its TCP/IP settings actually identify *the LAN interfaces* through which the CPC is connected to the networks. The TCP/IP settings still essentially identify the CPC, but only in the network to which it is connected through a particular LAN interface. Therefore, if the CPC is connected to two networks:

- The TCP/IP settings for LAN interface 1 identify the CPC only in the network to which it is connected through LAN interface 1.
- Likewise, the TCP/IP settings for LAN interface 2 identify the CPC only in the network to which it is connected through LAN interface 2.

SNA address

Displays the fully-qualified SNA address of the Support Element of the CPC.

Node ID

Displays the SNA node ID, also called exchange identification (XID), of the Support Element of the CPC.

LAN interface 1 address

Displays the universal local area network (LAN) address and adapter type of LAN interface 1 in the Support Element of the CPC.

LAN interface 2 address

Displays the universal local area network (LAN) address and adapter type of LAN interface 2 in the Support Element of the CPC.

TCP/IP information for the CPC

Displays the network information for the CPC.

Name

Displays the TCP/IP name of the CPC along with the Ethernet port identification.

Protocol

Identifies the IPv4 or IPv6 address.

Type
Identifies the IPv6 scope.

Mask/Prefix
Displays the TCP/IP subnetwork mask/prefix of the LAN interface.

Primary address
Displays the TCP/IP address of the LAN interface.

Alternate address
Displays the universal LAN address and adapter type of the LAN interface (if installed) in the Support Element of the CPC.

STP Information

This page displays the current Server Time Protocol (STP) information for the server (CPC).

Note: This tab is available only when STP is enabled and the selected CPC is in an operating state.

Timing state
Specifies the synchronization state of the Time of Day (TOD) clock with respect to the timing network reference time. The possible timing states include:

Synchronized
The server is in this state when the TOD clock is synchronized with the timing network reference time, defined:

- If the server is in ETR timing mode, the server is synchronized with the Sysplex Timer.
- If the server is in STP timing mode, the server is synchronized with Coordinated Server Time (CST).

Unsynchronized
The server is in this state when the TOD clock is not synchronized with the timing network reference time, defined:

- If the server is in ETR timing mode, the server has lost synchronization with the Sysplex Timer.
- If the server is in STP timing mode, the server has lost or has not been able to attain synchronization with CST. The server is out of synchronization with CST when the TOD differs from CST by an amount that exceeds a model dependent STP-sync-check-threshold value.

Stopped
The server is in this state when the TOD clock is either in the stopped state or TOD clock recovery is in progress. After TOD clock recovery completes, the TOD clock enters either the synchronized or unsynchronized state.

Timing mode
Specifies the method by which the TOD clock is maintained for purposes of synchronization within a timing network. The possible timing modes include:

Local
The server is in this mode when the TOD clock has been initialized to a local time and is being stepped at the rate of the local hardware oscillator. The server is not part of a synchronized timing network.

ETR (External Time Reference)
The server is in this mode when the TOD clock has been initialized to the ETR and is being stepped by stepping signals from the ETR. To be in ETR timing mode, the server must be part of an ETR network.

STP (Server Time Protocol)
The server is in this mode when the TOD clock has been initialized to Coordinated Server Time (CST) and is being stepped at the rate of the local hardware oscillator. In STP timing mode, the TOD clock is steered to maintain or attain synchronization with CST. To be in STP timing mode, the server must be part of an STP network.

Timing network [ID]
Specifies the type of timing network in which the CPC is participating and its associated identifier. The network can be Unconfigured, ETR, Mixed CTN (ETR and STP), or STP-only CTN.

Stratum level

Specifies the hierarchy of the server in the timing network. A stratum level 0 indicates that the stratum level is undefined. A stratum level 1 is the highest level in the hierarchy of a timing network that uses STP messages for synchronization. A stratum level 2 server uses STP messages to synchronize to a Stratum 1 server. A stratum level 3 server uses STP messages to synchronize to a Stratum 2 server.

Note: This field is displayed only for a Mixed CTN or an STP-only CTN.

Role of CPC in CTN
Specifies the server roles in a coordinated timing network. The roles include the following:

Note: This field is displayed only for a Mixed CTN or an STP-only CTN.

Preferred Time Server
Is the server you select to be the Preferred Stratum 1 server in an STP-only CTN.

Backup Time Server
Is the server you select to take over as the Current Time Server (Stratum 1 server), because of either a planned or an unplanned reconfiguration.

Current Time Server
Is the server that is currently the Stratum 1 for an STP-only CTN.

Arbiter
Is the server you select to provide additional means for the Backup Time Server to determine if it should take over as the Current Time Server.

Member of the CTN
Is a server that is a member of the CTN but does not currently have a role.

Time zone
Specifies the time zone for this CPC.

Degrade Reasons

A degraded status indicates that, although the CPC is still operating, some hardware is not available. This page indicates why the CPC is in a Degraded status.

Note: This tab is available only when an object is in a degraded state.

Some conditions that can cause the Degraded status include:

- Loss of memory
- Loss of channels due to CPC hardware failure
- Loss of functioning for one or more books
- Open ring connecting the books
- Expiration of capacity backup resources
- Reduced processor frequency due to temperature problem
- IML of CPC during temperature problem.

Busy Status

This page identifies the user ID, the location of the user, and the task that caused the object to become busy.

Energy Management

This page displays the power and thermal monitoring information for the specified CPC and zCPC.

CPC

Power rating
Specifies the maximum power draw in watts (W) and Btu/hr. of this CPC. This is a calculated value as indicated by the electrical rating labels or system rating plates of the CPC components.

Power consumption
Specifies the current power consumption in watts (W) and Btu/hr. for this CPC.

Power saving
Specifies the current power saving setting for the CPC. Power saving reduces the energy consumption of a system and you can manage it using the **Set Power Saving** task. The possible settings include:

High performance
Specifies not reducing the power consumption and performance of the CPC. This is the default setting.

Low power
Specifies low power consumption for all components of the CPC enabled for power saving.

Custom
Specifies that some, but not all, components of the CPC are in the **Low power** setting.

Not supported
Specifies not supporting power saving for this CPC.

Not available
Specifies that power saving is not available for this CPC.

Not entitled
Specifies that the server is not entitled for power saving.

Power save profile
Specifies the selected power save profile that is in the options section of the currently active activation profile.

Power capping
Specifies the current power capping setting for the CPC. Power capping limits peak power consumption of a system and, you can manage it using the **Set Power Cap** task. The possible settings include:

Disabled
Specifies not setting the power cap of the CPC not limiting the peak power consumption. This is the default setting.

Enabled
Specifies capping all components of the CPC available for power capping to limit the peak power consumption of the CPC.

Custom
Specifies permitting individual configuration of the components of the CPC for power capping.

Not supported
Specifies not supporting power capping for this CPC.

Not entitled
Specifies that the server is not entitled for power capping.

Cap range
Specifies the minimum and maximum values for the CPC cap value in watts (W) and Btu/hr. This is a sum of the minimum and maximum cap values of the component

Current cap
Specifies the current power capping setting for the CPC in watts (W) and Btu/hr. The current cap value indicates the power budget for the zCPC.

zCPC

Power rating
Specifies the maximum power draw of this zCPC in watts (W) and Btu/hr. This is a calculated value as indicated by the electrical rating labels or system rating plates of the zCPC components.

Power consumption
Specifies the current power consumption of the zCPC in watts (W) and Btu/hr.

Ambient temperature
Specifies the input air temperature in degrees Celsius (°C) and degrees Fahrenheit (°F) as measured by the system.

Exhaust temperature
Specifies the exhaust air temperature in degrees Celsius (°C) and degrees Fahrenheit (°F) as calculated by the system. This is useful in determining potential hot spots in the data center.

Humidity
Specifies the amount of water vapor in the air as measured by the system. The humidity sensor gives a reading of the relative humidity of the air entering the system. The recommended long-term relative humidity for a system with an altitude from sea level to 900 meters (2953 feet) is 60%. The range of acceptable relative humidity is 8 - 80%.

For more information, see the chapter related to environmental specifications in the *Installation Manual for Physical Planning*.

Dew point
Specifies the air temperature in degrees Celsius (°C) and degrees Fahrenheit (°F) at which water vapor condenses into water. This is a calculated value based on the current temperature and relative humidity. Cooling the server to the dew point can result in condensation on critical internal parts, leading to equipment failure, unless the computer room environment is adequately maintained to prevent it.

For more information, see the chapter related to environmental specifications in the *Installation Manual for Physical Planning*.

Heat load
Specifies the amount of heat in Btu/hr. removed from the system. This value is the sum of the heat loads removed by forced-air and water.

Heat load (forced-air)
Specifies the amount of heat in Btu/hr. removed from the system by forced-air.

Heat load (water)
Specifies the amount of heat in Btu/hr. removed from the system by chilled water.

Note: This field is 0 if the system is not cooled by chilled water.

Maximum potential power
Specifies the maximum potential power consumption of a system in watts (W) and Btu/hr. This value is based on the configuration of the system and can be used for power and cooling planning.

Maximum potential heat load
Specifies the maximum potential heat load of a system in watts (W) and Btu/hr. This value is based on the configuration of the system and can be used for power and cooling planning.

Power saving

Specifies the current power saving setting of the zCPC. Power saving reduces the energy consumption of a system, and you can manage it using the **Set Power Saving** task. The possible settings include:

High performance
Specifies not reducing the power consumption and performance of the zCPC. This is the default setting.

Low power
Specifies reducing the performance of the zCPC.

Not supported
Specifies not supporting power saving for this zCPC.

Not available
Specifies that power saving is not available for this zCPC.

Not entitled
Specifies that the server is not entitled for power saving.

Power capping

Specifies the current power capping setting of the zCPC. Power capping limits peak power consumption of a system, and you can manage it using the **Set Power Cap** task. The possible settings include:

Disabled
Specifies not setting the power cap of the zCPC and not limiting the peak power consumption. This is the default setting.

Enabled
Specifies limiting the peak power consumption of the zCPC to the Current cap value.

Not supported
Specifies not supporting power capping for this zCPC.

Not entitled
Specifies the server is not entitled for power capping.

Cap range
Specifies the minimum and maximum values for the zCPC cap value in watts (W) and Btu/hr.

Current cap
Specifies the current cap value for the zCPC in watts (W) and Btu/hr. The current cap value indicates the power budget for the zCPC.

Note: This tab or certain information on this tab is available only when the appropriate feature is installed.

System BCPii Permissions

This page allows you to dynamically enable the Base Control Program internal interface (BCPii) permissions for the system.

Enable the system to receive commands from partitions
To enable the selected system to receive BCPii commands from partitions, select **Enable the system to receive commands from partitions**. When selected, the system can receive BCPii commands from other active logical partitions.

All partitions
Select this option if you want the system to receive BCPii commands from all active logical partition.

“Add partition” on page 1348 (Selected partitions)
Select this option if you want to add or remove the logical partitions that are allowed to send BCPii commands to the system.

Add
To add a system and logical partition to BCPii commands to the system, click **Add**.

Remove
To remove a selected logical partition that can send BCPii commands to the system, click **Remove**.

Add partition

Use this window to specify the partitions from which the target system can receive BCPii commands.

Enter system and partition manually
System: Enter the system name for the logical partition from which the target system can receive BCPii commands.

Netid: Enter the Netid name for the selected system.

Partition: Enter the logical partition name from which the target system can receive BCPii commands.

Select a system and partition

System: Select from the drop-down menu the system for the logical partition from which the target system can receive BCPii commands.

Netid: The Netid displays for the selected system.

Partition: Select from the drop-down menu the active logical partition from which the target system can receive BCPii commands.

Additional functions on this window include:

Add

To add the system and partition, click **Add**.

Cancel

To exit the current window without saving changes, click **Cancel**.

System Details (DPM)

Accessing the System Details task

Use this task for information about the selected system that is Dynamic Partition Manager (DPM) enabled.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

You can access this task from the main console page by selecting the Systems Management node, by selecting a specific DPM-enabled system, or be selecting this task in the Tasks index. You can use either the default SYSPROG user ID or any user IDs that a system administrator has authorized to this task through customization controls in the **User Management** task.

To display and optionally modify the details for the selected DPM-enabled system, complete the following steps.

1. Select the system that is DPM-enabled.
2. Open the **System Details** task. The System Details window is displayed.
3. View or modify the editable fields.
4. Click **Apply** to save the changes.

System Details

Use this task to view and manage properties of the selected Dynamic Partition Manager (DPM)-enabled system.

Use the navigation links to display each tab or use the **Expand All** and **Collapse All** icons to display each section view.

- Select the navigation link or the **Expand** icon to display the “General” on page 1350 details tab section.
- Select the navigation link or the **Expand** icon to display the “Status” on page 1351 details tab section.
- Select the navigation link or the **Expand** icon to display the “Processors and Memory” on page 1352 details tab section.
- Select the navigation link or the **Expand** icon to display the “Adapters” on page 1354 details tab section. You can use the Filter function string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.
- Select the navigation link or the **Expand** icon to display the “Management Networks” on page 1355 details tab section. You can use the Filter function string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.
- Select the navigation link or the **Expand** icon to display the “Energy” on page 1356 details tab section.

- Select the navigation link or the **Expand** icon to display the "Time Server" on page 1357 details tab section.
- Select the navigation link or the **Expand** icon to display the "Start Options" on page 1358 details tab section.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

The navigation pane also includes the following links to related tasks.

System Information
Opens the **System Information** task for the selected system that is Dynamic Partition Manager enabled.

Monitor System
Switches the foreground window to the **Monitor** tab for the selected system that is Dynamic Partition Manager enabled.

Additional functions on this window include:

OK
To save the current changes and exit the window, click **OK**. The **OK** button is not displayed in view-only mode.

Apply
To save the current changes you made without exiting the window, click **Apply**. The **Apply** button is not displayed in view-only mode.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to view the information and modify the description for the selected DPM-enabled system. Use the **Expand All** icon to display the General section. The following list provides a description of each element on the General section.

Name
Specifies the name for the selected system.

Description
Specify an optional meaningful text that describes the selected system. The description can be up to 1024 characters in length.

Object ID
Specifies the associated universal unique identifier (UUID) of the selected system.

Machine type - model
Displays the machine type and model number of the selected system.

Machine serial
Displays the serial number of the selected system.

Machine sequence
Displays the sequence number of the selected system.

Support Element version
Displays the Support Element firmware level of the system.

System mode
Identifies the operating mode established by the most recent power-on reset for the selected system.

CP Assist for Crypto functions
Displays whether the Cryptographic CP Assist feature is installed.

Note: If the CP Assist feature is not installed, some functions of the Integrated Cryptographic Service Facility (ICFS) might fail. See the *ICSF Application Programmer's Guide* or the *ICSF System Programmer's Guide* for more information.

Secure Execution

Indicates whether the IBM Secure Execution for Linux feature is enabled on this system, and whether the required global key and host key are installed on the Support Element (SE). This field is displayed only when the feature was ordered for this system and installed.

This indicator is also available on the **Systems** tab on the HMC **Systems Management** view, but the Secure Execution column on that tab is not displayed in the predefined default table view. To display the Secure Execution column, select the **Manage Views** icon in the work pane table toolbar to customize the table view.

This task includes a button through which you can open a separate task to view or manage the keys. **Manage Keys** opens the **Manage Secure Execution Keys** task on the HMC or SE in read-only mode, through which you can view details about each key. If you are logged in to the SE using the SERVICE user ID or an ID with equivalent permissions, you can import the required global key or host key bundle; view the hashes for the existing global or host key; or clear the global or host key, which immediately prevents further usage by any partition on the system, and deletes the corresponding key bundle file from the system.

Status

Use the Status details tab section to view the current system status and the acceptable status settings for the selected DPM-enabled system. The acceptable status settings determine the system statuses are acceptable or unacceptable. Use the **Expand All** icon to display the Status section. The following list provides a description of each element in the Status section.

Status

Displays a combined current status of the CPC objects for the selected system. If any objects of the CPC are unacceptable, then the overall current status is unacceptable.

Degrade reasons

A degraded status indicates that, although the system is still operating, some hardware is not available.

Some conditions that can cause the Degraded status include:

- Loss of memory
- Loss of channels due to a system hardware failure
- Loss of functioning for one or more books
- Open ring connecting the books
- Expiration of capacity backup resources
- Reduced processor frequency due to a temperature problem
- System was IMLed during a temperature problem.

Acceptable statuses

Use the check boxes to change the settings:

- A check mark in a check box indicates an acceptable status.
- An empty check box indicates an unacceptable status.
- To change one setting to the other, clear or select the check box.
- To the right of the Acceptable statuses label is a tooltip icon  .

Active

To indicate that the state in which the system is active is an acceptable status for the system, select **Active**.

No power

To indicate that the system power is off is an acceptable status for the system, select **No power**.

Status check

To indicate that loss of communication is an acceptable status for the system, select **Status check**.

Not operating

To indicate if a power-on reset has not been performed: System power is on, but its CPs cannot operate until a power-on reset of the system is performed is an acceptable status for the system, select **Not operating**.

If a power-on reset was performed: no CPs are operating, but the exact status of the CPs vary.

The following CP status values are summarized as not operating:

- Check stopped
- Loading
- Recovering
- Reset active
- Stepping
- Stopped

Exceptions

To indicate that at least one Central Processor (CP) is operating, but at least one CP is not operating is an acceptable status for the system, select **Exceptions**.

Degraded

To indicate that a degraded status where the system is operating but some hardware is not available is an acceptable status for the system, select **Degraded**.

Service required

To indicate that the system is still operating but is using the last redundant part of a particular type is an acceptable status for the system, select **Service required**.

Your system is shipped with more than the required number of parts to operate the system. You now have only the required number of parts to keep the system running. This is a reminder to you and your support system representative to make repairs at the earliest possible time before additional parts fail that would make your system nonoperational.

Communication not active

To indicate that the Support Element of the system is not communicating with this Hardware Management Console is an acceptable status for the system, select **Communication not active**.

Service

To indicate that a state where the system is in service status is an acceptable status for the system, select **Service**.

A console operator enabled service status for the system (ordinarily done at the request of a support system representative to allow providing service for the system).

Processors and Memory

Use the Processors and Memory details tab section to graphically view the system memory and summarize system processors for the selected system that is Dynamic Partition Manager (DPM) enabled. The physical processors can be Central Processors (CP) or Integrated Facility for Linux (IFL). Use the

Expand All icon to display the Processors and Memory section. The following list provides a description of each element on the Processors and Memory section:

Processors

Indicates the system processor limit, total number of installed physical processors, and the shared and dedicated physical processors on the system. The bar chart scale ranges from 0 to the total amount of physical processors that can be installed on the system. To show the actual number of physical processors that each bar segment represents, hover your cursor over the colored segment. To the right of the Processor label is a tooltip icon. A dotted line indicates the systems limit and the total number of installed physical processors on the system. To the right of the bar chart, a color legend identifies each segment and values of the bar chart:

System limit
Indicates the system limit size of CPs. It is the maximum number of physical processors that can be installed on the system. The values is represented as a dotted line in the bar chart.

Installed
Indicates the number of physical processors currently installed on the system. This number may be greater than the number of entitled processors. The values are represented as a dotted line in the bar chart.

Shared IFLs
Indicates the number of entitled IFL processors that are not dedicated (the number of physical processors supporting all dedicated virtual IFL processors). If there are no entitled IFL processors, the value is not included in the bar chart.

Dedicated IFLs
Indicates the number of entitled IFL processors that are dedicated (the number of physical processors supporting all dedicated virtual IFL processors). If there are no entitled IFL processors, this value is not included in the bar chart. If there are entitled IFLs, but none are dedicated, this value on the legend is 0.

Shared CPs
Indicates the number of entitled CP processors that are dedicated. (the number of physical processor supporting all shared virtual CP processors). If there are not entitled CP processors, this value is not included in the pie chart.

Dedicated CPs
Indicates the number of entitled CP processors that are dedicated (the number of physical processors support dedicated virtual CP processors). Dedicated amount of CPs dedicated to active and reserved partitions in the system. If there are not entitled CP processors, this value is not included in the pie chart. If there are entitled CPs, but none are dedicated, this value on the legend is 0.

Memory

Indicates the system memory, installed, entitled, and allocated processor memory on the selected system that is Dynamic Partition Manager enabled. The bar chart scale ranges from 0 to the total amount of memory that can be installed on the system. To show the actual amount of allocated memory that each bar segments represents, hover your cursor over the colored segment. To show the actual number of processor memory that each bar segment represents, hover your cursor over the colored segment. To the right of the Memory label is a tooltip icon. A dotted line indicates the systems limit and the total number of installed processor memory on the system. To the right of the bar chart, a color legend identifies each segment and values of the bar chart:

System limit
Indicates the maximum amount of memory that can be installed on the system. The values is represented as a dotted line in the bar chart.

Installed
Indicates the amount of physical memory that can be installed on the system. The values is represented as a dotted line in the bar chart.

Entitled
Indicates the amount of entitled memory for this system. Entitled memory is the amount of memory that is licensed for use, which might be less than the total amount of memory that is installed on the system. The value is represented as a dotted line in the bar chart.

Allocated
Indicates the total amount of allocated memory, which is the total memory assigned to all active and reserved partitions on the system.

Model-Capacity identifier
Identifies the software model based on all permanent and all temporary active processors on the selected system that is Dynamic Manager enabled.

Model Temporary-Capacity identifier
Identifies the software model based on the permanent processor capacity plus only the active temporary capacity-based record.

Model Permanent-Capacity identifier
Identifies the software model based on only the capacity in the permanent processor record.

Adapters

Use the Adapters details tab section to view the adapter information for the selected DPM-enabled system. Use the **Expand All** icon to display the General section. The following list provides a description of each element on the Adapters section:

Adapter table toolbar

You can work with the table by using the table icons or **Actions** list from the Adapter table tool bar. If you place your cursor over an icon, the icon description displays.

Configure Options 
Provides a way to exclude or include specific columns from the table display. To configure table options, click the **Configure Options** icon. Available columns are in lists by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print 

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter 
Provides advanced filter option through which you can reduce the total number of table entries. To access filter options, click the **Filter** icon.

Columns in the Adapter table

The following columns are displayed for the Adapters table. You can modify the columns in the default table display by using the **Configure Options** icon.

Type
Indicates the adapter type supported on the selected DPM-enabled system.

Number Installed
Indicates the number of adapters installed in your system and configured.

Device Allocation
Displays the current allocation for all adapters (progress bar value, which includes Network Interface Cards (NICs), Host Bus Adapters (HBAs), virtual functions, and usage domains of active and reserved partitions).

The Adapter section also includes the following links to related tasks.

Manage Adapters
Open the **Manager Adapters** task for the selected DPM-enabled system.

Management Networks

Use the Management Networks details tab section displays the current information for the two management interfaces on the selected DPM-enabled system. Use the **Expand All** icon to display the Management Networks section. The following list provides a description of each element on the Management Networks section:

Management Networks table toolbar

You work with the table by using the table icons or **Actions** list from the Management Network table tool bar. If you place your cursor over an icon, the icon description displays.

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print 

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Standard table functions

The icons perform the following functions in the Management Networks table:

Configure Options 
Provides a way to exclude or include specific columns from the table display. To configure table options, click the **Configure Options** icon. Available columns are in listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**

Columns in Management Networks table

The following columns are displayed for the Management Networks table. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Protocol
Identifies the IPv4 or IPv6 address.

Type
Identifies the IPv6 scope.

Mask/Prefix
Displays the TCP/IP subnetwork mask/prefix of the LAN interface.

Primary Support Element IP Address
Displays the TCP/IP address of the LAN interface for IPv4. Displays the universal LAN address and adapter type of the LAN interface (if installed) in the Support Element of the system for IPv6.

Alternate Support Element IP Address
Displays the TCP/IP address of the LAN interface for IPv4. Displays the universal LAN address and adapter type of the LAN interface (if installed) in the Support Element of the system for IPv6.

Energy

Use the Energy details tab section to view the power and thermal monitoring information for the selected DPM-enabled system. Use the **Expand All** icon to display the Energy section. The following list provides a description of each element on the Energy section:

Power rating
Specifies the maximum power draw in watts (W) and Btu/hr of this system. This is a calculated value as indicated by the electrical rating labels or system rating plates of the system components.

Power saving
Specifies the current power saving setting for the system. Power saving reduces the energy consumption of a system and you can manage it using the **Set Power Saving** task. The possible settings include:

High performance
Specifies not reducing the power consumption and performance of the system. This is the default setting.

Low power
Specifies low power consumption for all components of the system enabled for power saving.

Not entitled
Specifies that the server is not entitled for power saving.

Enable power capping
Select the power capping setting to enable power capping and set a cap field to limit the peak consumption of the system resource. Unselected indicates that power capping is disabled.

Cap
Specifies the minimum and maximum values for the Cap Value in watts (W). This defines the set of acceptable values for setting the power cap.

Power capping
Specifies the current power capping setting for the system. Power capping limits peak power consumption of a system and, you can manage it using the **Set Power Cap** task. The possible settings include:

Disabled
Specifies not setting the power cap of the system not limiting the peak power consumption. This is the default setting.

Enabled
Specifies capping all components of the system available for power capping to limit the peak power consumption of the system.

Custom
Specifies permitting individual configuration of the components of the system for power capping.

Not supported
Specifies not supporting power capping for this system.

Not entitled
Specifies that the server is not entitled for power capping.

Maximum potential power (W):
Specifies the maximum potential power consumption of a system in watts (W) and Btu/hr. This value is based on the configuration of the system and can be used for power and cooling planning.

Maximum potential heat load (BTU/hr):
Specifies the maximum potential heat load of a system in watts (W) and Btu/hr. This value is based on the configuration of the system and can be used for power and cooling planning.

Time Server

Use the Time Server details tab section to view the current Server Time Protocol (STP) information for the selected DPM-enabled system. Use the **Expand All** icon to display the Timer Server section.

Note: No information is displayed if the STP feature is not installed and enabled on the system.

The following list provides a description of each element on the Timer Server section:

Timing state
Specifies the synchronization state of the time-of-day (TOD) clock with respect to the timing network reference time. The possible timing states include:

Synchronized
The server is in this state when the TOD clock is synchronized with the timing network reference time, defined:

- If the server is in ETR timing mode, the server is synchronized with the Sysplex Timer.
- If the server is in STP timing mode, the server is synchronized with Coordinated Server Time (CST).

Unsynchronized
The server is in this state when the TOD clock is not synchronized with the timing network reference time, defined:

- If the server is in ETR timing mode, the server has lost synchronization with the Sysplex Timer.
- If the server is in STP timing mode, the server has lost or has not been able to attain synchronization with CST. The server is out of synchronization with CST when the TOD differs from CST by an amount that exceeds a model dependent STP-sync-check-threshold value.

Stopped
The server is in this state when the TOD clock is either in the stopped state or TOD clock recovery is in progress. After TOD clock recovery completes, the TOD clock enters either the synchronized or unsynchronized state.

Timing mode
Specifies the method by which the TOD clock is maintained for purposes of synchronization within a timing network. The possible timing modes include:

Local
The server is in this mode when the TOD clock has been initialized to a local time and is being stepped at the rate of the local hardware oscillator. The server is not part of a synchronized timing network.

ETR (External Time Reference)
The server is in this mode when the TOD clock has been initialized to the ETR and is being stepped by stepping signals from the ETR. To be in ETR timing mode, the server must be part of an ETR network.

STP (Server Time Protocol)
The server is in this mode when the TOD clock has been initialized to Coordinated Server Time (CST) and is being stepped at the rate of the local hardware oscillator. In STP timing mode, the TOD clock is steered to maintain or attain synchronization with CST. To be in STP timing mode, the server must be part of an STP network.

Timing network type
Specifies the type of timing network in which the system is participating. The network can be Unconfigured, ETR, Mixed CTN (ETR and STP), or STP-only CTN.

Timing network ID
Specifies the timing network identifier.

Stratum level

Specifies the hierarchy of the server in the timing network. A stratum level 0 indicates that the stratum level is undefined. A stratum level 1 is the highest level in the hierarchy of a timing network that uses STP messages for synchronization. A stratum level 2 server uses STP messages to synchronize to a Stratum 1 server. A stratum level 3 server uses STP messages to synchronize to a Stratum 2 server.

Note: This field is displayed only for a Mixed CTN or an STP-only CTN.

CTN roles
Specifies the server roles in a coordinated timing network. The roles include the following:

Note: This field is displayed only for a Mixed CTN or an STP-only CTN.

Preferred Time Server
Is the server you select to be the Preferred Stratum 1 server in an STP-only CTN.

Backup Time Server
Is the server you select to take over as the Current Time Server (Stratum 1 server), because of either a planned or an unplanned reconfiguration.

Current Time Server
Is the server that is currently the Stratum 1 for an STP-only CTN.

Arbiter
Is the server you select to provide additional means for the Backup Time Server to determine if it should take over as the Current Time Server.

Member of the CTN
Is a server that is a member of the CTN but does not currently have a role.

Time zone
Specifies the time zone for this system.

The Timer Server section also includes the following links to related tasks.

Manage System Time
Open the **Manage System Time** task for the selected DPM-enabled system.

Start Options

Use the Start Options details section to view and add partitions and groups of partitions that will be auto-started with the system. By default all group rows are expanded to show partitions in that group. Individual partitions and groups of partitions will be started in the order defined. You can optionally enter

how long to delay after starting a partition or group of partitions before starting the next. The following list provides a description of each element on the Start Options details section:

The Start Options table toolbar

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both:

“Add Partitions” on page 1360

Opens the Add Partitions window, through which you can add one or more partitions to the Auto-Start table. The Add Partitions function is enabled only if you have not selected any partitions or if one group is selected. Select this option from the **Actions** list or click the **Add Partitions** icon.

“New Auto-Start Group” on page 1362

Opens the New Auto-Start Group window, through which you can define a new group of partitions that will Auto-Start at the same time. If you selected any partitions in the New Auto-Start Group table, all of those selected partitions are added to the new group. The New Auto-Start Group function is always enabled. Select this option from the **Actions** list or click the **New auto-Start Group** icon.

Move Up

Moves the selected partition or partition groups up in the table. Select this option from the **Actions** list or click the **Move Up** icon.

Move Down

Moves the selected partition or partition groups down in the table. Select this option from the **Actions** list or click the **Move Down** icon.

Export

Export as HTML

Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV

Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print

Print All

Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected

Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview

Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Remove
Opens a confirmation window through which you can remove the auto-start group, remove partitions from an auto-start group, or remove a partition from the table. The Remove from Group function is not enabled unless the selected partitions all belong to the same group.

In the window, click **Remove** to confirm that you want to remove the selections, or click **Cancel** to close the window without removing the selections.

"Auto-Start Group Details" on page 1363
Opens the Auto-Start Group Details window, through which you can view information about only one selected partition group. The Auto-Start Group Details function is not enabled if you have selected more than one group, or have selected one or more partitions.

Partition Details
Opens the **Partition Details** task in a separate window. If you select more than one partition, a separate window is opened for each selected partition. The Partition Details function is enabled if you have selected one or more partition rows.

Select All
Selects all partitions and partition groups in the Start Options table.

Deselect All
Deselects all partitions and partition groups in the Start Options table.

Expand All
Expands all partitions groups in the Start Options table.

Collapse All
Collapses all partition groups in the Start Options table.

Columns in the Start Options table

The Processors table contains the following columns in the default display.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries. To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a partition or a partition groups that will be auto-started with the system.

- The name of each partition is a hyperlink through which you can open the **Partition Details** task.
- The name of each partition group is a hyperlink through which you can open the **Group Details** window.

Post-Start Delay
Indicates the amount of time (in seconds) for the console to wait after starting one partition and before starting the next partition, when starting multiple partitions. If a partition is a member of a group, the Post-Start Delay column for the partition in the group is blank. You can use the spinner controls to increment or decrement the number of seconds.

Description
Displays the user-provided description, if any, of the partition or partition group.

Add Partitions

Use the Add Partitions table to add partitions to the Start Options table that will be auto-started with the system. The following topics describe each element on the Add Partitions Dialog page.

Add Partitions table toolbar

You work with the table by using the table icons or **Actions** list from the Add Partitions table tool bar. If you place your cursor over an icon, the icon description displays. The icons perform the following functions in the Add Partitions table:

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options 
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the **Configure Options** icon. Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter 
Provides advanced filter option through which you can reduce the total number of table entries. To access filter options, click the **Filter** icon.

Columns in the Add Partitions table

The following columns are displayed for the Add Partitions table. You can modify the columns in the default table display by using the **Configure Options** icon or actions.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a partition or a partition group. Partitions that do not belong to a group are listed before any table entries for a partition group. If a partition is a member of a group, its table entry is listed only under the group to which it belongs. By default, all group rows are expanded to show the table entry for each member partition.

- The name of each partition is a hyperlink through which you can open the **Partition Details** task.

- The name of each partition group is a hyperlink through which you can open the **Group Details** window.

Description
Displays the user-provided description, if any, of the partition or partition group.

Additional functions on this window include:

Add
After you have selected the partitions to and added them to the Start Options table, click **Add**. The **Add** button is not displayed in view-only mode.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

New Auto-Start Group

Use the New Auto-Start Group dialog to create a group of partitions that auto-start with the system at the same time. Enter a name and description for the New Auto-Start group. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional. The following list provides a description of each element on the New Auto-Start Group Dialog page:

Name
Enter a required unique name for the New Auto-Start Group. The name can be 1 - 64 characters in length. Supported characters are alphanumeric, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters.

Description
Optionally enter a description for the New Auto-Start Group. The description can be up to 1024 characters in length.

Post-Start Delay
Use the spinner controls to indicate the amount of time (in seconds) for the console to wait after starting one partition and before starting the next partition, when starting multiple partitions.

New Auto-Start Group table toolbar

You work with the table by using the table icons or **Actions** list from the New Auto-Start Group table tool bar. If you place your cursor over an icon, the icon description displays. The icons perform the following functions in the New Auto-Start Group table:

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options 
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the **Configure Options** icon. Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter 
Provides advanced filter option through which you can reduce the total number of table entries. To access filter options, click the **Filter** icon.

Columns in the New Auto-Start Group table

The following columns are displayed for the New Auto-Start Group table. You can modify the columns in the default table display by using the **Configure Options** icon.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a partition or a partition group. Partitions that do not belong to a group are listed before any table entries for a partition group. If a partition is a member of a group, its table entry is listed only under the group to which it belongs. By default, all group rows are expanded to show the table entry for each member partition.

- The name of each partition is a hyperlink through which you can open the **Partition Details** task.
- The name of each partition group is a hyperlink through which you can open the **Group Details** window.

Description
Displays the user-provided description, if any, of the partition or partition group.

Additional functions on this window include:

OK
To save the current changes and exit the window, click **OK**. The **OK** button is not displayed in view-only mode.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Auto-Start Group Details

Use the Auto-Start Group Details Dialog page to modify properties of a created group. Enter a name and description for the Auto-Start Group. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional. The following list provides a description of each element on the Auto-Start Group Details Dialog page:

Name
Enter a required unique name for the Auto-Start Group Details. The name can be 1 - 64 characters in length. Supported characters are alphanumeric, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters.

Description
Optionally enter a description for the Auto-Start Group. The description can be up to 1024 characters in length.

Post-Start Delay
Use the spinner controls to indicate the amount of time (in seconds) for the console to wait after starting one partition and before starting the next partition, when starting multiple partitions.

Additional functions on this window include:

OK
To save the current changes and exit the window, click **OK**. The **OK** button is not displayed in view-only mode.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

System Information

Accessing the View Console Information task

This task displays information about the Hardware Management Console and its licensed internal code. The machine information could include:

- Engineering Change (EC) number
- Machine type
- Version of the Hardware Management Console
- Licensed Internal Code (LIC) control level
- Machine model number
- Engineering Changes AROM
- Machine serial number
- Bundle level of the Hardware Management Console

Licensed internal code controls many of the operations available on the Hardware Management Console. Internal code changes may provide new operations, or correct or improve existing operations.

Product support assigns the EC number to a set of licensed internal code. The number identifies the licensed internal code and its purpose.

If a set of licensed internal code is modified, its EC number is supplemented with a state level. A state level distinguishes between different versions of the same set of licensed internal code.

To view the console information:

1. Open the **View Console Information** task. The View Console Information window is displayed.
2. Select a licensed internal code from the list.
3. Click **EC Details...** to view the additional information about internal code state levels.
4. Click **OK** when you are done viewing the information.

Accessing the System Information task

This task displays information about a selected CPC (server) and its licensed internal code. The machine information could include:

- Engineering Change (EC) number
- Machine type
- Version of the Support Element
- Licensed Internal Code (LIC) control level
- Machine model number
- Engineering Changes AROM or Concurrent Engineering Changes
- Machine serial number
- Driver level of the Support Element
- Bundle level of the Support Element

The internal code changes information includes the engineering change (EC) number, the state levels of each set of licensed internal code associated with the Support Element, and a description.

Licensed internal code controls many of the operations available on the Support Element. Internal code changes may provide new operations, or correct or improve existing operations.

The part number and EC number are assigned to a set of licensed internal code by product support. The numbers identify the licensed internal code and its purpose.

If a set of licensed internal code is modified, its EC number is supplemented with a state level. A state level distinguishes between different versions of the same set of licensed internal code.

To view the system information:

1. Select one or more CPCs (servers).
2. Open the **System Information** task. The System Information window is displayed.
3. Select the internal code information you want to view.
   - To view the additional information about this internal code, click **EC Details...**.
   - To display information about further actions that may need to be taken, click **Query Additional Actions...**.

     Note: This option is available only if the selected CPC is at Version 2.10.0 or later.
4. Click **OK** when you have completed this task.

View Console Information/System Information

Use the **View Console Information** task to display information about the internal code changes stored on the console.

Use the **System Information** task to display information about the internal code changes stored on the Support Element of the selected systems.

Licensed internal code, also referred to as internal code, controls many of the operations available on the console or on the systems and their Support Elements. Internal code changes may provide new internal code, or correct or improve existing internal code.

A console or a systems Support Element automatically keeps records of information about the internal code changes stored on it. The record-keeping begins when changes are retrieved from their source to the console. For each internal code change the information identifies:

- Its Engineering Change (EC) number and description
- The change level most recently retrieved
- The highest retrieved internal code change level that can be installed and activated concurrently
- The change level most recently activated
- The change level most recently accepted

- Additional details include the most recent date and time each task was performed.

The information may assist you with planning and managing the internal code change process. For example, review the information to either:

- Determine whether the console or system is operating with your latest available levels of internal code changes.
- Determine which tasks you must perform next to make the console or system operate with the latest available levels of internal code changes.

Note: Service representatives will provide assistance applying and managing internal code changes.

Machine Information

EC number
Displays the Engineering Change (EC) number of the Hardware Management Console or selected systems where the internal code changes are applied.

Type
Displays the machine type of the Hardware Management Console or selected systems where the internal code changes are applied.

Version
Displays the version of the Hardware Management Console or selected systems where the internal code changes are applied.

LIC control level
Displays the Licensed Internal Code level of the Hardware Management Console or selected systems where the internal code changes are applied.

Model number
Displays the machine model number of the Hardware Management Console or selected systems where the internal code changes are applied.

Engineering Changes AROM
This label is displayed when the system is preloaded for disruptive activation of a new Engineering Changes (ECs) level.

Serial number
Displays the machine serial number of the Hardware Management Console or selected systems where the internal code changes are applied.

Driver
Displays the driver level of the Hardware Management Console or selected systems where the internal code changes are applied.

Note: The Driver information only appears if you are using this task with a user ID definition that is based on the *Service Representative* task roles.

Bundle level
Displays the bundle level of the Hardware Management Console or selected systems where the internal code changes are applied.

Note: This information is not available for IBM zEnterprise 196 and IBM zEnterprise 114 machines and earlier.

Internal Code Change Information

For additional information about an internal code change, select an EC number, then click **EC Details...**.

EC Number
Displays the engineering change (EC) number of the internal code change.

Retrieved Level
Displays the internal code change level that was most recently copied to the console or Support Elements of the systems, making it available for installation.

Installable Concurrent
Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for this console or for the systems, from the current installed level up to and including the installable concurrent level, without disrupting the operations of the systems defined to this console or the operations of the selected systems.

Activated Level
Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the console or selected systems.

Accepted Level
Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the console or selected systems.

Description
Displays a brief description of the internal code change.

Additional functions are available from this window:

EC Details...
To display detailed information for the selected internal code change, click **EC Details...**.

Query Additional Actions...

Note: This option is only available if the selected object is at Version 2.10.0 or later.

To display information for additional actions that are pending, click **Query Additional Actions...**. The **System Information Query Additional Actions** window is displayed. If further actions are required, instructions are provided, otherwise **NO** appears. Click **OK** to close the window.

OK
To close this window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Retrieved Level

This field displays the internal code change level that was most recently copied for an object, making it available for installation.

Compare the number in this field with the number displayed for the **installed level** to determine whether your latest available change level has been installed:

- If the retrieved level is higher than the installed level, then the change level has been retrieved, but has not been installed.

  The object, when activated, will operate without your latest available level of the internal code change.
- If the retrieved level is equal to the installed level, then the change level has been retrieved and installed.

  The object, when activated, will operate with your latest available level of the internal code change.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Installable Concurrent

This field displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for an object, from the current installed level up to and including the installable concurrent level, without disrupting the operations of the console or the operations of the selected system.

Compare the number in this field with the number displayed for the **installed level** to determine whether one or more retrieved change levels can be installed and activated concurrently:

- If the installable concurrent level is blank, then none of the retrieved change levels from the current installed level up to and including the current retrieved level can be installed and activated concurrently.
- If the installable concurrent level is equal to the installed level, then all of the retrieved change levels that can be installed and activated concurrently are already installed.

  Note: Compare the installable concurrent level with the **activated level**. If they are equal, then the installed concurrent change levels are also already activated. Otherwise, you can use console tasks for changing internal code to activate concurrent internal code changes for the object.
- If the installable concurrent level is higher than the installed level, then all retrieved change levels from the current installed level up to and including the installable concurrent level can be installed and activated concurrently.

  Note: You can use console tasks for changing internal code to install and activate concurrent internal code changes for the object.

  For example, when:

  – The **Installed Level** is: 002.

  – And the **Installable Concurrent Level** is: 004.

  Then you can use console tasks for changing internal code to install change levels: 003 and 004, and then activate them without disrupting the operations of the console or selected system.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Activated Level

This field displays the internal code change level that was most recently activated as a working part of the licensed internal code of an object.

Compare the number in this field with the number displayed for the **installed level** to determine whether a more recent change level has been installed:

- If the installed level is higher than the activated level, then a more recent change level has been installed, but has not been activated.

  The object is operating without your latest available level of the internal code change.
- If the installed level is equal to the activated level, then the change level has been installed and activated.

  Note: Compare the installed level with the **retrieved level** to determine whether the object is operating with your latest available level of the internal code change.

If the retrieved change level is installed and activated, compare the number in this field with the number displayed for the **accepted level** to determine whether your latest available change level has been accepted:

- If the activated level is higher than the accepted level, then the change level has been activated, but has not been accepted.

  The object is operating with your latest available level of the internal code change, but it is not yet a permanent working part of the licensed internal code of the object.
- If the activated level is equal to the accepted level, then the change level has been activated and accepted.

  Your latest available level of the internal code change is a permanent working part of the licensed internal code of the object.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Accepted Level

This field displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the object.

Compare the number in this field with the number displayed for the **activated level** to determine whether a more recent change level has been activated:

- If the activated level is higher than the accepted level, then a more recent change level is currently activated, but it is not yet a permanent working part of the licensed internal code of the object.
- If the accepted level is equal to the activated level, then the change level currently activated is a permanent working part of the licensed internal code of the object.

  Note: Check the **retrieved level** and **installed level** to determine whether the object is operating with your latest available level of the internal code change.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

System Information

Use this task to display information about the internal code changes stored on the Support Element of the selected systems.

Licensed internal code, also referred to as internal code, controls many of the operations available on the console or on the systems and their Support Elements. Internal code changes may provide new internal code, or correct or improve existing internal code.

A console or a systems Support Element automatically keeps records of information about the internal code changes stored on it. The record-keeping begins when changes are retrieved from their source to the console or a systems Support Element. For each internal code change the information identifies:

- Its part number and Engineering Change (EC) number, type, and description
- The change level most recently retrieved
- The highest retrieved internal code change level that can be installed and activated concurrently
- The change level most recently activated
- The change level most recently accepted
- Additional details include the most recent date and time each task was performed.

The information may assist you with planning and managing the internal code change process. For example, review the information to either:

- Determine whether the console or system is operating with your latest available levels of internal code changes.
- Determine which tasks you must perform next to make the console or system operate with the latest available levels of internal code changes.

Note: A service representative will provide assistance applying and managing internal code changes.

Machine Information

EC number
Displays the Engineering Change (EC) number of the Hardware Management Console or selected systems where the internal code changes are applied.

Type
Displays the machine type of the Hardware Management Console or selected systems where the internal code changes are applied.

Version
Displays the version of the Hardware Management Console or selected systems where the internal code changes are applied.

LIC control level
Displays the Licensed Internal Code level of the Hardware Management Console or selected systems where the internal code changes are applied.

Model number
Displays the machine model number of the Hardware Management Console or selected systems where the internal code changes are applied.

Engineering Changes AROM
This label is displayed when the system is preloaded for disruptive activation of a new Engineering Changes (ECs) level.

Serial number
Displays the machine serial number of the Hardware Management Console or selected systems where the internal code changes are applied.

Driver
Displays the driver level of the Hardware Management Console or selected systems where the internal code changes are applied.

Note: The Driver information only appears if you are using this task with a user ID definition that is based on the *Service Representative* task roles.

Bundle level
Displays the bundle level of the Hardware Management Console or selected systems where the internal code changes are applied.

Note: This information is not available for IBM zEnterprise 196 and IBM zEnterprise 114 machines and earlier.

Internal Code Change Information

For additional information about an internal code change, select an EC number, then click **EC Details...**.

EC Number
Displays the engineering change (EC) number of the internal code change.

Retrieved Level
Displays the internal code change level that was most recently copied to the console or Support Elements of the systems, making it available for installation.

Installable Concurrent
Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for this console or for the systems, from the current installed level up to and including the installable concurrent level, without disrupting the operations of the systems defined to this console or the operations of the selected systems.

Activated Level
Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the console selected systems.

Accepted Level
Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the console selected systems.

Description
Displays a brief description of the internal code change.

Additional functions are available from this window:

EC Details...
To display detailed information for the selected internal code change, click **EC Details...**.

Query Additional Actions...

Note: This option is only available if the selected object is at Version 2.10.0 or later.

To display information for additional actions that are pending, click **Query Additional Actions...**. The **System Information Query Additional Actions** window is displayed. If further actions are required, instructions are provided, otherwise **NO** appears. Click **OK** to close the window.

OK
To close this window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Retrieved Level

This field displays the internal code change level that was most recently copied for an object, making it available for installation.

Compare the number in this field with the number displayed for the **installed level** to determine whether your latest available change level has been installed:

- If the retrieved level is higher than the installed level, then the change level has been retrieved, but has not been installed.

  The console, when activated, will operate without your latest available level of the internal code change.
- If the retrieved level is equal to the installed level, then the change level has been retrieved and installed.

  The console, when activated, will operate with your latest available level of the internal code change.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Installable Concurrent

This field displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for an object, from the current installed level up to and including the installable concurrent level, without disrupting the operations of the console or the operations of the selected systems.

Compare the number in this field with the number displayed for the **installed level** to determine whether one or more retrieved change levels can be installed and activated concurrently:

- If the installable concurrent level is blank, then none of the retrieved change levels from the current installed level up to and including the current retrieved level can be installed and activated concurrently.
- If the installable concurrent level is equal to the installed level, then all of the retrieved change levels that can be installed and activated concurrently are already installed.

  Note: Compare the installable concurrent level with the **activated level**. If they are equal, then the installed concurrent change levels are also already activated. Otherwise, you can use console tasks for changing internal code to activate concurrent internal code changes for the object.
- If the installable concurrent level is higher than the installed level, then all retrieved change levels from the current installed level up to and including the installable concurrent level can be installed and activated concurrently.

  Note: You can use console tasks for changing internal code to install and activate concurrent internal code changes for the object.

For example, when:

- The **Installed Level** is: 002.
- And the **Installable Concurrent Level** is: 004.

Then you can use console tasks for changing internal code to install change levels: 003 and 004, and then activate them without disrupting the operations of the console or selected systems.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Activated Level

This field displays the internal code change level that was most recently activated as a working part of the licensed internal code of an object.

Compare the number in this field with the number displayed for the **installed level** to determine whether a more recent change level has been installed:

- If the installed level is higher than the activated level, then a more recent change level has been installed, but has not been activated.

  The object is operating without your latest available level of the internal code change.
- If the installed level is equal to the activated level, then the change level has been installed and activated.

  Note: Compare the installed level with the **retrieved level** to determine whether the object the object is operating with your latest available level of the internal code change.

If the retrieved change level is installed and activated, compare the number in this field with the number displayed for the **accepted level** to determine whether your latest available change level has been accepted:

- If the activated level is higher than the accepted level, then the change level has been activated, but has not been accepted.

  The objectis operating with your latest available level of the internal code change, but it is not yet a permanent working part of the licensed internal code of the object.
- If the activated level is equal to the accepted level, then the change level has been activated and accepted.

  Your latest available level of the internal code change is a permanent working part of the licensed internal code of the object.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Accepted Level

This field displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the object.

Compare the number in this field with the number displayed for the **activated level** to determine whether a more recent change level has been activated:

- If the activated level is higher than the accepted level, then a more recent change level is currently activated, but it is not yet a permanent working part of the licensed internal code of the object.
- If the accepted level is equal to the activated level, then the change level currently activated is a permanent working part of the licensed internal code of the object.

Note: Check the **retrieved level** and **installed level** to determine whether the object is operating with your latest available level of the internal code change.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Internal Code Change Details

This window displays details for an internal code change.

Attention: A service representative will provide new internal code changes and manage their initial use.

For internal code changes already retrieved, you should manage these changes only under the supervision of a service representative or with the assistance of the support system.

Selected Internal Code Change Item

Part number
Displays the part number of the internal code change.

Engineering change number
Displays the engineering change (EC) number of the internal code change.

Engineering change type
Identifies the type of internal code affected by the internal code change.

Base ECs
Indicates the internal code change affects the base internal code of the system.

National language EC
Indicates the internal code change affects the internal code for a specific national language.

Other optional EC
Indicates the internal code change affects internal code other than base or national language internal code.

Engineering change description
Displays a brief description of the internal code change.

Internal Code Change State Details

Type
Identifies the internal code change states of an internal code change.

Level
Displays the change level of the selected internal code change in the state.

Date
Displays the date the change level was put in the state.

Time
Displays the time the change level was put in the state.

Additional functions are available from this window:

OK
To close this window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

System Information Error

An error occurred when attempting to retrieve the system information for the objects listed below.

Use this window to view system information retrieval error details.

Select an object, click **Error Details...** to view the cause for this error.

OK
To close this window, click **OK**.

Error Details...
To view the cause for the selected error, click **Error Details...**.

Help
To display help for the current window, click **Help**.

System Input/Output Configuration Analyzer

Accessing the System Input/Output Configuration Analyzer task

This task is used to analyze and help you manage your current System Input/Output Configuration (SIOC). The data can be viewed in several different arrangements giving emphasis to one item. You can filter the data and it will be applied to all applicable views. You can also sort the data for the view you are currently observing. However, the results when sorting on the PCHID Control Unit or PCHID Partition views will be grouped together.

To analyze this information:

1. Select a CPC (server).
2. Open the **System Input/Output Configuration Analyzer** task. The System Input/Output Configuration Analyzer window is displayed. Initially, the PCHID Control Unit View window displays the current I/O configuration data by the PCHID control unit.

   A menu bar is displayed at the top of the window with the following options:

   - Select **File** to:
     - Save Data to USB Flash Memory Drive (This option is available only if you are accessing the Hardware Management Console locally.)

       Insert a USB flash memory drive so the data can be copied. A progress window is displayed when the operation has completed.
     - Refresh
     - Exit
   - Select **View** to display the following types of information you want displayed in the table:
     - PCHID Control Unit
     - PCHID Partition
     - Control Unit
     - Link Load
     - Node ID
   - Select **Filter** to display a smaller, narrowed down version of the information in the table you are working with. Some of the filter options may include:
     - PCHID
     - CSS.CHPID
     - Switch
     - Partition
     - Control Unit
     - Show All

- Select **Sort** to arrange the data in the table in descending or ascending order depending on the parameters you specified.

3. When you have finished reviewing this information, select **File** from the menu bar, then **Exit** to end the task and return to the Hardware Management Console workplace.

System Input/Output Configuration Analyzer

Use **System Input/Output Configuration Analyzer** to analyze and help manage your current I/O configuration on the support element.

Note: Any dynamic changes have to be saved and made active on the Support Element to display in the tool.

The data can be viewed in several different arrangements giving emphasis to one item.

- You may filter the data and it will be applied to all applicable views.
- You may sort the data for the view you are currently observing. However, the results when sorting on the PCHID control unit or PCHID partition views will be grouped together.

File

To perform an action to save displayed data for the current I/O configuration, refresh, or exit the window, select **File** from the menu bar. The following choices are available from the **File** drop-down menu:

Save Data to USB Flash Memory Drive

To save displayed data for the current I/O configuration to a USB flash memory drive, click **Save Data to USB Flash Memory Drive**.

Note: This option is only available if you are accessing the console locally.

Plug the USB flash memory drive into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

Save Data via FTP

To save displayed data for the current I/O configuration to a secure FTP location, click **Save Data via FTP**.

Refresh

To update the display window with the current I/O configuration data, click **Refresh**.

Exit

To end this task and return to the workplace, click **Exit**.

View

To display different views for the current I/O configuration data, select **View** from the menu bar. The following choices are available from the **View** drop-down menu:

PCHID Control Unit

Displays the current I/O configuration data by the PCHID control unit.

PCHID Partition

Displays the current I/O configuration data by the PCHID partition.

Control Unit

Displays the current I/O configuration data by the control unit.

Link Load

Displays the current I/O configuration data by the link load.

Node ID

Displays the current I/O configuration data by the node ID.

Filter
To filter out or to display specific information for the current I/O configuration, select **Filter**. The data entered is applied to all the views that contain the data and the information is displayed. From the menu, select the data that you want to be filtered. Some of the filter options may include:

PCHID
Allows you to enter the PCHID to filter on.

CSS.CHPID
Allows you to enter the CSS.CHPID to filter on.

Switch
Allows you to enter the switch to filter on.

Partition
Allows you to enter the partition to filter on.

Control Unit
Allows you to enter the control unit to filter on.

Show All
Allows you to display all the current I/O configuration data.

Sort
To sort the current view, select **Sort**. The data is sorted using the parameters specified and then the view is displayed. Only the current view is sorted with the exception of PCHID control unit and PCHID partition views. These views are tightly coupled.

Help
To display help for the current window, click **Help**.

System Input/Output Configuration Analyzer

Use this window to export displayed data for the current I/O configuration to a specified FTP destination. Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Export
To export the displayed current I/O configuration data to an FTP destination, click **Export**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

System Input/Output Configuration Analyzer - Filter

Use this window to enter specific data on how you want the data to be displayed (for example, if filtering PCHIDs and you entered 0120 then all data related to PCHID 0120 will be displayed). The data entered is applied to all the views that contain the data and the information is displayed.

OK
To perform the filter action you entered, click **OK**.

Cancel
To close the current window, click **Cancel**.

Help
To display help for the current window, click **Help**.

System Input/Output Configuration Analyzer - Sort

Use this window to enter specific data on how you want the current I/O configuration to sort the displayed information. If you want to sort the current window columns in ascending order, you must indicate it on the window.

OK
To perform the sort action you entered, click **OK**.

Cancel
To close the current window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Task Information

Object Selection

Use this window to select the object that the task will be performed on. This task can only be performed on a **single** object. Select an object from the Object Name list and click **OK**.

Object Name
This list displays the objects that may be targeted for the selected task.

Note: Only a single target object may be chosen at one time. Select an entry in the list to view the profile that will be used for that object.

OK
To perform the task on the object you chose, click **OK**.

Cancel
To end the task and exit the window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Secondary Object Notification for Disruptive Task

One or more of the objects to be targeted for the selected task have associated secondary objects that will also be affected by this task. The selected task is considered to be disruptive and will also cause disruption to the associated secondary objects. Use this window to review the list of secondary objects that will also be affected before continuing this task.

Service Status
This list displays the secondary objects that will be affected by the task as well as their current operating status.

Yes
To continue with the task, click **Yes**, understanding that the secondary objects listed will also be affected.

No
To end the task, click **No**, without disrupting the secondary objects.

Help
To display help for the current window, click **Help**.

Single Task Confirmation

Use this window to review the displayed objects before proceeding with the task.

Object Names
This list displays the objects that are to be targeted for the selected task.

Note: Select an entry in the list to view the profile that will be used for that object.

Yes
To perform the task on the objects displayed in the list, click **Yes**.

No
To end the task and exit the window without saving any changes, click **No**.

Help
To display help for the current window, click **Help**.

Invalid Target Object List

This window appears when one or more of the targeted objects for a selected task have a status that would cause the task to fail. Use this window to view the list of objects targeted for the selected task and the reason the targeted objects can or cannot be used to perform the selected task.

Object Status
This list displays the object names and the reason why the object can or cannot perform the selected task. Review the object list to determine which objects are currently not valid for the task.

Yes

To continue the task with only the valid objects as targets, click **Yes**.

No

To end the task and exit the window, click **No**.

Help
To display help for the current window, click **Help**.

Multiple Task Confirmation

Use this window to review the displayed objects and confirmation text for each object before proceeding with the task.

Object Status
This list displays the objects that are to be targeted for the selected task.

Note: Select an entry in the list to view the profile that will be used for that object.

Yes
To perform the task on the objects displayed in the list, click **Yes**.

No
To end the task and exit the window without saving any changes, click **No**.

Help
To display help for the current window, click **Help**.

Task Progress

Targeted Progress

This window displays the estimated duration and elapsed time of an active task. The name of the task in progress is displayed in the window title.

This window is also for a task that has multiple targets. The table displays one line for each of the targets of the task. Each line includes the name and the task status of the objects on which the task is performed. These lines are updated one at a time as a task finishes its processing for each of the targets.

Estimated function duration time
This displays the estimated amount of time necessary to complete the task.

Note: The function duration time when deactivating an object may not match the elapsed time because the operating system installed on the object may respond differently to the shutdown request.

Elapsed time
This displays the actual amount of time that has passed as the task progresses.

OK
To close the window when the task completes, click **OK**.

Details...
To display additional information about the selected object, click **Details...**.

Force
To override the normal processing shutdown of the selected object without waiting for the operating system to respond, click **Force**.

Cancel
To cancel running the task, click **Cancel**. This is not available for all tasks. If **Cancel** is available and you click it, it becomes disabled while the task tries to end. **Cancel** does not close the window.

Help
To display help for the current window, click **Help**.

Force termination

Use this window to view object(s) that you are requesting a force termination.

Object Name
Displays the name of the object(s) to force a termination.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Select All/Deselect All
You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions are available from this window:

OK
To continue with the force termination of the listed objects(s), click **OK**.

Cancel
To close the window without forcing a termination on the listed object(s), click **Cancel**.

Help
To display help for the current window, click **Help**.

Non-Targeted Progress

This window displays the estimated duration and elapsed time of an active task. The name of the task in progress is displayed in the window title.

This window is for a task that has a single target. The table displays progress information for the task.

Estimated function duration time
This displays the estimated amount of time necessary to complete the task.

Elapsed time
Displays the actual amount of time that has passed as the task progresses.

Progress table
This table displays the status of the task for the object. The status is a brief message indicating the progress of the task.

OK
To close the window when the task completes, click **OK**.

Details...
To display additional information about the object, click **Details...**.

Cancel
To cancel running the task, click **Cancel**. This is not available for all tasks. If **Cancel** is available and you click it, it becomes disabled while the task tries to end. **Cancel** does not close the window.

Help
To display help for the current window, click **Help**.

Tip of the Day

Accessing the Tip of the Day task

This task allows you to view information about using the Hardware Management Console. A different fact or tip is displayed each time you log on.

To control the tip of the day message:

1. Open the **Tip of the Day** task. The Tip of the Day window is displayed.
2. You can select the following options from this window:

- Select **Show tips each time you log on** to display a tip each time you log on to the Hardware Management Console.
- Click **Previous Tip** or **Next Tip** to scroll through the information.

Note: You can also control the display of the tips by using the **User Settings** task. From the User Settings window, select the **Controls** tab and select or deselect **Show tips each time you log on**.

3. Click **Close** when you have completed this task.

Toggle Lock

Accessing the Toggle Lock task

This task allows you to set a disruptive task lockout for the selected object.

Note: This task cannot be used on IBM Dynamic Partition Manager (DPM) objects.

To lockout an object:

1. Select the **Toggle Lock** task from the Tasks Index. The Target Object Selection window is displayed.
2. Choose one or more objects, then click **OK**. The object or objects selected displays a lock icon. This indicates that the object is locked and a disruptive task cannot be performed. If you want to remove the lock, select the **Toggle Lock** task again.

   Note: You can also select the object first and then click **Toggle Lock** from the Tasks area of the window.

For more information on Disruptive tasks and locking an object, go to the Help Table of Contents and select **Introduction** > **Disruptive tasks** > **Locking an object**.

Transmit Console Service Data

Accessing the Transmit Service Data task

Note: If you want to access this task remotely you must enable access to the support system.

This task allows you to send service data by copying it to a removable media (USB flash memory drive) for delivery, by transmitting it through a remote connection to the support system, or by transmitting data to an FTP server.

Sending service data is necessary only when service data is requested, usually through either your service representative or the support system. Typically, service data is requested after a problem is reported if analyzing the service data is necessary to determine the cause of the problem.

Service data is a set of system information, such as program and event traces, collected by the Support Element. Service data assists the service representative in servicing the problem.

To send the Support Element's service data:

1. Select the system.
2. Open the **Transmit Service Data** task. The Transmit Service Data window is displayed.
3. Select the data you want to send and the destination for the data. You can also enter the related problem management number if it is known.
4. Click **Send** to transmit the selected data or **Cancel** to end the task without sending any data.

Accessing the Transmit Console Service Data task

This task provides the ability to send information that is stored on the Hardware Management Console hard disk that can be used for problem determination.

The data may be *traces, logs*, or *dumps* and the destination for the data may be the support system, removable media (USB flash memory drive), or by transmitting data to an FTP server.

Before you can send information to the support system it must be *enabled*. To enable remote service, see the **Customize Console Services** task.

To transmit console service data:

1. Open the **Transmit Console Service Data** task. The Transmit Service Data window is displayed.
2. Select the type of data you want transmitted along with any additional information, including the destination.
3. Click **Send** to send the information to the selected destination or **Cancel** to exit the task without sending any information.

Transmit Service Data

Use this window to select the types of service data and how it is to be sent.

Service data is a set of program and event traces and storage dumps. The data in the traces and the contents of storage assists in servicing the system.

Use this window only when directed by your service representative or support system. Select the service data categories requested. Service data in selected categories is collected in a file or group of files for transmission.

Before you can send information to the support system, *call-home server* and *remote service* must be enabled.

Note: Some service data categories may not be available for selection. Such categories appear grayed. This indicates that no data is available for that category.

Service Categories:

"Service Data Destination" on page 1382
Use this section to specify how your service data is sent.

Note: The removable media selection is the only destination allowed on the alternate SE.

"Service Data Selections" on page 1384
Use the displayed categories in this section to select the types of service data to send.

"Problem Management Hardware Number" on page 1384
If provided, specify the five character alphanumeric number that identifies the problem.

"Virtual Support Repository Files" on page 1384
Use this section to transmit a data service file or a group of data service files to the support system.

Additional functions are available from this window:

Send
To send service data to the selected destination, click **Send**. The Select Media Device window is displayed. From this window you can choose the media you want to send the data to. You can click **OK** to continue with the task, click **Refresh** to re-display your media selections, or click **Cancel** to return to the previous window.

Cancel
To exit this task without making any selections, click **Cancel**.

Reset
To clear current selections, click **Reset**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Service Data Destination

Use this section to specify how your service data is sent to the support system.

The following options are available:

Support System
To use the Remote Support Facility (RSF) to transmit the service data to the support system, select **Support System**.

Removable media
To copy the service data to a removable media (USB flash memory drive), select **Removable media**.

Notes:

- When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.
- This option is not available if the console is running remotely.

FTP Server
To transfer data using an FTP server, select **FTP Server**.

Service Data Send to FTP Server

Use this window to configure FTP settings when you use an external server to transmit your files to the specified directory.

Host name
Specify the host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved. This is a required field.

Transmit
To submit this information to the specified directory, click **Transmit**.

Cancel
To close the window without providing information, click **Cancel**.

Help
To display help for the current window, click **Help**.

Service Data Selections

Use the displayed categories in this section to select the types of service data to send to the support system.

Select one or more service data categories as requested. Service data in selected categories is collected in a file or group of files for transmission to the support system.

Problem Management Hardware Number

The Problem Management Hardware (PMH) number is five alphanumeric characters and is provided by a service representative.

When sending data on a removable media, the removable media can be formatted in the **Format Media** task with an internal volume label of SRVDAT.

The problem management hardware number is used for problem identification. If the data that is being sent is not problem oriented, or a number has not been issued, this field is optional.

Note: At this time the number cannot be validated.

Virtual Support Repository Files

Use this window to transmit a data service file or a group of data service files to the support system.

Note: This field is displayed only during a service call.

Enter the file name or a global file name (for example, **/console/data/iqyylog.log** or **d:IOCKIQZK*.***), and then click **Send**.

List of restrictions on the file name:

- Only the console's hard drives are valid.
- Standard wild cards (* and ?) apply.
- Specifying an entire directory or subdirectory is not allowed.

Transmit Vital Product Data (HMC)

Accessing the Transmit Vital Product Data task

This task collects Vital Product Data (VPD) from the Hardware Management Console and either transmits the data to the support system or stores the information on diskette (if one is available), USB flash memory drive, or the Hardware Management Console hard disk.

Note: To transmit the data to the support system, the Hardware Management Console must be enabled for using the Remote Support Facility (RSF). If the Hardware Management Console is not equipped and enabled for using the RSF, select **Diskette** to copy the VPD to a diskette to mail to the support system.

To transmit vital product data:

1. Open the **Transmit Vital Product Data** task. The Transmit Vital Product Data window is displayed.
2. Select one of the VPD destinations.
3. Click **OK** to continue with the task, or **Cancel** to end the task.

Transmit Vital Product Data

Use this window to select the method for sending the Hardware Management Console's Vital Product Data (VPD) to the support system.

Vital Product Data Destination

Select the vital product data destination, then click **OK**.

Support system
To transmit vital product data to the support system, select **Support system**.

The Hardware Management Console must be equipped and enabled for using the Remote Support Facility (RSF) to use this destination.

USB flash memory drive
To copy vital product data to a USB flash memory drive, select **USB flash memory drive**.

If the USB flash memory drive is not already inserted, insert it into a USB port, then click **OK**. The **Select Media Device** window is displayed. From this window you can select the USB flash memory drive you want to send VPD to. You can click **OK** to continue with the task, click **Refresh** to redisplay your media selections, or click **Cancel** to return to the previous window.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Hardware Management Console hard disk
To copy vital product data to the hard disk, select **Hardware Management Console hard disk**.

FTP server
To copy vital product data to an FTP server, select **FTP server**.

Additional functions are also available from this window.

OK
To transmit vital product data to support system by the destination you selected, click **OK**. If you selected media as the destination, the **Select Media Device** window is displayed. From this window you can choose the media you want to send the data to. You can click **OK** to continue with the task, click **Refresh** to redisplay your media selections, or click **Cancel** to return to the previous window.

Cancel
To close this window without saving any of the changes made to transmit vital product data to the support system, click **Cancel**.

Help
To display help for the current window, click **Help**.

Transmit Vital Product Data (SE)

Accessing the Transmit Vital Product Data task

This task provides a window for you to collect Vital Product Data (VPD) from the Support Element of all CPCs that are defined to your Hardware Management Console and to either transmit the data to the support system or to store the information on USB flash memory drive or Hardware Management Console hard disk.

To send vital product data from the Support Element to the Hardware Management Console:

1. Select one or more CPCs (servers).
2. Open the **Transmit Vital Product Data** task. The Transmit Vital Product Data window is displayed.
3. Select the type of vital product data you want to transmit from the Transmit Vital Product Data window:
   - System (Support Element) vital data
   - Hardware Management Console vital product data
4. Select the destination to which you want to transmit:
   - Support system
   - USB flash memory drive

- Hardware Management Console hard disk

and then click **OK** to proceed.

Transmit Vital Product Data

Use this window to select the type of Vital Product Data (VPD) that you want transmitted and select a method for sending the VPD to the support system. VPD data can be retrieved from one or more systems, or from the Hardware Management Console.

Vital Product Data to be Transmitted
Select the type of Vital Product Data (VPD) to be transmitted. Only one choice may be selected at one time (either system (Support Element) or Hardware Management Console data).

System (Support Element) vital product data
To transmit vital product data for one or more selected Central Processor Complexes (CPCs), select **System (Support Element) vital product data**.

Select all CPCs that you want to transmit vital product data for.

Hardware Management Console vital product data
To transmit vital product data for the Hardware Management Console, select **Hardware Management Console vital product data**.

Vital Product Data Destination
Select the vital product data destination, then click **OK**.

Support system
To transmit vital product data to support system, select **Support system**.

The console must be equipped and enabled for using the Remote Support Facility (RSF) to use this destination.

USB flash memory drive
To copy vital product data to a USB flash memory drive, select **USB flash memory drive**.

Then insert a USB flash memory drive into a USB port, and click **OK**.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Hardware Management Console
To copy vital product data to the hard disk, select **Hardware Management Console hard disk**.

FTP server
To copy vital product data to an FTP server, select **FTP server**. Ensure you have defined the FTP destination using the **Configure Backup Settings** task.

OK
To transmit vital product data to the support system based on the selections that you chose, click **OK**. If you selected media as the destination, the **Select Media Device** window is displayed. From this window you can choose the media you want to send the data to. You can click **OK** to continue with the task, click **Refresh** to redisplay your media selections, or click **Cancel** to return to the previous window.

Cancel
To close this window without transmitting vital product data to the support system, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update PCI Adapter Internal Code

Accessing Update PCI Adapter Internal Code task

To update PCI adapter internal code:

1. Locate and open the **Update PCI Adapter Internal Code** task.

   The Update PCI Adapter Internal Code window displays.

Update PCI Adapter Internal Code

Use this window to view and update the PCI adapters which have pending internal code updates for the selected PCHIDs.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

PCHID
Indicates the PCHID that is assigned to the PCHID adapter

State
Indicates the current state of the PCHID

Status
Indicates the current status for the selected PCHID

Type
Indicates the PCI adapter type for the selected PCHID

Number of Online IDs
Indicates the number of online PCI adapter IDs. Select the hyperlink to display the PCI adapter IDs associated the PCHID

Adapter Changes Pending Install and Activate
Indicates there are staged MCL updates which causes the Update Pending conditions once an Install/Activate is performed for the selected PCHID. It is recommended to use the **Change Internal Code** task prior to updating the selected PCHID.

Note: This column displays for SERVICE mode only.

Pending Update
Indicates a PCI adapter internal code update is pending for the selected PCHID.

The icons perform the following functions in the PCHID definition table:

Select All/Deselect All
You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Update Adapter Firmware
To update the firmware internal code on the selected PCHID(s), select **Update Adapter Firmware**.

Close
To close this window and exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

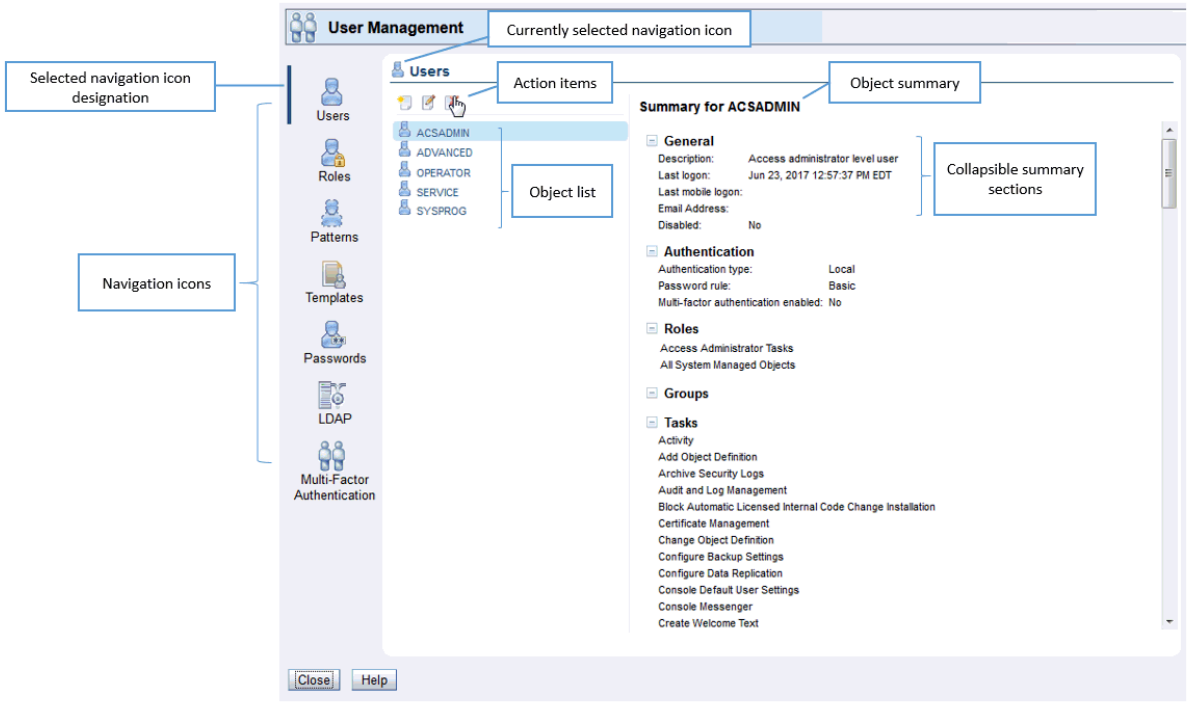
User Management

Accessing the User Management task

This task is used by an access administrator or a user that is assigned Access Administrator Tasks role to manage users, roles, user patterns, user templates, password rules, LDAP server definitions, and multi-factor authentication for your system users that log on to the console. This task can also be used when no administrator role is provided as view only for their own user information. The user can change their own password and set a default group.

To manage user access and permissions to the console:

1. Open the **User Management** task in access administrator role. The **User Management** dashboard is displayed.



2. Select the icon for the area of user management you want to customize. Users is the first icon in the navigation pane and is the default selection when the User Management dashboard is opened.

3. Select a currently defined object from the object list to view the current values in the object summary area.
4. Select the icons above the objects list to perform the following actions:

   New
   To create a new object

   Details
   To view or modify existing properties for the selected object

   Delete
   To delete the selected object

User Management

This task gives the access administrator a common area to view and manage users, roles, user patterns, user templates, password rules, and LDAP server definitions for your system. The navigation icons on the dashboard are listed in the order of highest usage and not the sequence an administrator would use to initially set up access to the console. See “Getting Started” on page 1391 for some scenarios to assist an administrator with first time usage of the **User Management** dashboard. See “Default Permissions” on page 1404 for the list of permissions that are granted to every user by default and therefore not shown on the **User Management** dashboard.

To use the User Management dashboard:

1. Select the icon for the area of user management you want to customize. Users is the first icon in the navigation pane and is the default selection when the User Management dashboard is opened.

   Note: Only icons permitted for the current user display (For example, the **Roles** icon is shown to users who have permission to the **Manage User Roles** task.) See the navigation icon description for the permissions that correspond to the icons.
2. Select a currently defined object from the object list to view the current values in the object summary area.
3. Select the icons above the objects list to perform the following actions:

   New
   To create a new object

   Details
   To view or modify existing properties for the selected object

   Delete
   To delete the selected object

The navigation icons are as follows:


Users

A *user* object defines the user's authentication, roles which determine access permissions, and a default group to which any objects created by the user will be added. Select “Users” on page 1404 to create a new user or modify user properties. Permission to the **Manage Users** task is required for the capability of managing users other than the current user.


Attention: In the state of California, US, the use of default passwords are no longer allowed. The first time a default user ID logs on to the console, the default password must be changed. A prompt is displayed requiring the password change. This is initiated in this task by SERVICE or a user that is assigned a role with Manage Users task permission.


Roles

A *role* defines permissions to tasks, type of objects or specific objects, groups, and task lists. Select “Roles” on page 1413 to create a new role or modify role properties. Permission to the **Manage User Roles** task is required for the icon and corresponding dashboard view to be available.

User Patterns

A *user pattern* is used to automatically create users on this system based on successful authentication of user IDs that conform to a defined string pattern. The user pattern requires a template definition to specify the user capabilities. Select "User Patterns" on page 1422 to create a new user pattern or modify user pattern properties. Permission to the **Manage User Patterns** task is required for the icon and corresponding dashboard view to be available.

User Templates

A *user template* defines the settings and permissions for users authenticated with a user pattern. The template requires an LDAP server definition. Select "User Templates" on page 1429 to create a new user template or modify user template properties. Permission to the **Manage User Templates** task is required for the icon and corresponding dashboard view to be available.

Password Rules

A *password rule* defines a set of rules to be used when creating a user password. Select "Password Rules" on page 1436 to create a new password rule or modify password rule properties. Permission to the **Manage Password Rules** task is required for the icon and corresponding dashboard view to be available.

LDAP Server Definitions

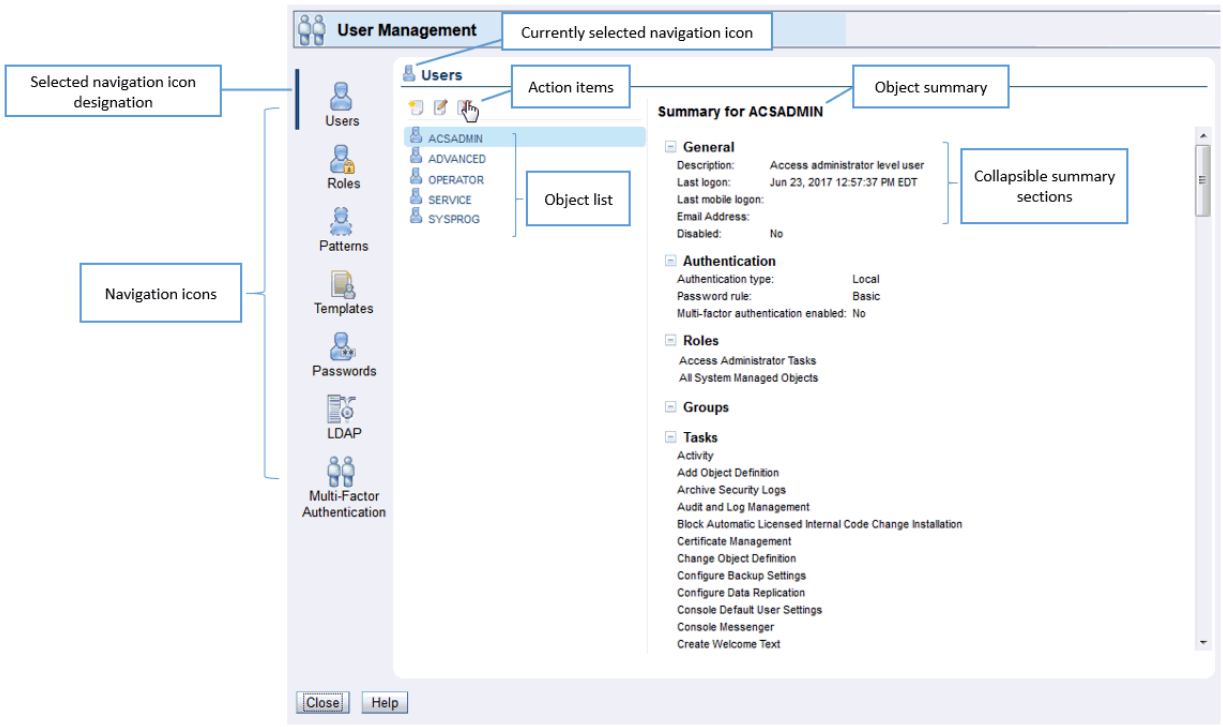
An *LDAP server definition* specifies host connection and directory entry location information to be used for authentication. Select "LDAP Server Definitions" on page 1442 to create a new LDAP server definition or modify LDAP server definitions. Permission to the **Manage LDAP Server Definitions** task is required for the icon and corresponding dashboard view to be available.

Multi-Factor Authentication

A *multi-factor authentication* requires additional security tokens to verify the identity of a user when logging on to the console. Select "Multi-Factor Authentication" on page 1447 to enable multi-factor authentication for users and user templates. Permission to the **Manage Multi-factor Authentication** task is required for the icon and corresponding dashboard view to be available.

Note: Each of the views for the User Management dashboard is only displayed if the current user has access to their corresponding task.

The user management interface is comprised of several major components: the navigation icon area, the object list, and the object summary.



Navigation icon area
The navigation icon area is located in the left portion of the window and provides a common area for an administrator to work with all aspects of user access to the console. You can hover over the icons to display the name of the icons.

Object list
The object list contains a list of the currently defined objects for the selected navigation icon.

Object summary
The object summary displays the current values for the selected item in the object list.

Getting Started

The **User Management** dashboard provides a common area for an administrator to work with all aspects of user access to the console. This section gives some common scenarios and the detailed steps for using the dashboard to accomplish a specific goal. The scenarios touch on each of the navigation areas: Users, Roles, User Patterns, User Templates, Password Rules, LDAP Server Definitions, and Multi-factor Authentication. Any reference to a page in the step-by-step instructions refers to the page listed in the left navigation (which might not match the page title).

The list of scenarios for getting started with the **User Management** dashboard are as follows. Click the links, in any order, to get the step-by-step details to accomplish the goal.

User default changes from Version 2.13.1 to Version 2.14.0

The table below lists the default changes from Version 2.13.1 to Version 2.14.0 for increased security and ease of use.

Table 18. User default changes from Version 2.13.1 to Version 2.14.0

Setting	Previous Default (Version 2.13.1)	New Default (Version 2.14.0)
New User		

Table 18. User default changes from Version 2.13.1 to Version 2.14.0 (continued)		
Setting	**Previous Default (Version 2.13.1)**	**New Default (Version 2.14.0)**
Email address	Not available	Provide address to enable; requires Simple Mail Transfer Protocol (SMTP) setup in **Monitor System Events** task
Users		
STORAGEADMIN default user ID	Not available	Task and resource permissions to the DPM **Configure Storage** task
User Pattern		
User setting retention time	Disabled, now suggesting 1 when enabled	90 days
Multi-factor Authentication		
Multi-factor Authentication	Not available	Select users and templates to enable
Reset shared secret keys	Not available	Select users and templates to reset

User default changes from Version 2.12.1 to Version 2.13.0

The table below lists the default changes from Version 2.12.1 to Version 2.13.0 for increased security and ease of use.

Table 19. User default changes from Version 2.12.1 to Version 2.13.0		
Setting	**Previous Default (Version 2.12.1)**	**New Default (Version 2.13.0)**
New User		
Description	Required	Not required
Password rule	Basic	Standard
Force user to change password	Not checked	Checked
Managed objects/roles	Required to select 1 or more of each	Not required
Session timeout	Disabled, indicated by 0	Disabled, now suggesting 300 when enabled
Idle timeout	Disabled, indicated by 0	Disabled, now suggesting 20 when enabled
Delay login after failed attempts	Disabled	Enabled
Number of failed attempts before disable delay	0	3
Delay (minutes) (for login delay after failed attempts)	0	1
Minimum time between password changes	Disabled, indicated by 0	Disabled, now suggesting 1440 when enabled

Table 19. User default changes from Version 2.12.1 to Version 2.13.0 (continued)		
Setting	**Previous Default (Version 2.12.1)**	**New Default (Version 2.13.0)**
User Pattern		
Description	Required	Not required
User setting retention time	Blank, user must specify a value	Disabled, now suggesting 1 when enabled
User Templates		
Description	Required	Not required
Managed objects/roles	Required to select 1 or more of each	Not required
Session timeout	Disabled, indicated by 0	Disabled, now suggesting 300 when enabled
Idle timeout	Disabled, indicated by 0	Disabled, now suggesting 20 when enabled
Delay login after failed attempts	Disabled	Enabled
Number of failed attempts before disable delay	0	3
Delay (minutes) (for login delay after failed attempts)	0	1
Password Rule		
Case sensitive	No	Yes
LDAP Server		
Connection port	Blank	389
Use SSL connection	No change to connection port when toggled	Changes connection port from 389 to 636 when toggled

Create a new user based on a system default user

The goal of this scenario is to create a new user for John based on the SYSPROG default user. John requires the System Programmer level authority and access to all system resources (all objects of all types).

Steps to create a new user based on a system default user:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on user and select *SYSPROG*. In the User Details section enter *John* in the Name field. Optionally, enter meaningful text in the Description field to describe your user, and enter a valid email address in the Email Address field. Then click **Next**.

5. On the Authentication page, keep the default selection **HMC password authentication**. Leave the Password rule as the default *Standard*. Enter *johnpw* as the password in the Password and Confirm password fields, then click **Force user to change the password at next logon**, and then click **Next**.
6. On the Roles page, the roles *Defined System Managed Objects*, and *System Programmer Tasks* are preselected from the SYSPROG user. Select the check box for role *All Resources* to give John access to all objects of all types. Optionally, you can clear the check box on the row for role *Defined System Managed Objects*, since these permission are contained in the *All Resources* role. When complete, click **Next**.

   Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modification to user-defined roles from **Role Details**.
7. Review the details on the Summary page, then click **Finish**. The user John is created.
8. On the dashboard, user *John* is added to the Users list and is the current selected user. View the *Summary for John* to see the Roles, Groups, Tasks, Object Types, and Objects that John is granted permission.

John is now able to logon to the console with user ID *john* and password *johnpw*. John is required to change the password the first time he logs on.

Create a single customized role containing all desired task and object permissions

The **User Management** task provides the capability to include all desired permissions for tasks, objects, groups, and task lists in a single role. For administrators who are familiar with the **Customize User Controls** task in HMC version 2.12.1, **Customize User Controls** required separate roles to specify permissions for tasks, and separate roles for each object type. This scenario creates a single role that grants permission to the object types, tasks, and custom groups required for operations personnel. This role can then be assigned to your operations users.

Steps to create a custom role for your operations personnel:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on role and select *Operator Tasks*. (Roles are listed in alphabetic order. You can type the start of the role name in the box to narrow down the number of roles and make it easier to find your desired role for selection.) In the Role Details section, enter *Operators* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, and then click **Next**.
5. On the Tasks page, notice that the tasks from the system default role *Operator Tasks* are preselected. In addition to those tasks, select any other tasks you would like your operators to perform. As an example, select the row for *Customize/Delete Activation Profiles*. You can type *customize/* in the filter box to narrow the table to your desired selection, or you can scroll down to find the selection. When you've made all your task selections, click **Next**.
6. On the Objects by Type page, select the rows for the following object types:
   - *Defined CPC*
   - *LPAR Image*
   - *Pattern Match Group*
   - *User-defined Group*.

   Additionally, select any other desired object types, then click **Next**.
7. On the Specific Objects page, select any desired specific objects, then click **Next**.

8. On the Groups page, if any custom groups are available, select any desired custom groups you want your operators to be able to manage, then click **Next**. This page grants Group Management permission (ability to manage to the group, but not to manage the objects in the group).
9. On the Objects by Group page, if any custom groups are available, select any desired groups containing objects for which you want your operators to have permission, then click **Next**. This page grants Child Management permission (ability to manage the objects in the group, but does not grant permission to manage the group). You can click on the group name links to view the current contents of the group.
10. Review the details on the Summary page, then click **Finish**. The role *Operators* is created.
11. On the dashboard, the role *Operators* is added to the list of roles and is the current selected role. View the *Summary for Operators* to verify the Groups, Tasks, Object Types, and Object that the role granted permission are correct.

The role *Operators* can now be assigned to your operations personnel users.

Create a user who authenticated using an LDAP server

If you want to create users that authenticate using your Lightweight Directory Access Protocol (LDAP) server, you first need to create an LDAP server definition. Then you can specify LDAP authentication when you create your users.

Steps to create an LDAP server definition:

1. From the **User Management** dashboard, select the **LDAP Server Definitions** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New LDAP Server Definition** wizard is started.
3. On the Welcome page of the **New LDAP Server Definition** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Server Details section, enter *xyz-ldap* in the Name field. Optionally, enter meaningful text in the Description field to describe your server, then click **Next**.
5. On the Host Connection page, enter the name or IP address of your server in the Primary host name field. Specify any other appropriate selections as needed, then click **Next**.
6. On the Bind Information page, optionally supply appropriate bind credentials.
7. On the Directory Location page, select how to locate a user's directory entry. For example, select **Use DN pattern** and enter *uid={0},type=user,o=xyz.com* in the Pattern field, then click **Next.**
8. Review the details on the Summary page, then click **Finish**. The LDAP server definition xyz-ldap is created.

Steps to create the new user using LDAP authentication:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the User Details section, enter *Terry* in the Name field. Optionally, enter meaningful text in the Description field to describe your user, then click **Next**.
5. On the Authentication page, select **LDAP password authentication**. Click the drop-down list for the Server and select *xyz-ldap*. Optionally, enter an LDAP user ID in the User ID field, then click **Next**.
6. On the Roles page, select the desired roles for your user, then click **Next**.

Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Roles Details**.

7. Review the details on the Summary page, then click **Finish**. The user Terry is created.
8. On the dashboard, user *Terry* is the current selected user. *View the Summary for Terry* to see the Roles, Groups, Tasks, Object Types, and Objects that Terry is granted permission.

Terry is now able to logon to the console with user ID *Terry* and password specified in the xyz-ldap server. Terry cannot change the password via the console.

Authenticate all employees using an LDAP server

To grant console access to all employees at xyz.com using your Lightweight Directory Access Protocol (LDAP) server, you first need to create an LDAP server definition. Then create a user template defining the settings and permissions for your users. Finally, create a user pattern specifying the specific string pattern used to identify the specific authorized users.

Steps to create an LDAP server definition:

1. From the **User Management** dashboard, select the **LDAP Server Definitions** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New LDAP Server Definition** wizard is started.
3. On the Welcome page of the **New LDAP Server Definition** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Server Details section, enter *xyz-ldap* in the Name field. Optionally, enter meaningful text in the Description field to describe your server, then click **Next**.
5. On the Host Connection page, enter the name or IP address of your server in the Primary host name field. Specify any other appropriate selections as needed, then click **Next.**
6. On the Bind Information page, optionally supply appropriate bind credentials.
7. On the Directory Location page, select how to locate a user's directory entry. For example, select **Search a DN tree** and enter *ou=xyzpages,o=xyz.com* in the DN field. Enter *mail={0}* in the Search filter field, then click **Next**.
8. Review the details on the Summary page, then click **Finish**. The LDAP server definition xyz-ldap is created.

Steps to create a user template:

1. From the **User Management** dashboard, select the **User Templates** icon () in the navigation area.
2. Select the **New** icon (). The **New User Template** wizard is started.
3. On the Welcome page of the **New User Template** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the User Template Details section, enter *xyz-template* in the Name field. Optionally, enter meaningful text in the Description field to describe your user template, then click **Next**.
5. On the Authentication page, select the *xyz-ldap* server row from the table, then click **Next**.
6. On the Roles page, select the desired roles for your users, then click **Next**.

   Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.
7. Review the details on the Summary page, then click **Finish**. The user template xyz-template is created.

Steps to create the user pattern:

1. From the **User Management** dashboard, select the **User Patterns** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User Pattern** wizard is started.
3. On the Welcome page of the **New User Pattern** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Pattern Details section, enter *xyz-template* in the Name field. Optionally, enter meaningful text in the Description field to describe your user pattern, then click **Next**.
5. On the User Pattern page, select **Regular expression**. Optionally, click **Help** for details on use of regular expressions. Enter *.*@xyz.com* in the User pattern field, then click **Next**.
6. On the Template page, select the template *xyz-template*, then click **Next**.
7. Review the details on the Summary page, then click **Finish**. The user pattern xyz.com is created.

All user IDs ending in @xyz.com are now able to logon to the console with their LDAP user ID and password. Users are automatically created with the settings and permissions specified in the user template. For example, employee John Doe logs on with user ID johndoe@xyz.com using his LDAP password and then has permission to all roles specified in the xyz-template.

Verify who has permission to a task (for example, the Activate task)

To make sure you have granted the desired roles and users permission to a specific task, you can use the **Tasks** link on the **User Management** dashboard Roles view. The following example looks at the **Activate** task.

Steps to ensure you have the desired permission to the **Activate** task:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. In the **View by**: title, select the **Tasks** link. The dashboard view switches to list all tasks that can have customized permissions.
3. Select the **Activate** task in the objects list.
4. In the *Summary for Activate*, view the list of Users and User Templates that have access permission to the task and the set of Roles that contain the task.

Verify who has access to a specific object

To make sure that you have granted the desired roles and users permission to a specific object, you can use the **Objects** link on the **User Management** dashboard Roles view. The following example looks at the SYS_A object.

Steps to ensure you have the desired permission to the SYS_A object:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. In the **View by**: title, select the **Objects** link. The dashboard view switches to list all of the current system objects that can have customized permissions.
3. Select the SYS_A object in the objects list (scroll down if needed).
4. In the *Summary for SYS_A*, view the list of Users and User Templates that have access permission to the object and Roles that contain the object. You can also see which Tasks can be performed on this object.

Ensure all users are following your security standards for passwords

The **User Management** Password Rules view of the dashboard shows the list of password rules that can be assigned to users. The system defined password rules are Basic, Standard, and Strict. You can create your own customized password rules for your specific security requirements. In the example, the

password needs to be changed every 90 days and must be 8 to 16 characters beginning with a letter. The password is case sensitive and must also contain a number and a special character.

Note: User-defined password rules are case sensitive by default. If you desire to have case insensitive passwords, you can use the **Password Rule Details** task and change the setting for the **Case sensitive** field.

Steps to create a customized password rule:

1. From the **User Management** dashboard, select the **Password Rules** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Password Rule** wizard is started.
3. On the Welcome page of the **New Password Rule** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Password Rule Details section, enter *xyz-rules* in the Name field. Optionally, enter meaningful text in the Description field to describe your password rule, then click **Next.**
5. On the Password Rules page, select **Expiration (days)**. Enter 90 in the Expiration (days) field. Enter 8 in the Minimum length field. Enter 16 in the Maximum length field. Optionally, customize any other settings on the page, then click **Next**.
6. On the Character Rules page, select **Add** in the **Actions** drop-down list. The Edit Character Rule dialog opens.
7. On the Edit Character Rule dialog, leave the Minimum length 1 and Maximum length 1. In the drop-down list for Alphabetic characters select **Required**. This character rule ensures that the password must start with an alphabetic character. Click **OK**. Your character rule is now in the table.
8. Again, on the Character Rules page, select **Add** in the **Actions** drop-down list. The Edit Character Rule dialog opens.
9. On the Edit Character Rule dialog, change the Minimum length to 7 and Maximum length to 15. In the drop-down list for Alphabetic characters select **Allowed**. In the drop-down list for Numeric characters select **Required**. In the drop-down list for Special characters select **Required**. This character rule ensures that the password must have at least one numeric character and at least one special character. Click **OK**. Your second character rule is now in the table. Click **Next**.
10. Review the details on the Summary page. Click **Finish**. The password rule xyz-rules is created.

Steps to assign the password rule to each of your existing users:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. Select the first user you want to customize in the list and select the **Details** icon (). The **User Details** task is opened.
3. Click the Authentication section. Under the Local Authentication radio button, select *xyz-rules* in the Password rule drop-down list.
4. Select the **Force user to change the password at the next logon** check box. This ensures that the next time the user logs on with their current password, the user must create a new password following your security rules. Otherwise, the user is not required to change the password at their next logon even if the password does not conform to the new password rule.
5. Click **OK** on the **User Details** task. The user is updated with the new password rule.
6. On the dashboard, in the Summary for your user, the Authentication section reflects the xyz-rules password rule is in effect.
7. Repeat the above steps for each of your existing users.

Note: As the administrator, you are not required to change the password when you change to a new password rule. Thus, the user is responsible for creating the password that follows the new password rule the next time the password is changed.

Separate system resources between users

If you want to separate system resources between users, you create roles containing the different objects and then assign the appropriate roles to the users. For this example, we have two LPARs on system SYS_A. User Zoey is assigned LPAR image LP01 and user Paul is assigned LPAR image LP02.

Steps to create custom roles for the LPAR image objects:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Role Details section, enter *LP01* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, then click **Next**.
5. On the Tasks page, click **Next**.
6. On the Objects by Type page, click **Next**.
7. On the Specific Objects page, enter *lpar image* in the filter box. The table of objects is filtered to show only rows containing text *LPAR Image*. Thus, the view is now limited to all the LPAR images currently on the system. Since our role requires access to just a single LPAR, select the check box on the row with name *LP01* and system *SYS_A*, then click **Next**.
8. On the Groups page, click **Next.**
9. On the Objects by Group page, click **Next.**
10. Review the details on the Summary page, then click **Finish**. The role LP01 is created.
11. On the dashboard, role *LP01* is the current selected role. View the *Summary for LP01* to verify the Objects that role LP01 is granted permission. The Objects section should show object SYS_A:LP01.
12. Repeat the above steps to create the role named *LP02* for LPAR image LP02.

Steps to assign the custom roles to users:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the User Details section, enter *Zoey* in the Name field. Optionally, enter meaningful text in the Description field to describe your user, then click **Next.**
5. On the Authentication page, keep the default selection **HMC password authentication**. Leave the Password rule as the default *Standard*. Enter *zoeypw* as the password in the Password and Confirm password fields. Ensure **Force user to change the password at next logon** is selected, then click **Next**.
6. On the Roles page, enter *LP* in the filter. The table is filtered to show LP01 and LP02 roles. Select the check box on row *LP01*. Clear the filter box and scroll the table to locate *Operator Tasks*. Select the check box on row *Operator Tasks*. Note that the bottom of the table indicates you have *Selected: 2*. Click **Next.**

Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.

7. Review the details on the Summary page, then click **Finish.** The user Zoey is created.
8. Again, from the dashboard, select the **New** icon ( ). The **New User** wizard is started.
9. On the Welcome page of the **New User** wizard, click **Next**.
10. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on user and select *Zoey*. In the User Details section, enter *Paul* in the Name field. Optionally, enter meaningful text in the Description field to describe your user, then click **Next**.
11. On the Authentication page, enter *paulpw* as the password in the Password and Confirm password fields, then click **Next**.
12. On the Roles page, scroll the table to locate LP01. Note that it is preselected from user Zoey. Clear the check box for that role, and select the check box for role LP02. Note that the bottom of the table indicates you have *Selected: 2*. *Operator Tasks* is preselected from user Zoey. Click **Next**.
13. Review the details on the Summary page, then click **Finish**. The user Paul is created.
14. On the dashboard, user *Paul* is the current selected user. View the *Summary for Paul* to verify the Roles are *LP02* and *Operator Tasks*. Also verify Objects is limited to SYS_A:LP02.
15. On the dashboard, select user *Zoey* and repeat the previous step for user *Zoey* to verify she has access to LP01.

Zoey and Paul are now able to logon to the console with their respective user IDs and passwords. They are required to change the password on their first logon. Zoey has access to SYS_A:LP01 and can perform all operator tasks on that LPAR. Similarly, Paul has access to SYS_A:LP02 and can perform all operator tasks on that LPAR.

Assign view only variant of a task to a user (for example, the Hardware Messages task)

There are several view only variants of tasks that you might want to assign to your users (for example: Configure Channel Path On/Off, Hardware Messages, Operating System Messages, OSA Advanced Facilities, and Manage System Time). In this scenario, the **Hardware Messages (view only)** task is assigned to user Terry.

Steps to create a customized role for the **Hardware Messages (view only)** task:

1. From the **User Management** dashboard, select the **Roles** icon ( ) in the navigation area.
2. From the action icons, select the **New** icon ( ). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next.**
4. On the Name page, in the Create Option section, keep the default option **New**. In the Role Details section, enter *Hardware Messages view only* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, then click **Next**.
5. On the Tasks page, enter *view only* in the filter. The list of tasks is filtered to only show the view only tasks. Select the check box on the row for *Hardware Messages (view only)*, then click **Next**.
6. On the Objects by Type page, click **Next**.
7. On the Specific Objects page, click **Next**.
8. On the Groups page, click **Next**.
9. On the Objects by Group page, click **Next.**
10. Review the details on the Summary page, then click **Finish**. The role *Hardware Messages view only* is created.

Steps to add the customized role to user Terry:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. Select the user Terry in the list and select the **Details** icon (). The **User Details - Terry** task is opened.
3. Click the Roles page. Select **Add Roles** in the **Actions** drop-down list. The Add Roles dialog is opened.

   Note: You can click the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.
4. On the Add Roles dialog, enter *view only* in the filter. Select the check box in the *Hardware Messages view only* row, then click **OK**. The role is added to the list of roles for the user.
5. Click **OK** on the **User Details** task. The user Terry is updated with the additional role.
6. On the dashboard, in the *Summary for Terry*, the Roles section includes the new role and the Tasks section contains the **Hardware Messages (view only)** task.

Modify a user to grant remote access to the console

Modify a user to grant remote access to the console User properties can be modified by using the **User Details** task launched from the **User Management** dashboard. In this example, the user Terry is granted remote access to the console.

Steps to modify user Terry:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. Select the user *Terry* in the list and select the **Details** icon (). The **User Details - Terry** task is opened.
3. In the General section, select **Allow remote access to the console**.
4. Click **OK** on the **User Details** task. The user Terry is updated with the additional privilege.
5. Open the **Customize Console Services** task. Ensure **Enabled** is selected from the **Remote operation** drop-down list, then click **OK**.

User Terry can now logon the console remotely from a web browser.

Create a customized managed object role (similar to the approach available in HMC version 2.12.1)

For administrators who are familiar with the **Customize User Controls** task in HMC version 2.12.1, this scenario guides you through creating a customized managed object role (formerly managed resource role) using the **User Management** task. For this example, we copy the HMC system defined role *Defined System Managed Objects* (formerly *Defined zCPC Managed Objects*) to create a new role that has access to defined systems and undefined systems (whereas normally the access is limited to defined systems). When assigned to a user, the new role would grant permission to view systems currently managed by the HMC, and systems that could be managed by the HMC if added by the **Add Object Definition** task. Separate role permission is needed for the user to have permission to the **Add Object Definition** task.

Steps to create a custom role for the Defined System Managed Objects:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.

4. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on role and select *Defined System Managed Objects*. (Roles are listed in alphabetic order. You can type the start of the role name in the box to narrow down the number of roles and make it easier to find your desired role for selection.) In the Role Details section, enter *Defined and Undefined System Managed Objects* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, and then click **Next**.
5. Since we are creating a role specific for objects, on the Tasks page, click **Next**.

   Note: With the **User Management** task, a role can contain a mixture of objects (resources) and tasks, whereas the **Customize User Controls** task required separate roles. Therefore, if desired, you could grant permission to the **Add Object Definition** task at this point.
6. On the Objects by Type page, notice that there are object types preselected from *Defined System Managed Objects* role. Leave all the preselected object types. Additionally, select the row for *Undefined CPC*, and then click **Next**.
7. On the Specific Objects page, click **Next**.
8. On the Groups page, click **Next**.
9. On the Objects by Group page, click **Next**.
10. Review the details on the Summary page, then click **Finish**. The role *Defined and Undefined System Managed Objects* is created.
11. On the dashboard, role *Defined and Undefined System Managed Objects* is the current selected role. View the *Summary for Defined and Undefined System Managed Objects* to verify the Object Types that the role granted permission are correct.

Note: When creating a name longer than the designated name length in the objects list, a scroll bar is displayed at the bottom of the object list area for you to scroll to view the entire name.

The role *Defined and Undefined System Managed Objects* can now be assigned to desired users.

Create a customized task role (similar to the approach available with HMC version 2.12.1)

For administrators who are familiar with the **Customize User Controls** task in HMC version 2.12.1, this scenario guides you through creating a customized task role using the **User Management** task. For this example, we copy the HMC system defined role *Operator Tasks* to create a new role that adds permission to customize activation profiles. When assigned to a user, the new role would grant permission to operators to modify and delete activation profiles, whereas normally they are limited to viewing activation profiles.

Steps to create a custom role for the Operator Tasks:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on role and select *Operator Tasks*. (Roles are listed in alphabetic order. You can type the start of the role name in the box to narrow down the number of roles and make it easier to find your desired role for selection.) In the Role Details section, enter *Operator Tasks with Activation Profiles* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, then click **Next**.
5. On the Tasks page, notice that there are tasks preselected from *Operator Tasks* role. Use the scroll bars as needed to select the row for *Customize/Delete Activation Profiles*, clear the check box on the row for *View Activation Profiles*, and then click **Next**.
6. On the Objects by Type page, click **Next**.
7. On the Specific Objects page, click **Next**.

8. On the Groups page, click **Next**.
9. On the Objects by Group page, click **Next**.
10. Review the details on the Summary page, then click **Finish**. The role *Operator Tasks with Activation Profiles* is created.
11. On the dashboard, role *Operator Tasks with Activation Profiles* is the current selected role. View the *Summary for Operator Tasks with Activation Profiles* to verify the Tasks that the role granted permission are correct.

The role *Operator Tasks with Activation Profiles* can now be assigned to desired users.

Create an HMC user for OSA/SF

In order to utilize the Open System Adapter/Support Facility (OSA/SF) configuration windows on your Hardware Management Console, the HMC access administrator must create a user for the OSA/SF system administrator. This new user has the required permissions for the objects and tasks required on the HMC for the OSA/SF system administrator.

Steps for the HMC access administrator to create a custom role for your OSA/SF system administrator are as follows:

1. From the **User Management** dashboard, select the **Roles** icon in the navigation area.
2. From the actions icons, select the **New** icon. the **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, leave the selection **New**. In the Role Details section, enter *OSASF Tasks* in the Name filed. Optionally, enter meaningful text (that is, *OSA Support Facility tasks*) in the Description field to describe your role, and then click **Next**.
5. On the Tasks page, select the **OSA Advanced Facilities** task. You can type *facilities* in the filter to narrow down the list of tasks in the table, or you can scroll down to find the selection. When you have made the task selection, click **Next**.
6. On the Objects by Type page, select the rows for the following object types. When complete, click **Next**.
   a. *Defined CPC*
   b. *LPAR Image*
7. On the Specific Objects page, make no selections, then click **Next.**
8. On the Groups page, make no selections, then click **Next**.
9. On the Objects by Group page, make no selections, then click **Next**.
10. Review the details on the Summary page, then click **Finish**. The role *OSASF Tasks* is created. On the dashboard, the role *OSASF Tasks* is added to the list of roles and is the current selected role. View the *Summary for OSASF Tasks* to verify the Tasks and Object Types that the role granted permission are correct.

Steps to create the user for the OSA/SF system administrator are as follows:

1. From the **User Management** dashboard, select the **Users** icon in the navigation area.
2. From the actions icons, select the **New** icon. The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, leave the selection **New**. In the User Details section, enter *OSASF* in the Name field. Optionally, enter meaningful text (that is, *OSA Support Facility user*) in the Description field to describe your user, and then click **Next**.
5. On the Authentication page, keep the default selection **HMC password authentication**. Leave the Password rule as the default *Standard*. Enter the desired password in the Password and Confirm password fields, then click **Next**.

6. On the Roles page, select the check box for role *OSASF Tasks* to give the user access to the required objects and tasks. You can type *osa* in the filter to narrow down the list of roles in the table, or you can scroll down to find the selection. When you have made the task selection, click **Next**.
7. Review the details on the Summary page, then click **Finish**. The user *OSASF* is created.
8. On the dashboard, user *OSASF* is added to the **Users** list and is the current selected users. View the *Summary for OSASF* to see the Roles, Tasks, and Object Types that OSASF is granted permission

For more information on using the OSA/SF on the Hardware Management Console, see the *Open System Adapter/Support Facility on the Hardware Management Console*, SC14-7580.

Default Permissions

The system grants every user permission to certain tasks, groups, objects, and object types. These specific permissions cannot be set up or removed by the **User Management** task. Therefore, the access administrator is not required to manage these permissions.

The list of default permissions provided to every user is as follows:

- Tasks
  - Details tasks as follows:
    - Image Details
    - System Details

    Note: The Details tasks are the read only version and might limit the information displayed.
  - Change Password
  - Logoff or Disconnect
  - User Management (This is limited to the Users navigation and only for viewing or updating specific settings for the current user.)
- Groups
  - All system defined managed object groups (such as Systems Management). Note that a system defined managed object group does not display in the Navigation Pad unless the logged on user has permission to one or more objects contained in that managed object group.
  - All system defined task lists (such as Daily, etc.). Note that a task list does not display in the Tasks Pad unless the logged on user had permission to one or more tasks contained in that task list.
- Objects
  - Console object
- Object Types (on the Hardware Management Console only)
  - Fibre Channel Network
  - Hardware Management Console
  - HMC Optical Network

Users

This task is used by an access administrator or a user that is assigned a role with Manage Users task permission. A *user* is a combination of a user name (user ID), permissions, authentication mode, and a text description. Permissions represent the authority levels that are assigned to the user for the objects and tasks the user has permission to access.

The user ID and password are used to verify a user's authorization to log on to the console. The password is determined by the password rule that is chosen for the user. The default choices are *Basic*, *Strict*, and *Standard*, however, other rules may also be available if they were defined in the **Password Rules** task. All

these rules have their own set of specifications for assigning a password. Your access administrator determines what password rule is appropriate for you, whether you must change your password at the next logon, and whether you can log on to the console locally or remotely.

Use this task to choose the type of password authentication you want to assign to a user. If you choose the **HMC password authentication**, then the password authentication is performed by using the console. If you choose the **LDAP password authentication**, then the password authentication is delegated to an LDAP server. You use the **LDAP Server Definitions** task to define the LDAP server. You can also enable multi-factor authentication for a user that requires the user to log on to the console with additional requirements.

The user definition specifies roles that are assigned to the user. You can choose from a list of available default roles or create user-defined roles using the **New Role** task. A role defines permissions to tasks, types of objects or specific objects, groups, and task lists.

The system contains the following predefined default users:

- ACSADMIN
- ADVANCED
- OPERATOR
- SERVICE
- STORAGEADMIN
- SYSPROG

You cannot change the roles of the default users. You can create a new user based on the desired system default user and modify the roles for the new user.

Attention: In the state of California, US, the use of default passwords are no longer allowed. The first time a default user ID logs on to the console, the default password must be changed. A prompt is displayed requiring the password change.

This password default change is controlled by SERVICE or a user that is assigned a role with Manage Users task permission by selecting **Default Users** from the **Users** view and then clicking the **Details** icon. The Change default user passwords prompt is displayed. If you are using a user that is assigned a role with Manage Users task permission, then each default user's password is reset to its default value and all default users are required to change their passwords the next time they log in. If you are using SERVICE, then only that password is reset to the default and all default users are required to change their passwords the next time they log in.

The **Users** dashboard view displays a list of all currently defined users with user summary sections as follows:

General
This section contains the description, last logon, and disabled fields for the selected user.

Authentication
This section contains the authentication type and corresponding authentication settings.

Roles
This section lists all of the role permissions assigned to the selected user.

Groups
This section lists all of the user-defined custom groups (including pattern match groups) that the selected user has Group Management permission to modify. Groups that the user is granted only Child Management permission are not shown.

Tasks
This section lists all of the tasks the selected user is granted permission by the assigned roles. The list does not include tasks that the user has available by “Default Permissions” on page 1404.

Object Types
This section lists all of the types the selected user is granted permission by the assigned roles. The list does not include object types that the user has available by “Default Permissions” on page 1404.

Objects
This section lists all the objects the user is granted permission to access by the assigned roles. Permission has been granted in a role by either object type, specific object, or Child Management permission to a group. The list does not include objects that the user has available by "Default Permissions" on page 1404.

You can view the object summary using the **Expand** and **Collapse** icons to view or hide sections. You can create a new user definition using the **New User** wizard or manage an existing user definition with **User Details**.

- Click the **"New User" on page 1406** () icon to create a new user definition. When the **New User** wizard completes, the new user is added to the Users list.
- Click the **"User Details" on page 1409** () icon to manage an existing user definition. You cannot modify the roles specified in the system defined default users. You can also use this icon with **Default Users** to reset the passwords of the default user IDs.
- Click the **Delete** () icon to delete an existing user definition. You can delete system default users, but be sure you have created new customized users based on these system default users before deleting.

New User

Use the **New User** wizard to guide you through creating a new user. The **New User** wizard is organized into the following pages, each page of which is listed on the left navigation. The currently displayed page is highlighted. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

- Use the "Name" on page 1407 page to specify the user name, along with an optional description and email address. It also provides capability to create a new user or copy an existing user.
- Use the "Authentication" on page 1408 page to select an authentication type for the new user.
- Use the Roles page to select one or more roles to define access permissions for this new user. You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Roles Details**.
- Use the Summary page to view a summary report of the new user to be created. When you click **Finish**, the new user is created and populated with the values specified in the **New User** wizard.

The **New User** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new user. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New User** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new user, click **Finish**.

Cancel
To exit the wizard without creating the new user, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and optional description for the new user you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option

This option determines how the object is created.

New:

Create a new user.

New based on:

Select an existing user to base the new user on. The settings in the new user are initialized to those of the existing user. The system default users are as follows:

- ACSADMIN
- ADVANCED
- OPERATOR
- SERVICE
- STORAGEADMIN
- SYSPROG

Note: You cannot change the roles of the default users.

If you want the ability to change the roles for a default user, create your own version by copying an existing default user.

User Details

This section requires a name and an optional description.

Name:

Specify the user name for the user you are creating. When creating a new user, the user name can be 4 to 320 characters in length and a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- back slash (\)
- greater than (>)
- less than (<)
- asterisk (*)
- ampersand (&)
- question mark (?)
- apostrophe (')
- comma (,)
- colon (:)
- left and right parentheses ( )
- semicolon (;)
- number sign (#)
- percent sign (%)
- equals sign (=)
- plus sign (+)
- dash (-)
- underscore (_)
- at sign (@)
- slash (/)
- period (.)

The name must be unique among existing user names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text that describes your user. The description can be up to 1024 characters with no character restrictions.

Email Address:
Enter an optional, valid email address for this user.

Authentication

Use the Authentication page to select the password authentication you want to assign to the new user.

Password authentication and password rules

If you choose the **HMC password authentication**, then the password authentication is performed by using the console. If you choose the **LDAP password authentication**, then the password authentication is delegated to an LDAP server. After entering the information, click **Next** to proceed to the next page.

Choose the password authentication that you want by selecting one of the following:

- Select **HMC password authentication** to perform password authentication by using the console.

Password rule:
You must select a password rule to be used for the specified new user. Click the drop-down arrow for a list of rules, then select one. The system defined default password rules are as follows:

Basic
The basic password rules consist of:

- A password must be a minimum of four characters and a maximum of eight characters long.
- These characters include A-Z, a-z, 0-9.

Standard
The standard password rules consist of:

- Password expires in 186 days.
- A password must be a minimum of six characters and a maximum of 30 characters long.
- The first and last character in a password can be alphabetic or special.
- A password can contain letters, numbers, and special characters.
- No character can repeat more than twice.
- A password can only match three characters from the previous password.
- You can repeat a password after using four unique passwords.

Strict
The strict password rules consist of:

- Password expires in 180 days.
- A password must be a minimum of six characters and a maximum of eight characters long.
- A password must contain both letters and numbers.
- The first and last character in a password must be alphabetic.
- No character can repeat more than twice.

Password:
Specify the password for the new user. Follow the password rule specified in the Password rule field.

Confirm password
Specify the password again for verification.

Select **Force user to change the password at next logon** to specify whether the user should be forced to change the password the next time the log in to the console.

- Select **LDAP password authentication** to delegate password authentication to an LDAP server.

  Server
  You must specify an LDAP server to be used for the new user. Click the drop-down arrow for a list of LDAP servers, then select one. Use the "LDAP Server Definitions" on page 1442 dashboard view to create and manage LDAP server definitions.

  User ID
  Specify an optional LDAP user ID if it is different from the new user name.

Multi-factor authentication (MFA)

- Select **No MFA**, if this user is not required to use multi-factor authentication when logging on to the console.
- Select **HMC MFA** to require this user to use the console's TOTP authentication when logging on to the console.
- Select **IBM Z Multi-Factor Authentication** to require this user to use RSA SecurID authentication through an IBM Z MFA server when logging on to the console.

  MFA ID
  Provides the user's RACF ID of the user name that was entered on the previous step. This is a required field.

  Primary server
  Select a primary IBM Z MFA server. This is a required field.

  Backup server
  Select a backup IBM Z MFA server. Specifying a backup server is recommended for high availability.

  Policy name
  Provide the name of the MFA policy to use with the server. The policy specifies the authentication factors the user is required to provide. The only factor supported by the HMC is RSA SecurID. No other factors are permitted in the policy. This is a required field.

User Details

Use the **User Details** task to view and manage the properties of a selected user. Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each section view.

- Select the "General" on page 1410 navigation link or the **Expand** icon to display the General details tab section.
- Select the "Session" on page 1410 navigation link or the **Expand** icon to display the Session details tab section.
- Select the "Authentication" on page 1411 navigation link or the **Expand** icon to display the Authentication details tab section.
- Select the **Roles** navigation link or the **Expand** icon to display the Roles details tab section. Use the **Actions** menu to "Add Roles" on page 1413 or Remove Roles defining access permission for the user. You can click the links for the roles to open **Role Details** for that role. If desired, you can make modification to user-defined roles from **Role Details**.

You can also use **User Details** when you select **Default Users** to reset the default user ID default passwords.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**.

Apply
To save the current changes for the user without exiting the task, click **Apply**.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information that you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to view the name and modify the description and other settings for the user.

Name:
Specifies the name for the user you are modifying.

Description:
Specify an optional meaningful text that describes your user.

Email address:
Enter an optional, valid email address for this user.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This value cannot be modified.

Default group:
The "Default Group" on page 1413 specifies a group to which any objects created by the user will be added by default. Select a group or **No default group** from the drop-down list. Be sure that the user has Group Management permission to the group selected.

Disable user
Indicates that you want to disable the user from logging into the console. A user is not allowed to disable their own user.

Note: This option changes to **Disabled due to inactivity** when the amount of days specified in the **Disable for inactivity (days)** has been exceeded.

Disabled due to inactivity
Indicates that the user's inactivity has exceeded the amount of days specified in the **Disable for inactivity (days):** option. Select **Disabled due to inactivity** to remove the check and re-enable the user.

Allow remote access to the console
Enables access to monitor and/or control the system from a remote site to a local console through a web browser.

Note: The user is only able to access the system remotely if remote operation of the system is enabled within the **Customize Console Services** task.

Allow access to Web Services management interfaces
Enables access to the Web services Application Programming Interface (API).

Allow access to Web Services management interfaces (0-9999):
Specify the number of times the user can be logged into a web API session simultaneously without disconnecting.

Idle web services API session timeout (1-360 minutes):
Specify the number of minutes the user's API session can be idle. If the user does not interact with the session in the specific amount of time, the session will be disconnected.

Session

Use the Session details tab section to view or modify the interval, in minutes, the user's session can run before being prompted for identity verification.

Note: If you use the **Single Object Operations** task from the Hardware Management Console, the session timeout is disabled on the Support Element for the duration of the Single Object Operations session.

Session timeout (minutes):
Select this to specify the interval, in minutes, over which a user's session can run before being prompted for identity verification. If a value other than zero is specified, the user is prompted after the specified minutes have been reached to re-enter their password. If a password is not re-entered within the amount of time that was specified in the *Verify timeout minutes* field, then the session is disconnected. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Verify timeout (minutes):
Select this to specify the amount of time that is required for the user to re-enter their password when prompted, if a value was specified in the *Session timeout minutes* field. If the password is not re-entered within the specified time, the session will be disconnected. The default is 15 minutes. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Idle timeout (minutes):
Select this to specify the number of minutes the user's session can be idle. If the user does not interact with the session in the specified amount of time, the session will be disconnected. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Authentication

Use the Authentication details tab section to view or modify the method of authenticating the user.

Password authentication and password rules

- To perform password authentication by using the console, select **HMC password authentication**.

Password rule:
You must select a password rule to be used for the specified user. Click the drop-down arrow for a list of rules, then select one. The system defined default password rules are as follows:

Basic
The basic password rules consist of:

- A password must be a minimum of four characters and a maximum of eight characters long.
- These characters include A-Z, a-z, 0-9.

Standard
The standard password rules consist of:

- Password expires in 186 days.
- A password must be a minimum of six characters and a maximum of 30 characters long.
- The first and last character in a password can be alphabetic or special.
- A password can contain letters, numbers, and special characters.
- No character can repeat more than twice.
- A password can only match three characters from the previous password.
- You can repeat a password after using four unique passwords.

Strict
The strict password rules consist of:

- Password expires in 180 days.
- A password must be a minimum of six characters and a maximum of eight characters long.
- A password must contain both letters and numbers.
- The first and last character in a password must be alphabetic.
- No character can repeat more than twice.

Password:
Specify the password for the user. Follow the password rule specified in the Password rule field.

Confirm password
Specify the password again for verification.

- To delegate password authentication to an LDAP server, select **LDAP password authentication**.

  Server
  You must specify an LDAP server definition to be used for the user. Click the drop-down arrow for a list of LDAP servers, then select one.

  User ID
  Specify an optional LDAP user ID if it is different from the user name.
- To require the user to change their password the next time they log on to the console, click **Reset**.
- Select **Delay login after failed attempts** to enable the login delay for continual invalid login attempts.

  Number of failed attempts before disable delay
  Specify the number of failed attempts before the user is temporarily disabled from being able to log on.

  Delay (minutes)
  Specify the amount of time in minutes the user is temporarily disabled after reaching the number of failed attempts.
- Select **Disable for inactivity (days):** to specify that a user is disabled if they have not logged on within a specified number of days. Then, specify the number of days after which the inactive user becomes disabled.
- Select **Minimum time between password changes (minutes)** to specify the minimum amount of time in minutes that must elapse between changes for the user's password. Unselected indicates that a user's password can be changed immediately after it has been changed.

  Note: This field is not applicable to a user that has LDAP authentication.
- Select **Require password for disruptive actions** to enable a password requirement, for this user, on a task that causes disruptive actions. This option, by default, is selected.

  Note: This option is disabled for the default SERVICE user. Therefore, the SERVICE user is always required to specify its password before proceeding with a task that causes disruptive actions.
- Select **Require text input for disruptive actions** to enable a text input requirement before performing a disruptive action on an object.

Multi-factor authentication (MFA)

- Select **No MFA**, if this user is not required to use multi-factor authentication when logging on to the console.
- Select **HMC MFA** to require this user to use the console's TOTP authentication when logging on to the console.
- Select **IBM Z Multi-Factor Authentication** to require this user to use RSA SecurID authentication through an IBM Z MFA server when logging on to the console.

  MFA ID
  Provides the user's RACF ID of the user name that was entered on the previous step. This is a required field.

  Primary server
  Select a primary IBM Z MFA server. This is a required field.

  Backup server
  Select a backup IBM Z MFA server. Specifying a backup server is recommended for high availability.

Policy name
Provide the name of the MFA policy to use with the server. The policy specifies the authentication factors the user is required to provide. The only factor supported by the HMC is RSA SecurID. No other factors are permitted in the policy. This is a required field.

- To require this user receive a new shared secret key the next time the user logs on to the console, click **Reset**. This option is only available when you select **HMC MFA**.

Default Group

Use the Default group field to choose the default group for the user. A *default group* is a user-defined group to which objects created by the user will be added by default. Use the drop-down to choose either **No default group** or select the desired group.

Default group
Choose a group that objects created by the user are added by default. The administrator should ensure that the user has access permission to manage the default group. Select **No default group** if you do not want to have new objects created by the user added to a group.

The default group cannot be a pattern match group since new objects defined by the user might not match the specific pattern for the group. Thus, no pattern match groups are included in the list.

Tasks that result in objects being added to a default group are as follows:

- Add Object Definition
- Grouping

A custom group cannot be deleted if it is designated as the default group for at least one user or user template.

Add Roles

Use this action to select new role permissions to add to the user. You can use the Filter function string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.

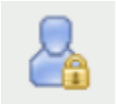
Additional functions on this window include:

OK
To perform the operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Roles



This task is used by an access administrator or a user that is assigned a role with Manage User Roles task permission. A ***role*** is a collection of authorizations that define permissions to tasks, type of objects or specific objects, groups, and task lists. A role can be created to define the set of tasks and managed objects allowed for a given class of user. Once you have defined or customized the role you can use the **Users** task to create new users with their own permissions.

Use this window to define and customize roles. A role assigns permission to a task or a managed object or group of objects, such as a managed system or logical partition. The **Roles** view can be changed by selecting the **Roles**, **Objects**, and **Tasks** links.

- **“View by Roles” on page 1414**

- **"View by Objects" on page 1414**
- **"View by Tasks" on page 1415**

You can view the object summary using the **Expand** or **Collapse** icons to view or hide sections.

The following actions are only available in the **View by Roles** dashboard view. You can create a new role definition using the **New Role** wizard or manage an existing user definition with **Role Details**.

- Click the **"New Role" on page 1415** () icon to create a new role definition. When the **New Role** wizard completes, the new role is added to the Roles list.
- Click the **"Role Details" on page 1417** () icon to view or modify an existing role definition. You cannot modify system defined roles.
- Click the **Delete** () icon to delete an existing role definition. You cannot delete system defined roles or roles that are associated with a user or user template.
- Click the **"New Task List" on page 1420** () icon to open the **Role Details** task and create a new task list for the selected role. The **New Task List** icon is only available for user-defined roles.

View by Roles

The **View by Roles** dashboard view displays a list of all currently defined roles with role summary sections as follows:

General
A statement describing the selected role.

Users
A list of users who have access to this role.

User Templates
A list of user templates that have access to this role.

Groups
A list of user-defined custom groups (including pattern match groups) granted Group Management permission by the role. Groups which are granted only Child Management permission are not shown.

Tasks
A list of tasks available in the role.

Object Types
A list of object types permitted by the role.

Objects
A list of all objects permitted by the role. It lists any objects the role would grant access by object type, specific object, or Child Management permission to a group.

Task Lists
A list of task lists permitted by the role.

View by Objects

The **View by Objects** dashboard view displays all currently defined and undefined objects on the system that can have permission assigned. The administrator can view roles that contain a particular object.

General
A statement describing the selected object.

Users
An alphabetized list of users who have access to this object.

Tasks
An alphabetized list of tasks that can target this object if the role permits.

Roles
An alphabetized list of roles that contain this object.

View by Tasks

The **View by Tasks** dashboard view displays a list of all system tasks that can have customized permissions. The administrator can view roles and users that have permission to a particular task.

General
A statement describing the selected task.

Users
A list of users who have access to this task.

Groups
A list of user-defined custom groups (including pattern match groups) that are allowable targets for the task. You can launch the task on the children of the custom group by selecting the group in the navigation area, selecting all targets in the table, and then launching the task.

Roles
A list of roles that permit this task.

Object Types
A list of types of objects that are allowable targets for the task.

Objects
A list of objects that are allowable targets for the task.

New Role

Use the **New Role** wizard to guide you through creating a new role. The **New Role** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

- Use the "Name" on page 1416 page to specify the role name and optional description. It also provides capability to create a new role or copy an existing role.
- Use the Tasks page to select the tasks to be included in the new role. The list of tasks contains all system tasks that can have customized permissions.
- Use the Objects by Type page to select the type of objects to include in the role. By adding an object type to the role, all objects of that type, regardless of whether they currently exist or are created in the future, are permitted to users or user templates with the role.
- Use the Specific Objects page to select specific objects to include in the new role. The list of objects contains all currently defined and undefined objects on the system that can have permission assigned.
- Use the Groups page to select groups to include in the new role. Adding a group gives permission to manage the group (Group Management), but does not give permission to objects in the group. The groups listed include all custom groups including pattern match groups. System defined groups such as Defined CPCs are not included.
- Use the Objects by Group page to select a group that contains the objects you want to include in the new role. Adding a group grants permission to objects in the group (Child Management), but does not grant permission to manage the group. You can use the links provided on the group name to view the objects ("Group Resources" on page 1416) currently in that group. The groups listed include all custom groups except pattern match groups.
- Use the Summary page to view a summary report of the new role to be created. When you click **Finish**, the new role is created and populated with the values specified in the **New Role** wizard.

The **New Role** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new role. Select **Show this**

welcome page next time to clear the box if you do not want to display the Welcome page next time you use the **New Role** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new role, click **Finish**.

Cancel
To exit the wizard without creating the new role, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new role you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new role

New based on:
Select an existing role to base the new role on. The settings in the new role are initialized to those of the existing role.

Role Details
This section specifies a name and an optional description.

Name:
Specify the name for the new role you are creating. When creating a new role, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing role names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text describing your role. The description can be up to 1024 characters with no character restrictions.

Associated system defined role:
Defines the role to be used for the **Single Object Operations** (SOO) task. Also, used to enable/disable certain features of the tasks (such as the **Users and Tasks** task).

Group Resources

Displays an informational table listing the objects currently contained in the group.

Additional functions on this window include:

Close
To exit the current window, click **Close**.

Help
To display help for the current window, click **Help**.

Role Details

Use the **Role Details** task to view the role properties of a selected role. Optionally, you can modify properties of a user-defined role. Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each view. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

- Select the "General" on page 1417 navigation link or the **Expand** icon to display the General section.
- Select the **Types** navigation link (or the **Expand** icon) to display the Types section. View or modify the role types by using the actions "Add Types to Role" on page 1418 or **Remove Types from Role**.
- Select the **Objects** navigation link (or the **Expand** icon) to display the Objects section. View or modify the role objects by using the actions "Add Objects to Role" on page 1418 or **Remove Objects from Role**.
- Select the **Tasks** navigation link (or the **Expand** icon) to display the Tasks section. View or modify the role tasks by using the actions "Add Tasks to Role" on page 1418 or **Remove Tasks from Role**.
- Select the **Groups** navigation link (or the **Expand** icon) to display the Groups section. View or modify the role groups by using the actions "Add Groups to Role" on page 1419 , **Remove Groups from Role**, or "Edit Group Permissions" on page 1419.
- Select the **"Task Lists" on page 1419** navigation link (or the **Expand** icon) to display the Task Lists section. View or modify the task list using actions New Task List, Task List Details, Delete Task List, Add Tasks to Task List, and Remove Tasks from Task List.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**. This function is available only for user-defined roles.

Apply
To save the current changes for the role without exiting the task, click **Apply**. This function is available only for user-defined roles.

Close
To exit the window, click **Close**. This function is available only for system defined roles since they cannot be modified.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved. This function is available only for user-defined roles.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to modify the description for the selected role.

Name:
Specifies the name of the role you are modifying.

Description:
Specify an optional meaningful text for your role.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This field cannot be modified.

Associated system defined role:
Defines the role to be used for the **Single Object Operations** (SOO) task. Also used to enable/disable certain features of the tasks (such as the **Users and Tasks** task).

"Include All Hosted Objects" on page 1418
Select this to include all hosted objects in a selected custom role.

Include All Hosted Objects

Use this check box to specify whether role inheritance is enabled.

A check mark indicates:
If the roles permits access to a parent managed object, then all managed objects that are hosted by the parent managed objects are permitted by the role.

An empty check box indicates:
Role inheritance is not enabled.

Add Types to Role

Use this action to add additional object types to the role. The list of object types includes all object types that are not already included in the role. By adding an object type to the role, all objects of that type, regardless of whether they currently exist or are created in the future, are permitted to users or user templates with the role. If all object types are already contained in the role, the message "No items to display" is shown. You can select all types by selecting the top check box.

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Additional functions on this window include:

OK
To perform the operation and save the changes to the role, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Objects to Role

Use this action to add additional objects to the role. The list of objects includes all managed objects that are not already included in the role. If all objects are already contained in the role, the message "No items to display" is shown. You can select all objects by selecting the top check box.

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Additional functions on this window include:

OK
To perform the operation and save the changes to the role, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Tasks to Role

Use this action to add tasks to the role. The list of tasks includes all tasks (that can have permission assigned) that are not already included in the role. If all tasks are already contained in the role, the message "No items to display" is shown. You can select all tasks by selecting the top check box.

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Additional functions on this window include:

OK
To perform the operation and save the changes to the role, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Groups to Role

Use this action to add additional user-defined groups to the role. The list of groups includes all user-defined groups that are not already included in the role. If all groups are already contained in the role, the message "No items to display" is shown. You can select all groups by selecting the top check box. Select the permission type you want to add to the group:

Group management
Grants permission to manage the group, but does not grant permission to objects in the group.

Child management
Grants permission to manage objects in the group, but does not grant permission to the group.

Group and child management
Grants permission to manage the group and permission to the objects in the group.

Note: You cannot assign **Child management** or **Group and child management** to a pattern match group.

Additional functions on this window include:

OK
To perform the operation and save the changes to the role, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Group Permissions

Use this action to edit the group permissions for the selected group. The permission type to select:

Group management
Grants permission to manage the group, but does not grant permission to objects in the group.

Child management
Grants permission to manage objects in the group, but does not grant permission to the group.

Group and child management
Grants permission to manage the group and permission to the objects in the group.

Note: You cannot assign **Child management** or **Group and child management** to a pattern match group.

Additional functions on this window include:

OK
To perform the operation and update the group selection permission, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Task Lists

A *task list* is a grouping of tasks for a defined purpose such as Daily tasks or Configuration tasks. You can create your own custom task lists for your specific purpose. New task lists are displayed in the user interface under the Tasks Pad for users that have permission to the role that defines the task list.

You can also modify system defined task lists to add tasks to the list. For example, you can add the **Integrated 3270 Console** to the Daily task list by creating a new task list with the name Daily and adding the task to the list. The task is added to the Daily list alphabetically. You cannot remove tasks from a system defined task list.

Only groupable tasks can be added to a task list. Console actions tasks or root tasks (such as System Details) cannot be added to a task list.

Use the Task List section to create new task lists or manage existing task lists assigned to the role by using the following actions:

- "New Task List" on page 1420
- "Task List Details" on page 1421
- Delete Task List
- "Add Tasks to Task List" on page 1422
- Remove Tasks from Task List

New Task List

Use this action to create a new task list for the selected role. The table contains the list of groupable tasks contained in the role. You can select all tasks by selecting the top check box. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Name
Specify the name for the new task list you are creating. When creating a new task list, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing task list names. The comparison for duplicate name is case insensitive.

Description
Specify an optional meaningful text for your task list. The description can be up to 1024 characters with no character restrictions.

You can work with the table by using the table icons or **Action** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar:

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Selects the columns that you want to display. All available columns are in the list by their column name. Select the columns that you want displayed or hidden by selecting or clearing the items in the list. When you complete the configuration, click **OK**. The columns are displayed in the table as you specified.

Additional functions on this window include:

OK
To perform the operation and create a new Task List, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Task List Details

Use this action to modify the selected task list.

You can work with the table by using the table icons or **Actions** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar:

Add Tasks to Task List
Adds one or more tasks to the task list.

Remove Task from Task List
After confirmation, removes the select task from the task list. This action is only available if you have selected a task row in the table.

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Selects the columns that you want to display. All available columns are in the list by their column name. Select the columns that you want displayed or hidden by selecting or clearing the items in the list. When you complete the configuration, click **OK**. The columns are displayed in the table as you specified.

Additional functions on this window include:

OK
To perform the operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Tasks to Task List

Use this action to add one or more tasks to the selected task list. The table contains the list of groupable tasks contained in the role that are not already included in the task list. If the task list already contains all groupable tasks in the role, then the message "No items to display" is shown. You can select all tasks by selecting the top check box.

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

You can work with the table by using the table icons or **Actions** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. the following functions are available from the table toolbar:

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Selects the columns that you want to display. All available columns are in the list by their column name. Select the columns that you want displayed or hidden by selecting or clearing the items in the list. When you complete the configuration, click **OK**. The columns are displayed in the table as you specified.

Additional functions on this window include:

OK
To perform the operation and update the Task Lists table, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

User Patterns

This task is used by an access administrator or a user that is assigned a role with Manage User Patterns task permission.

Use the **User Patterns** tasks to define a group of console users at once whose user IDs all match a certain pattern. These user IDs are validated against entries in your LDAP server. When a user logs on, if the user ID is not defined locally, it is matched against all the patterns defined. The order of the pattern definitions in the list controls the order in which they are tried. When a match is found, a temporary user definition is created from the user template named in the pattern definition. The user definition exists only so long as

the user is logged on, though any settings they customize will be retained for the amount of time given in the pattern definition. If the user logs on again within that period, they do not need to customize the same settings they did previously.

If preferred, you can name an LDAP attribute whose value is the name of the user template that should be used for that user instead of the one named in the pattern definition. This capability gives certain users different privileges than the default for that pattern. Additionally, you can name an LDAP attribute whose value is the name of the console domain that is allowed to log on using that LDAP entry. LDAP attributes can have multiple values in an LDAP entry, and if this attribute name is specified in the pattern definition, one of the attribute values must match the console's domain name.

The **User Patterns** dashboard view displays a list of all currently defined user patterns with user pattern summary sections as follows:

General
This section contains the name and description for the selected user pattern.

Pattern
This section contains the user pattern, the pattern type, and the user settings retention time for the selected user pattern.

Template
This section contains the user template definition, additional LDAP settings, server definition, template name override attribute, and domain name restrictions attribute.

You can view the object summary using the **Expand** or **Collapse** icons to view or hide sections. You can create a new user pattern using the **New User Pattern** wizard or manage an existing user pattern definition with **User Pattern Details**.

- Click the **"New User Pattern" on page 1423** () icon to create a new user pattern. When the **New User Pattern** wizard completes, the new user pattern is added to the User Patterns list.
- Click the **"User Pattern Details" on page 1427** () icon to view or modify an existing user pattern.
- Click the **Delete** () icon to delete an existing user pattern. You can delete a pattern that currently has users authenticated using the pattern definition. Use the **Users and Tasks** task to see the list of users currently logged on. You can then forcibly logoff any users that are using the pattern being deleted.
- Click the **Move Up** arrow to move a specific defined user pattern up in the list of defined patterns. You can use this to change the order in which the user patterns are searched.
- Click the **Move Down** arrow to move a specific defined user pattern down in the list of defined patterns. You can use this to change the order in which the user patterns are searched.

New User Pattern

Use the **New User Pattern** wizard to guide you through creating a new user pattern. The **New User Pattern** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted.

- Use the "Name" on page 1424 page to specify the user pattern name and optional description. It also provides capability to create a new pattern or copy an existing pattern.
- Use the "User Pattern" on page 1424 page to define the string pattern to match user IDs.
- Use the "Template" on page 1426 page to select the user template to use with this user pattern.
- Use the Summary page to view a summary report of the new user pattern to be created. When you click **Finish**, the new user pattern is created and populated with the values specified in the **New User Pattern** wizard.

The new **User Pattern** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new user pattern. Select

Show this welcome page next time to clear the box if you do not want to display the Welcome page next time you use the **New User Pattern** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new user pattern, click **Finish**.

Cancel
To exit the wizard without creating the new user pattern, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new user pattern you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new user pattern

New based on:
Select an existing pattern to base the new user pattern on. The settings in the new user pattern are initialized to those of the existing user pattern.

Pattern Details
This section requires a name and an optional description.

Name:
Specify the name for the new user pattern you are creating or managing. When creating a new user pattern, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing user pattern names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text for your user pattern. The description can be up to 1024 characters with no character restrictions.

User Pattern

Use the User Pattern page to define the pattern string to use in matching user IDs. Select from glob-like pattern or regular expression. After entering the information, click **Next** to proceed to the next page.

Glob-like
Indicates a particular pattern. An asterisk in the pattern matches zero or more characters in the user ID, and a question mark in the pattern matches any single character in the user ID.

Regular expression

Indicate a specific means for matching strings of patterns; such as, particular characters, words, or patterns of characters.

The following table lists some of the common metacharacter symbols used in a regular expression and gives some examples of how to use them. For a complete description of regular expression rules, you can search the intranet.

Table 20. Common metacharacter symbols

Metacharacter	Match	Regular Expression Example	Example explanation
[]	Any characters inside brackets	*[ab]cd*	Specifies *acd* and *bcd* are valid user IDs.
.	Any single character	*2.29431*	Specifies that any user ID that matching the string has any single character in the between the 2's is valid (for example, *2i29431*).
*****	Match the preceding token zero or more times.	**a.***	Specifies all user IDs of any length starting with 'a' are valid
+	Match the preceding token one or more times.	**a+**	Specifies all user IDs of length one or more, containing all a's, are valid.
.+	One or more occurrences of any character.	**a.+**	Specifies all user IDs of length 2 or more, starting with 'a' are valid.
[^c1-c2]	Any but characters except those in brackets.	*sysprog[^0-9]*	Specifies that the last character of the user ID name cannot have any numbers between 0 and 9 (for example, *0123456789*). The example would allow *sysprogx* but not *sysprog1*.
[c1-c2]	Any range of characters in brackets	*sysprog[A-Z]*	Specifies that the last character of the user ID name must be a capital letter. The example would allow *sysprogA*, *sysprogB*, etc, but not *sysprogx* or *sysprog1*.
?	Makes the preceding token in the regular expression optional	*sysprog1?*	Specifies the '1' is optional at the end of the user ID. The example would allow *sysprog* and *sysprog1*.
|	Matches one expression or the other	*(userone|usertwo)@sampleco.com*	The example would allow *userone@sampleco.com*, *usertwo@sampleco.com*..

Table 20. Common metacharacter symbols (continued)

Metacharacter	Match	Regular Expression Example	Example explanation
\c	Turns off the meaning of any special char '**c**'. The backslash will escape the following special characters allowed in the LDAP user ID **\.?*+()**	*sysprog\+*	Specifies that the last character is a plus sign, not that the user ID can end in one or more backslash's. The example would allow user name *sysprog+*.

User pattern:
Specify the user pattern for the selected pattern type that is matched against the user ID that is entered when the user attempt to log on. This value is required to continue.

Retain user settings
Indicates to retain the settings of users authenticated using this pattern. The values specified in the Retention time (days):

- One or more indicates the number of days to retain.
- Unselected indicates not to retain the settings.
- Default retention time is 90 days.

Template

Use the Template page to define which template is used when a user matches this pattern. Select the user template that specifies the settings for users matching the pattern. After entering the information, click **Next** to proceed to the next page.

User Template
From the table, select the user template that specifies the settings for users matching the pattern. Use the "User Templates" on page 1429 dashboard view to create and manage user templates.

Optionally, you can select **Enable additional LDAP-based lookup and validation settings**:

Server
The selected server will be used to authenticate user IDs matching the user pattern. Select the name of the LDAP server definition, click the drop-down arrow, that is used to validate the user ID when processing a logon for users that match the pattern.

Note: The field is not available when the setting for **Enable additional LDAP-based lookup and validation settings** is unselected.

Template name override attribute
Specify the name of the LDAP attribute whose value, if defined, will override the selected template. The value of the attribute specifies the name of the template to be used to grant user permissions.

Note: The field is not available when the setting for **Enable additional LDAP-based lookup and validation settings** is unselected.

Domain name restriction attribute
Specify the name of the LDAP attribute that contains the information about what console the user is allowed to log on.

Note: The field is not available when the setting for **Enable additional LDAP-based lookup and validation settings** is unselected.

User Pattern Details

Use the **User Pattern Details** task to view and manage the properties of a selected user pattern. Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each view.

- Select the "General" on page 1427 navigation link or the **Expand** icon to display the General details tab section.
- Select the "Pattern" on page 1427 navigation link or the **Expand** icon to display the Pattern details tab section.
- Select the "Template" on page 1429 navigation link or the **Expand** icon to display the Template details tab section.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**.

Apply
To save the current changes for the user pattern without exiting the task, click **Apply**.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to view or modify a user pattern name and description for the selected user pattern.

Name:
Specifies the name for the user pattern you are modifying. When you are modifying the user pattern name, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

Description:
Specify an optional meaningful text for your user pattern.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This value cannot be modified.

Pattern

Use the Pattern details tab section to view or modify a particular pattern.

Glob-like
Indicates a particular pattern. An asterisk in the pattern matches zero or more characters in the user ID, and a question mark in the pattern matches any single character in the user ID.

Regular expression

Indicate a specific means for matching strings of patterns; such as, particular characters, words, or patterns of characters.

The following table lists some of the common metacharacter symbols used in a regular expression and gives some examples of how to use them. For a complete description of regular expression rules, you can search the intranet.

Table 21. Common metacharacter symbols

Metacharacter	Match	Regular Expression Example	Example explanation
[]	Any characters inside brackets	*[ab]cd*	Specifies *acd* and *bcd* are valid user IDs.
.	Any single character	*2.29431*	Specifies that any user ID that matching the string has any single character in the between the 2's is valid (for example, *2i29431*).
*****	Match the preceding token zero or more times.	**a.***	Specifies all user IDs of any length starting with 'a' are valid
+	Match the preceding token one or more times.	**a+**	Specifies all user IDs of length one or more, containing all a's, are valid.
.+	One or more occurrences of any character.	**a.+**	Specifies all user IDs of length 2 or more, starting with 'a' are valid.
[^c1-c2]	Any but characters except those in brackets.	*sysprog[^0-9]*	Specifies that the last character of the user ID name cannot have any numbers between 0 and 9 (for example, *0123456789*). The example would allow *sysprogx* but not *sysprog1*.
[c1-c2]	Any range of characters in brackets	*sysprog[A-Z]*	Specifies that the last character of the user ID name must be a capital letter. The example would allow *sysprogA*, *sysprogB*, etc, but not *sysprogx* or *sysprog1*.
?	Makes the preceding token in the regular expression optional	*sysprog1?*	Specifies the '1' is optional at the end of the user ID. The example would allow *sysprog* and *sysprog1*.
|	Matches one expression or the other	*(userone|usertwo)@sampleco.com*	The example would allow *userone@sampleco.com*, *usertwo@sampleco.com*.

Table 21. Common metacharacter symbols (continued)			
Metacharacter	**Match**	**Regular Expression Example**	**Example explanation**
\c	Turns off the meaning of any special char '**c**'. The backslash will escape the following special characters allowed in the LDAP user ID **\.? *+()**	*sysprog\+*	Specifies that the last character is a plus sign, not that the user ID can end in one or more backslash's. The example would allow user name *sysprog+*.

User pattern:
Specify the user pattern for the selected pattern type that is matched against the user ID that is entered when the user attempt to log on.

Retain user settings
Indicates to retain the settings of users authenticated using this pattern. The values specified in the Retention time (days):

- One or more indicates the number of days to retain.
- Unselected indicates not to retain the settings.

Template

Use the Template details tab section to view or modify which template is used when a user matched this pattern. Select the user template that specifies the settings for users matching the pattern. Optionally, you can select **Enable additional LDAP-based lookup and validation settings**.

Server
The selected server will be used to authenticate user IDs matching the user pattern. Select the name of the LDAP server definition, click the drop-down arrow, that is used to validate the user ID when processing a logon for users that match the pattern.

Note: The field is not available when the setting for **Enable additional LDAP-based lookup and validation settings** is unselected.

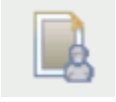
Template name override attribute
Specify the name of the LDAP attribute whose value, if defined, will override the selected template. The value of the attribute specifies the name of the template to be used to grant user permissions.

Note: The field is not available when the setting for **Enable additional LDAP-based lookup and validation settings** is unselected.

Domain name restriction attribute
Specify the name of the LDAP attribute that contains the information about what console the user is allowed to log on.

Note: The field is not available when the setting for **Enable additional LDAP-based lookup and validation settings** is unselected.

User Templates



This task is used by an access administrator or a user that is assigned a role with Manage User Templates task permission.

Use the **User Templates** task to create a *user template* that defines the settings and permission for users authenticated with a user pattern. The user IDs are validated against entries in the LDAP server specified by the template. When a user logs on, if the user ID is not defined locally, it is matched against all the patterns defined. The order of the pattern definitions in the list controls the order in which they are tried. When a match is found, a temporary user definition is created from the user template named in the pattern definition. The user definition exists only so long as the user is logged on, though any settings they customize will be retained for the amount of time given in the pattern definition. If the user logs on again within that period, they do not need to customize the same settings they did previously.

The **User Templates** dashboard view displays a list of all currently defined user templates with template summary sections as follows:

General
This section contains the description and LDAP server for the selected user template.

Roles
This section lists all of the role permissions assigned to the selected user template.

Groups
This section lists all of the user-defined custom groups (including pattern match groups) that the selected user template has Group Management permission to modify. Groups that the user template is granted only Child Management permission are not shown.

Tasks
This section lists all of the tasks the selected user template is granted permission by the assigned roles. The list does not include tasks that the user template has available by "Default Permissions" on page 1404.

Object Types
This section lists all object types the selected user template is granted permission by the assigned roles. The list does not include object types that the user template has available by "Default Permissions" on page 1404.

Objects
This section lists all the objects the selected user template is granted permission to access by the assigned roles. Permission has been granted in a role by either object type, specific object, or Child Management permission to a group. This does not include objects that the user template has available by "Default Permissions" on page 1404.

You can view the object summary using the **Expand** and **Collapse** icons to view or hide sections. You can create a new user template using the **New User Template** wizard or manage an existing user template definition with the **User Template Details** task.

- Click the **"New User Template" on page 1430** () icon to create a user template definition. When the **New User Template** wizard completes, the new user template is added to the User Templates list.
- Click the **"User Template Details" on page 1433** () icon to view or modify an existing user template.
- Click the **Delete** () icon to delete an existing user template. You cannot delete a user template that is utilized by a user pattern.

New User Template

Use the **New User Template** wizard to guide you through creating a new user template. The **New User Template** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted. Use the Filter function to enter a filter string in the Filter input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

- Use the "Name" on page 1431 page to specify the user template name and optional description. It also provides capability to create a new template or copy an existing template.

- Use the “Authentication” on page 1432 page to select from a list of LDAP servers to use with this user template.
- Use the “Roles” on page 1432 page to select one or more roles to define access permissions for the new user template. You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modification to user-defined roles from **Role Details**.
- Use the Summary page to view a summary report of the new user template to be created. When you click **Finish**, the new user template is created and populated with the values specified in the **New User Template** wizard.

The **New User Template** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new user template. This dashboard provides a summary of the steps that you will complete to create your new task permissions. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New User Template** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new user template, click **Finish**.

Cancel
To exit the wizard without creating the new user template, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new user template you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created

New
Create a new user template

New based on:
Select an existing template to base the new user template on

User Details
This option requires a name and an optional description.

Name
Specify the user name for the user profile you are creating. When creating a new user template , the user ID can be 4 to 320 characters in length and a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- back slash (\)
- greater than (>)
- less than (<)
- asterisk (*)
- ampersand (&)
- question mark (?)
- apostrophe (')
- quotation mark (")

- comma (,)
- colon (:)
- left and right parentheses ( )
- semicolon (;)
- number sign (#)
- percent sign (%)
- equals sign (=)
- plus sign (+)
- dash (-)
- underscore (_)
- at sign (@)
- slash (/)
- period (.)

Description
Specify an optional meaningful message for your records.

Authentication

Use the Authentication page to select the LDAP server and the MFA type to use with this new user template. Use the Filter function to enter a filter string in the input field or click the **Advanced Filter** icon to define a filter for any columns that limits the entries in a table.

- **Multi-factor authentication (MFA)**:
  - Select **No MFA**, if users defined by this template are not required to use multi-factor authentication when logging on to the console.
  - Select **HMC MFA** to require users defined by this template to use the console's TOTP authentication when logging on to the console.
  - Select **IBM Z Multi-Factor Authentication** to require users defined by this template to use RSA SecurID authentication through an IBM Z MFA server when logging on to the console.

    MFA override attribute name
    Specifies the name of the LDAP attribute that contains the MFA ID, such as a RACF user ID, that identifies the user to the MFA server that authenticates the user. If this value is not entered, the LDAP entry does not contain the specified attribute, or the attribute value is empty, then the user's IBM Z MFA ID defaults to the HMC user name.

    Primary server
    Select a primary IBM Z MFA server. This is a required field.

    Backup server
    Select a backup IBM Z MFA server. Specifying a backup server is recommended for high availability.

    Policy name
    Provide the name of the MFA policy to use with the server. The policy specifies the authentication factors the user is required to provide. The only factor supported by the HMC is RSA SecurID. No other factors are permitted in the policy. This is a required field.

Roles

Use the Roles page to select new role permissions for the new user template. Use the Filter function to enter a filter string in the input field or click the **Advanced Filter** icon to define a filter for any columns that limits the entries in a table.

You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**. Additional functions on this window include:

OK
To perform the operation and save the changes to user template, click **OK**.

Apply
To save the current changes without exiting the task, click **Apply**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

User Template Details

Use the **User Template Details** task to view and manage the properties of a selected user template. Use the navigation links on the left display each tab or use the **Expand All** and **Collapse All** icons to display each view.

- Select the "General" on page 1433 navigation link or the **Expand** icon to display the General details tab section.
- Select the "Session" on page 1434 navigation link or the **Expand** icon to display the Session details tab section.
- Select the "Authentication" on page 1434 navigation link or the **Expand** icon to display the Authentication details tab section.
- Select the **Roles** navigation link or the **Expand** icon to display the Roles details tab section. Use the **Actions** drop-down to "Add Roles" on page 1436 or Remove Roles defining access permission for the user template. You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**.

Apply
To save the current changes for the user template without exiting the task, click **Apply**.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General tab view to

Name
Specify the user name for the user template you are modifying. When modifying user template, the user ID can be 4 to 320 characters in length and a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- back slash (\)
- greater than (>)
- less than (<)
- asterisk (*)
- ampersand (&)
- question mark (?)
- apostrophe (')
- quotation mark (")
- comma (,)

- colon (:)
- left and right parentheses ( )
- semicolon (;)
- number sign (#)
- percent sign (%)
- equals sign (=)
- plus sign (+)
- dash (-)
- underscore (_)
- at sign (@)
- slash (/)
- period (.)

Description
Specify an optional meaningful message for your records.

Session

Use the Session details tab section to view or modify the interval, in minutes, that the user session can run before being prompted for identity verification.

Note: If you use the **Single Object Operations** task from the Hardware Management Console, the session timeout is disabled on the Support Element for the duration of the Single Object Operations session.

Session timeout (minutes):
Select this to specify the interval, in minutes, over which a user's session can run before being prompted for identity verification. If a value other than zero is specified, the user is prompted after the specified minutes have been reached to re-enter their password. If a password is not re-entered within the amount of time that was specified in the *Verify timeout minutes* field, then the session is disconnected. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Verify timeout (minutes):
Select this to specify the amount of time that is required for the user to re-enter their password when prompted, if a value was specified in the *Session timeout minutes* field. If the password is not re-entered within the specified time, the session will be disconnected. The default is 15 minutes. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Idle timeout (minutes):
Select this to specify the number of minutes the user's session can be idle. If the user does not interact with the session in the specified amount of time, the session will be disconnected. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Authentication

Use the Authentication details tab section to view or modify the LDAP server selected to be used for authentication.

- Use **Enterprise Directory Server (LDAP)** to modify the LDAP server selected for the user template. Click the drop-down for the list of servers, then select one.
- Select **Delay login after failed attempts** to enable the logon delay for continual invalid login attempts.

  Number of failed attempts before disable delay
  Specify the number of failed attempts before the user is temporarily disabled from being able to log on.

Delay (minutes)
Specify the amount of time in minutes the user is temporarily disabled after reaching the number of failed attempts.

- Select **Disable for inactivity (days):** to specify that a user is disabled if they have not logged on within a specified number of days. Then, specify the number of days after which the inactive user becomes disabled.
- Select **Require password for disruptive actions** to enable a password requirement, for this user template, on a task that causes disruptive actions. This option, by default, is selected.
- Select **Require text input for disruptive actions** to enable a text input requirement before performing a disruptive action on an object.
- **Multi-factor authentication (MFA)**:
  - Select **No MFA**, if users defined by this template are not required to use multi-factor authentication when logging on to the console.
  - Select **HMC MFA** to require users defined by this template to use the console's TOTP authentication when logging on to the console.
  - Select **IBM Z Multi-Factor Authentication** to require users defined by this template to use RSA SecurID authentication through an IBM Z MFA server when logging on to the console.

    MFA override attribute name
    Specifies the name of the LDAP attribute that contains the MFA ID, such as a RACF user ID, that identifies the user to the MFA server that authenticates the user. If this value is not entered, the LDAP entry does not contain the specified attribute, or the attribute value is empty, then the user's IBM Z MFA ID defaults to the HMC user name.

    Primary server
    Select a primary IBM Z MFA server. This is a required field.

    Backup server
    Select a backup IBM Z MFA server. Specifying a backup server is recommended for high availability.

    Policy name
    Provide the name of the MFA policy to use with the server. The policy specifies the authentication factors the user is required to provide. The only factor supported by the HMC is RSA SecurID. No other factors are permitted in the policy. This is a required field.
  - To require this template receive a new shared secret key the next time the user logs on to the console, click **Reset**. This option is only available when you select **HMC MFA**.

Default Group

Use the Default group field to choose the default group for the user. A *default group* is a user-defined group to which objects created by the user will be added by default. Use the drop-down to choose either **No default group** or select the desired group.

Default group
Choose a group that objects created by the user are added by default. The administrator should ensure that the user has access permission to manage the default group. Select **No default group** if you do not want to have new objects created by the user added to a group.

The default group cannot be a pattern match group since new objects defined by the user might not match the specific pattern for the group. Thus, no pattern match groups are included in the list.

Tasks that result in objects being added to a default group are as follows:

- Add Object Definition
- Grouping

Add Roles

Use this action to select new role permissions for the user template. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.

Additional functions on this window include:

OK
To perform the operation and save the changes to user template, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Password Rules

This task is used by an access administrator or a user that is assigned a role with Manage Password Rules task permission. Use this task to create, customize, or verify the password rules assigned to the system users.

Password rules assign individual rules for the system user when they are creating a password. In addition, you can optionally set more specific rules for individual parts of the password by specifying one or more character rules. There are three default password rules that you can choose from if you do not want to create your own. They are Basic, Strict, and Standard.

The **Password Rules** dashboard view displays a list of all currently defined password rules and password rule summary sections as follows:

General
This section contains the description for the selected password rule.

Password Rules
This section contains the expiration, minimum and maximum character length of password, consecutive number of characters allowed to be repeated in a row, similarity count, history count, and case sensitive settings for the selected password rule.

Character Rules
This section contains a table of the character rules for the selected password rule. The table specifies the minimum length, maximum length, alphabetic, numeric, special, and user-defined custom character specifications for the character rule parts.

You can view the object summary using the **Expand** and **Collapse** icons to view or hide sections. You can create a new password rule using the **New Password Rule** wizard or manage an existing password rule definition with **Password Rules Details**.

- Click the **"New Password Rule" on page 1437**() icon to create a new password rule. When the **New Password Rule** wizard completes, the password rule is added to the Password Rules list.
- Click the **"Password Rule Details" on page 1439**() icon to view or modify an existing password rule. You cannot modify the system defined password rules: Basic, Standard, and Strict.
- Click the **Delete** () icon to delete an existing password rule. You cannot delete a password rule that is utilized by at least one user.

New Password Rule

Use the **New Password Rule** wizard to guide you through creating a new case sensitive password rule. The **New Password Rule** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted.

- Use the "Name" on page 1437 page to specify the password rule name and optional description. It also provides capability to create a new password rule or copy an existing password rule.
- Use the "Password Rules" on page 1438 page to define settings and restrictions for the new password rule.
- Use the "Character Rules" on page 1438 page to create rules which define character restrictions for the sections of the password.
- Use the Summary page to view a summary report of the new password rule to be created. When you click **Finish**, the new password rule is created and populated with the values specified in the **New Password Rule** wizard.

The **New Password Rule** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new password rule. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New Password Rule** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new password rule, click **Finish**.

Cancel
To exit the wizard without creating the new password rule, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new password rule you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new password rule.

New based on:
Select an existing password rule to base the new password rule on. The settings in the new password rule are initialized to those of the existing password rule.

Password Rule Details
This section requires a name and an optional description.

Name:
Specify the name for the new password rule you are creating. When creating a new password rule, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)

- underscore (_)
- space ( )

The name must be unique among existing password rule names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text for your password rule. The description can be up to 1024 characters with no character restrictions.

Password Rules

Use the Password Rules page to specify the properties for the new password rule. After entering the information, click **Next** to proceed to the next page.

Password never expires
Select whether this password should expire after a set number of days or never expire.

Minimum length
Enter the minimum length of characters you are allowing for this part of the password.

Maximum length
Enter the maximum length of characters you are allowing for this part of the password.

Consecutive characters
Enter the number of times a character can be repeated consecutively. Zero means not set.

History count
Enter the number of previous passwords that are saved before a password can be reused.

Character Rules

Use the Character Rules page to specify the properties for the parts that you want to define for the password rule. A *character rule* sets specific rules for an individual part of the password. Use the **Actions** list to add additional rule parts, edit existing rule parts, remove a rule part for this password rule, or move a rule part up or down in the list of rule parts. After entering the information, click **Next** to proceed to the next page.

Minimum length
The minimum length of characters you are allowing for this part of the password. This value cannot be less than one.

Maximum length
The maximum length of characters you are allowing for this part of the password. This value cannot be less than one. The maximum must be greater than or equal to the minimum number of characters.

Alphabetic characters
Whether you Allowed, Not allowed, or Required use of an alphabetic character in the defined property. Use the drop-down arrow to make your selection.

Numeric characters
Whether you Allowed, Not allowed, or Required use of a numeric character in the defined property. Use the drop-down arrow to make your selection.

Special characters
Whether you Allowed, Not allowed, or Required use of a special character in the defined property. Use the drop-down arrow to make your selection.

Special characters include: greater than (>), less than (<), tilde (~), exclamation mark (!), at sign (@), number sign (#), question mark (?), dollar sign ($), vertical bar (|), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses ( ), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), back slash (\), forward slash (/), period (.), comma (,), colon (:), accent (`), quotation mark ("), semicolon (;), and apostrophe (').

Custom Character Set 1
Specifies a user-defined character set for this rule.

Custom Character Set 2
Specifies a second user-defined character set for this rule.

Add/Edit Character Rules

Use this action to add or edit the character rules for this fragment of the password. A *character rule* sets specific rules for an individual part of the password.

Minimum length
The minimum length of characters you are allowing for this part of the password. This value cannot be less than one.

Maximum length
The maximum length of characters you are allowing for this part of the password. This value cannot be less than one. The maximum must be greater than or equal to the minimum number of characters.

Alphabetic characters
Whether you Allowed, Not allowed, or Required use of an alphabetic character in the defined property. Use the drop-down arrow to make your selection.

Numeric characters
Whether you Allowed, Not allowed, or Required use of a numeric character in the defined property. Use the drop-down arrow to make your selection.

Special characters
Whether you Allowed, Not allowed, or Required use of a special character in the defined property. Use the drop-down arrow to make your selection.

Special characters include: greater than (>), less than (<), tilde (~), exclamation mark (!), at sign (@), number sign (#), question mark (?), dollar sign ($), vertical bar (|), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses ( ), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), back slash (\), forward slash (/), period (.), comma (,), colon (:), accent (`), quotation mark ("), semicolon (;), and apostrophe (').

Custom Character Set 1
Specifies a user-defined character set for this rule.

Custom Character Set 2
Specifies a second user-defined character set for this rule.

Additional functions on this window include:

OK
To perform the operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Password Rule Details

Use the **Password Rule Details** task to view and manage the properties of a password rule. You cannot modify the system defined password rules (Basic, Standard, and Strict). Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each view.

- Select the "General" on page 1440 navigation link or the **Expand** icon to display the General details tab section.
- Select the "Password Rules" on page 1440 navigation link or the **Expand** icon to display the Password Rule details tab section.
- Select the "Character Rules" on page 1440 navigation link or the **Expand** icon to display the Character Rule details tab section.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**. This function is available only for user-defined password rules.

Apply
To save the current changes for the role without exiting the task, click **Apply**. This function is available only for user-defined password rules.

Close
To exit the window, click **Close**. This function is available only for system defined password rules since they cannot be modified.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved. This function is available only for user-defined password rules.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to modify a description of a password rule.

Name:
Specifies the name for the password rule you are modifying.

Description:
Specify an optional meaningful text for your password rule.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This value cannot be modified.

Password Rules

Use the Password Rules details tab section to specify the settings and restrictions to which the password must adhere. After entering the information, click **Next** to proceed to the next page.

Note: You cannot change the rule data for the Basic, Strict, and Standard password rules.

Password never expires
Select whether this password should expire after a set number of days or never expire.

Minimum length
Enter the minimum length of characters you are allowing for this part of the password.

Maximum length
Enter the maximum length of characters you are allowing for this part of the password.

Consecutive characters
Enter the number of times a character can be repeated consecutively. Zero means not set.

History count
Enter the number of previous passwords that are saved before a password can be reused.

Case sensitive
Specifies whether or not the password should be treated in a case sensitive manner. By default, this setting is selected.

Character Rules

Use the Character Rules details tab section to specify the properties for the parts that you want to define for the password rule. A *character rule* sets specific rules for an individual part of the password. Use the **Actions** list to add additional rule parts, edit existing rule parts, remove a rule part for this password rule, or move a rule part up or down in the list of rule parts. After entering the information, click **Next** to proceed to the next page.

Minimum length
The minimum length of characters you are allowing for this part of the password. This value cannot be less than one.

Maximum length
The maximum length of characters you are allowing for this part of the password. This value cannot be less than one. The maximum must be greater than or equal to the minimum number of characters.

Alphabetic characters
Whether you Allowed, Not allowed, or Required use of an alphabetic character in the defined property. Use the drop-down arrow to make your selection.

Numeric characters
Whether you Allowed, Not allowed, or Required use of a numeric character in the defined property. Use the drop-down arrow to make your selection.

Special characters
Whether you Allowed, Not allowed, or Required use of a special character in the defined property. Use the drop-down arrow to make your selection.

Special characters include: greater than (>), less than (<), tilde (~), exclamation mark (!), at sign (@), number sign (#), question mark (?), dollar sign ($), vertical bar (|), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses ( ), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), back slash (\), forward slash (/), period (.), comma (,), colon (:), accent (`), quotation mark ("), semicolon (;), and apostrophe (').

Custom Character Set 1
Displays a user-defined character set for this rule.

Custom Character Set 2
Displays a second user-defined character set for this rule.

Add/Edit Character Rules

Use this action to add or edit the character rules for this fragment of the password. A *character rule* sets specific rules for an individual part of the password.

Minimum length
The minimum length of characters you are allowing for this part of the password. This value cannot be less than one.

Maximum length
The maximum length of characters you are allowing for this part of the password. This value cannot be less than one. The maximum must be greater than or equal to the minimum number of characters.

Alphabetic characters
Whether you Allowed, Not allowed, or Required use of an alphabetic character in the defined property. Use the drop-down arrow to make your selection.

Numeric characters
Whether you Allowed, Not allowed, or Required use of a numeric character in the defined property. Use the drop-down arrow to make your selection.

Special characters
Whether you Allowed, Not allowed, or Required use of a special character in the defined property. Use the drop-down arrow to make your selection.

Special characters include: greater than (>), less than (<), tilde (~), exclamation mark (!), at sign (@), number sign (#), question mark (?), dollar sign ($), vertical bar (|), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses ( ), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), back slash (\), forward slash (/), period (.), comma (,), colon (:), accent (`), quotation mark ("), semicolon (;), and apostrophe (').

Custom Character Set 1
Specifies a user-defined character set for this rule.

Custom Character Set 2
Specifies a second user-defined character set for this rule.

Additional functions on this window include:

OK
To perform the operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

LDAP Server Definitions

This task is used by an access administrator or a user that is assigned a role with Manage LDAP Server Definitions task permission. Use this task to create a new LDAP server definition or you can edit or remove an existing LDAP server definition. The Lightweight Directory Access Protocol (LDAP) support gives you the option to configure your console to use an LDAP server to perform user ID and password authentications at logon time. An LDAP server maintains a tree-structured database serving as a convenient place to put hierarchical information, such as a corporate employee directory. Each level of the LDAP tree generally represents a different type of information.

The **LDAP Server Definitions** dashboard view displays a list of all currently defined LDAP server definitions with LDAP server definition summary sections as follows:

General
This section contains the description for the selected LDAP server definition.

Host Connection Information
This section contains the primary host name, backup host name, connection port, Secure Sockets Layer (SSL) connection, allow self-signed or untrusted server certificates descriptions.

Initial Bind information
This section contains the Distinguished Name (DN) to bind with and is used to perform the search.

Directory Entry Location
This section specifies the method and details on how to locate a user's directory entry.

You can view the object summary using the **Expand** or **Collapse** icons to view or hide sections. You can create a LDAP server definition using the **New LDAP Server Definition** wizard or manage an existing LDAP server definition with **LDAP Server Definition Details**.

- Click **"New LDAP Server Definition" on page 1443**() to create a new LDAP server definition. When the new **LDAP Server Definition** wizard completes, the new LDAP server definition is added to the LDAP Server Definitions list.

- Click **"LDAP Server Definition Details" on page 1445**() to view or modify an existing LDAP server definition.

- Click **Delete** () to delete an existing LDAP server definition. You cannot delete an LDAP server definition that is being utilized by at least one user or user template.

New LDAP Server Definition

Use the **New LDAP Server Definition** wizard to guide you through creating a new LDAP server definition. The **New LDAP Server Definition** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted.

- Use the "Name" on page 1443 page to specify the LDAP server definition name and optional description. It also provides capability to create a new LDAP server definition or copy an existing LDAP server definition.
- Use the "Host Connection" on page 1444 page to set host connection information.
- Use the "Bind Information" on page 1444 page to optionally add users directory entry credentials.
- Use the "Directory Location" on page 1445 page to specify directory entry location settings.
- Use the Summary page to view a summary report of the new LDAP server definition to be created. When you click **Finish**, the new LDAP server definition is created and populated with the values specified in the **New LDAP Server Definition** wizard.

The New **LDAP Server Definition** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new LDAP server definition. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New LDAP Server Definition** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new LDAP server definition, click **Finish**.

Cancel
To exit the wizard without creating the new LDAP server definition, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new LDAP server definition. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new LDAP server definition

New based on:
Select an existing LDAP server definition to base the new LDAP server definition on. The settings in the new LDAP server definition are initialized to those of the existing LDAP server definition.

LDAP Server Definition Details
This section requires a name and an optional description.

Name:
Specify the name for the user you are creating or managing. When creating a new LDAP server definition, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)

- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing LDAP server definition names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text for your LDAP server definition. The description can be up to 1024 characters with no character restrictions.

Host Connection

Use the Host Connection page to add the host connection name for the LDAP server definition. After entering the information, click **Next** to proceed to the next page.

Primary host name:
Specify the host name or IP address of the computer running the enterprise directory server.

Backup host name:
Specify the host name or IP address of the computer running a backup enterprise directory server. This field is optional, but if specified, this server is accessed if the primary server is not accessible. The LDAP directory hosted by this server is expected to be a mirror of the primary server, allowing the same entry lookup criteria to be used.

Connection port:
Specify the TCP port on which the server accepts connections. If a port is not specified, the default port is used: 389 for a non-secure connection, 636 for a secure connection. 636 is used if you selected **Use a Secure Sockets Layer (SSL) connection**.

Use a Secure Sockets Layer (SSL) connection
Select if you want the console to use a secure socket connection when connecting to the LDAP server. This requires that the LDAP server and the console support a common SSL or TLS version (see the **Customize Console Services** task) and that they also support a common cipher suite.

Allow self-signed or untrusted server certificates
If you selected to use a secure sockets layer connection, then option to allow self signed or untrusted server certificates is available. Selecting this option suppresses the error that would otherwise be recognized when the server returns its certificate to the authentication client and that certificate is found to be signed by an unrecognized Certificate Authority. If the server's certificate is signed by a corporate signing certificate, then another option is to import that signing certificate using the **Certificate Management** task. After the import, the server's certificate chain can be verified.

Bind Information

Use the Bind Information page to optionally add the distinguished name (DN) and password for the new LDAP server definition. After entering the information, click **Next** to proceed to the next page.

Distinguished Name (DN):
Specify a distinguished name to bind with for initial connection. This DN is used to perform the search. If no connection name is specified, the initial connection is anonymous. The fully-qualified name of an entry is called the *distinguished name (DN)*. It is formed by starting with the name of the entry and appending the name of the nodes encountered when going from that entry to the root of the tree, separated by commas.

For example: "cn=Tom Smith, loc=New York, ou=ABC, o=xyz.com"

Password:
Specify a password to bind with on the initial connection. This is only required when a bind name is specified.

Confirm password:
Re-specify the password that you previously entered.

Directory Location

Use the Directory Location page to set a distinguished name pattern or search tree. After entering the information, click **Next** to proceed to the next page.

Use DN pattern:
Specify the distinguished name pattern in the input field. The DN pattern must include the characters `{0}`, indicating where in the pattern the user ID should be substituted. The user ID will be either the name of the user on the console, or, if provided, the string entered into the **LDAP User ID** field of the user definition.

Search DN tree:
Specify the distinguished name in the input field to find a user's directory entry by searching the distinguished name tree, then select one of the following search scope options:

- Select **Entire tree** to search the entire subtree under the base distinguished name entry.
- Select **One level** to search only one level under the base distinguished name entry.

Specify an LDAP **Search filter** that selects the user's entry in the directory. This usually matches an attribute in the entry against the user ID. The pattern must include the characters `{0}`, indicating where in the pattern the user ID should be substituted. The user ID will be either the name of the user on the console, or, if provided, the string entered into the **LDAP User ID** field of the user definition.

LDAP Server Definition Details

Use the **LDAP Server Definition Details** task to view and modify the properties of a selected LDAP server definition. Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each view.

- Select the "General" on page 1445 navigation link or the **Expand** icon to display the General details tab section.
- Select the "Host Connection" on page 1446 navigation link or the **Expand** icon to display the Host Connection details tab section.
- Select the "Bind Information" on page 1446 navigation link or the **Expand** icon to display the Bind Information details tab section.
- Select the "Directory Entry Location" on page 1446 navigation link or the **Expand** icon to display the Directory Entry Location details tab section.

Additional functions on this window include:

OK
To save the current changes and exit, click **OK**.

Apply
To save the current changes for the LDAP server definition without exiting the task, click **Apply**.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to modify the description for the LDAP server definition.

Name:
Specifies the name for the LDAP server definition you are modifying.

Description:
Specify an optional meaningful text for your LDAP server definition.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This value cannot be modified.

Host Connection

Use the Host Connection details tab section to view or modify the host connection name of the LDAP server definition.

Primary host name:
Specify the host name or IP address of the computer running the enterprise directory server.

Backup host name:
Specify the host name or IP address of the computer running a backup enterprise directory server. This field is optional, but if specified, this server is accessed if the primary server is not accessible. The LDAP directory hosted by this server is expected to be a mirror of the primary server, allowing the same entry lookup criteria to be used.

Connection port:
Specify the TCP port on which the server accepts connections. If a port is not specified, the default port is used: 389 for a non-secure connection, 636 for a secure connection. 636 is used if you selected **Use a Secure Sockets Layer (SSL) connection**.

Use a Secure Sockets Layer (SSL) connection
Select if you want the console to use a secure socket connection when connecting to the LDAP server. This requires that the LDAP server and the console support a common SSL or TLS version (see the **Customize Console Services** task) and that they also support a common cipher suite.

Allow self-signed or untrusted server certificates
If you selected to use a secure sockets layer connection, then the option to allow self signed or untrusted server certificates is available. Selecting this option suppresses the error that would otherwise be recognized when the server returns its certificate to the authentication client and that certificate is found to be signed by an unrecognized Certificate Authority. If the server's certificate is signed by a corporate signing certificate, then another option is to import that signing certificate using the **Certificate Management** task. After the import, the server's certificate chain can be verified.

Bind Information

Use the Bind Information details tab section to view or modify the bind information of the LDAP server definition.

Distinguished Name (DN):
Specify a distinguished name to bind with for initial connection. This DN is used to perform the search. If no connection name is specified, the initial connection is anonymous. The fully-qualified name of an entry is called the *distinguished name (DN)*. It is formed by starting with the name of the entry and appending the name of the nodes encountered when going from that entry to the root of the tree, separated by commas.

For example: "cn=Tom Smith, loc=New York, ou=ABC, o=xyz.com"

Password:
Specify a password to bind with on the initial connection. This is only required when a bind name is specified.

Confirm password:
Re-specify the password that you previously entered.

Directory Entry Location

Use the Directory Entry Location details tab section to view or modify the directory entry location of the LDAP server definition.

Use DN pattern:
Specify the distinguished name pattern in the input field. The DN pattern must include the characters "`{0}`", indicating where in the pattern the user ID should be substituted. The user ID will be either the name of the user on the console, or, if provided, the string entered into the **LDAP User ID** field of the user definition.

Search DN tree:
Specify the distinguished name in the input field to find a user's directory entry by searching the distinguished name tree, then select one of the following search scope options:

- Select **Entire tree** to search the entire subtree under the base distinguished name entry.
- Select **One level** to search only one level under the base distinguished name entry.

Specify an LDAP **Search filter** that selects the user's entry in the directory. This usually matches an attribute in the entry against the user ID. The pattern must include the characters "{0}", indicating where in the pattern the user ID should be substituted. The user ID will be either the name of the user on the console, or, if provided, the string entered into the **LDAP User ID** field of the user definition.

Multi-Factor Authentication

This task is used by an access administrator, a user ID that is assigned access administrator roles or a user that is assigned a role with multi-factor authentication task permission.

Use this task to enable or disable users and templates for HMC multi-factor authentication (HMC MFA) or IBM Z Multi-Factor Authentication, and reset shared secret keys for one or more users and templates. You can use the **GUIDANCE** information for assistance.

You can choose one of the following options from this window.

"IBM Z MFA" on page 1448
To assign a user or template with IBM Z Multi-Factor Authentication, which provides RSA SecurID authentication through the IBM Z MFA servers, click **IBM Z MFA**.

"HMC MFA" on page 1447
To assign a user or template with Time-based One-Time Password (TOTP) authentication verified by the console, click **HMC MFA**.

HMC MFA

Use the HMC MFA option to enable or disable users and users defined by templates for HMC multi-factor authentication (HMC MFA) and reset shared secret keys for one or more users and templates. You can use the **GUIDANCE** information for assistance.

Proceed with "Users and Templates" on page 1447 to configure for HMC MFA.

Users and Templates

Use this table to enable or disable HMC MFA for users and users defined by templates. You can select one or multiple names when enabling or disabling users and templates. You can also sort and search within this table. The table columns represent the following:

Name
Displays the names for all the users and templates. Use the arrow in the heading to sort the names alphabetically. Use the search icon above the table to locate a particular user name or template name.

Type
Displays the type of name (**User** or **Template**). Use the arrows in the heading to group the users or the templates.

HMC MFA
Displays a check mark for those users or templates, which have HMC MFA enabled. Use the arrows in the heading to group all the users and templates, which are enabled for HMC MFA.

As you select one or more users or templates to enable or disable for HMC MFA, options appear in an action bar above the table. Also, as you complete an option, a message is displayed above the table indicating the action is complete.

Note: You can select more than one name but the **Type** and HMC MFA enablement must be the same for all selected names.

The action bar selection includes:

Enable
To enable HMC multi-factor authentication for the selected users and templates, click **Enable**. A check mark is displayed in the HMC MFA column when the user or template is enabled for multi-factor authentication.

Disable
To disable HMC multi-factor authentication for the selected users and templates, click **Disable**. A check mark is no longer displayed in the HMC MFA column when the user or template is disabled for multi-factor authentication.

Reset Shared Secret Key
To have the selected users and templates receive a new shared secret key the next time they logon to the console, click **Reset Shard Secret Key**. This action is only available when all selections are enabled for HMC MFA.

Cancel
To return to the table without making any updates to the selection, click **Cancel**.

If multi-factor authentication is enabled for a User Template, then all users who are associated with that User Template through a User Pattern are required to use multi-factor authentication to log on to the console.

As changes are made within this table, success messages or error messages are displayed above the table. When you are done reviewing the messages, click the **x** to close.

IBM Z MFA

Use the **IBM Z MFA** option to assign users and users defined by templates IBM Z Multi-Factor Authentication. This authentication provides RSA SecurID authentication through the IBM Z MFA servers.

Ensure that “Servers” on page 1448 are identified for authentication, then you can manage “Users and templates” on page 1449 for IBM Z Mulit-Factor Authentication.

Servers

Before you enable users or templates for IBM Z MFA authentication, you must define and configure IBM Z MFA servers.

Note: Multiple IBM Z MFA servers are recommended for high availability.

If there are currently no servers available, click **Add Server** to define a multi-factor authentication server. The "Add a server" window is displayed. Provide the following information when you are defining a server.

Name
Provide a name for the MFA server. This name must be 1 - 64 characters long and can be made up of the following:

- Alphanumeric characters
- Blanks
- Periods
- Underscores
- Dashes
- at sign (@)

The name cannot be made up of leading or trailing blanks.

Description
Provide a description of the server. This field is optional.

Hostname or IP
Provide the hostname or IP address of the server.

Port
Provide the port number of the server. Default port number is 6789.

Cancel
To return to the previous window without adding a server, click **Cancel**.

Add
To add this server for IBM Z MFA, click **Add**. The "Trust and import MFA server certificate" window is displayed if the server has not been trusted.

Note: If the HMC attempts to connect to the IBM Z MFA server and it is not successful, then the server cannot be added.

The following actions can be used from this window.

Cancel
To return to the previous window without trusting this certificate, click **Cancel**.

Trust certificate
When you verified the content of this IBM Z MFA server certificate, click **Trust certificate** to proceed to add this server to the IBM Z MFA server table.

Note: You can import and trust a certificate ahead of time by using the **Certificate Management** task.

When servers are defined, use this table to manage the servers for IBM Z MFA. You can sort on each of the columns within this table and use the search function from the top of the table. The table consists of the following information.

Name
Identifies the name of the server.

Description
Displays a description of the server if a description was provided.

Hostname or IP
Displays the hostname or IP address of the server.

Port
Displays the port number of the server.

For each entry in the table, you can click the Actions icon (⋮) to perform the following functions for each server. As changes are made within this table, success messages or error messages are displayed above the table. When you are done reviewing the messages, click the **x** to close.

Edit
To change any of the values for the server, click **Edit** to make the updates. The "Edit server" window is displayed. You can make your change, then click **Save**. A success message is displayed to indicate that the change is saved.

Test connectivity
To test the connectivity of the server, click **Test connectivity**. A message is displayed to show that the connection is verified.

Remove
To delete a server you no longer need, click **Remove**. The "Remove server" window is displayed. You can verify that the server needs to be removed, then click **Remove**. A message is displayed to show that the server was removed and no longer appears in the table.

Users and templates

Use this table to enable or disable IBM Z MFA for one or more users and templates. You can select one or multiple names when enabling or disabling users and templates. You can also sort and search within this table. The table columns represent the following:

Name
Displays the names for all the users and users defined by templates. Use the arrow in the heading to sort the names alphabetically. Use the search icon above the table to locate a particular user name or template name.

MFA ID
Specifies the MFA ID of the user or the MFA override attribute of the template.

Type
Displays the type of name (**User** or **Template**). Use the arrows in the heading to group the users or the templates.

Primary
Specifies the primary IBM Z MFA server.

Backup
Specifies the backup IBM Z MFA server

Policy
Specifies a defined policy.

As you select one or more users or templates to enable or disable for IBM Z MFA, options appear in an action bar above the table. As changes are made within this table, success messages or error messages are displayed above the table. When you are done reviewing the messages, click the **x** to close.

Note: You can select more than one name but the **Type** and IBM Z MFA enablement must be the same.

Enable
To enable IBM Z MFA for the selected users and templates that have matching MFA configurations, click **Enable**. The "Enable IBM Z MFA" window is displayed. Provide an MFA ID or MFA override attribute, server, and policy information, then click **Enable**. The information you just input appears in the Users and templates table.

Disable
To disable IBM Z MFA for the selected users and templates, click **Disable**. A check mark is no longer displayed in the IBM Z MFA column when the user or template is disabled for multi-factor authentication.

Cancel
To return to the table without making any updates to the selection, click **Cancel**.

If multi-factor authentication is enabled for a User Template, then all users who are associated with that User Template through a User Pattern are required to use multi-factor authentication to log on to the console.

User Settings

Accessing the User Settings task

Notes:

- If Customizable Data Replication is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see the **Configure Data Replication** task.
- Only a user ID assigned access administrator roles sets the defaults of the Hardware Management Console settings by using the **Console Default User Settings** task.
- Because there are many main users interfaces (one for each logged on user), the Hardware Management Console provides each user the ability to change settings. In other words, if you change confirmation settings or controls, this does not cause that same change for other logged-on users.

This task enables you to customize settings that control how the Hardware Management Console operates. You can choose settings such as: single object selection, show tips, or choose when to display or not display confirmation windows.

User Settings

Use the **User Settings** task to customize settings that control how you want the console to operate for your user ID.

User Settings tabs

Use these tabs to control how you want the console to operate for your user ID.

"Confirmations" on page 629
To customize your preferences for using confirmation windows for a subset of console workplace tasks, select the **Confirmations** tab.

"Controls" on page 630
To select the object controls that you prefer, select the **Controls** tab.

Additional options are available from these pages:

Apply
To save the settings currently displayed on this tab, click **Apply**.

Reset
To discard any changes you made to the settings on this tab, and display again the current settings for this window, click **Reset**. If changes have been saved by clicking **Apply**, you can no longer discard the changes.

Defaults
To return to the preferences on this tab to the settings that are the default for the current user, click **Defaults**.

Note: If you are using this option from the **Console Default User Settings** task, then you are returning to the preferences on this tab to the settings that are the system default for all users.

OK
To save the settings on all tabs, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Confirmations

Use this page to customize preferences for using confirmation windows for a subset of tasks.

The preferences you set for using confirmation windows apply to the following subset of tasks:

- Activate
- Deactivate
- Load
- PSW Restart
- Reboot Support Element
- Remove Object Definition
- Reset Clear
- Reset Normal
- Single Object Operations
- Start All Processors
- Stop All Processors

You can customize the console for displaying a confirmation window upon starting any of the tasks listed above. A confirmation window identifies the task and, optionally, lists the task's target objects. The console operator must use a confirmation window either to confirm starting the task or to cancel it instead.

Confirmation windows reduce the possibility of inadvertently performing tasks, particularly tasks that may disrupt the operation of the Central Processor Complex (CPC) or its images.

Customize the settings to indicate your preferences, then click **Apply**.

Enabled with object list
To display a confirmation window upon starting any of the tasks listed above and to list the task's target objects, select **Enabled with object list**.

Note: The **Load** task does not support this option.

Enabled without object list
To display a confirmation window upon starting any of the tasks listed above, but without listing the task's target objects, select **Enabled without object list**.

Do not show confirmations
To start the tasks listed above without displaying confirmation windows, select **Do not show confirmations**.

Use 'No' as the default action
To set the confirmation window's default action to 'No' upon starting any of the tasks listed above, select **Use 'No' as the default action**.

- If this is selected (a check mark appears) it indicates the default action for the confirmation window is to cancel the task. That is, the **No** button is preselected on the confirmation window, click **No** to cancel the task.
- If this is not selected (a check mark does not appear) it indicates the default action for the confirmation window is to confirm starting the task. That is, the **Yes** button is preselected on the confirmation window, click **Yes** to confirm starting the task.

Controls

Use this page to select the object controls to use on the console.

Single object selection
To select only one object at a time while working on a task, select **Single object selection**. Otherwise, more than one object can be selected while working on a task.

Show tips each time you logon
To display different console facts or tips each time you log on, select **Show tips each time you logon**.

Accept Console Messenger messages
To allow your console sessions to receive Console Messenger chat and broadcast messages, select **Accept Console Messenger messages**. Otherwise, your sessions will not receive these messages, and other sessions attempting to initiate chats with your session will be told that you have elected not to participate in chats.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task.

Bring Chat Window to foreground on new message
The initial chat message window is always displayed in the foreground to notify you of the incoming chat message.

To have the Console Messenger task continue to bring an open chat message window to the foreground after the initial message is received, select **Bring Chat Window to foreground on new message**.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task.

Display timestamps using
To define the time zone that is used to localize timestamps, for those tasks that use timestamps. Select the drop-down arrow to choose your preference.

Notes:

- This is only available for those tasks that are enabled to respect this timestamp setting.
- From the **User Settings** task, if you change your preference and apply this change, a message appears indicating you must restart your login session before the change appears.

Client Time Zone
To display timestamps localized to the time zone of the client browser, select **Client Time Zone**. If you are on a local session, this is the same as the Console Time Zone.

Console Time Zone
To display timestamps localized to the time zone of the Hardware Management Console, select **Console Time Zone**. This is the default. If you are on a local session, this is the same as the Client Time Zone.

UTC Time Zone
To display timestamps localized to the UTC time zone, select **UTC Time Zone**.

Console Default User Settings

Use the **Console Default User Settings** task to set the default settings for operating the console.

Only the ACSADMIN default user ID or a user ID with access administrator roles can access this task.

This task will not affect currently logged on users until they log off then log back on.

Console Default User Settings tabs

Use these tabs to set the defaults for controlling how the console operates for all users.

“Confirmations” on page 629
To set preferences for using confirmation windows for a subset of console workplace tasks, select the **Confirmations** tab.

“Controls” on page 630
To set the object controls, select the **Controls** tab.

Additional options are available from these pages:

Apply
To save the settings currently displayed on this window, click **Apply**.

Reset
To discard any changes you made to the settings on this window, and display again the current settings for this window, click **Reset**.

Defaults
To return to the preferences that are the default for the current user, click **Defaults**.

OK
To save the settings, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Users and Tasks

Accessing the Users and Tasks task

This task displays a list of the tasks that are running and the users that are currently logged on to the Hardware Management Console.

To work with the users and tasks:

1. Open the **User and Tasks** task. The Users and Tasks window is displayed.
2.
3. The following information is displayed in the *Users Logged On* portion of the window:
   - An ID number associated with the user that is logged on
   - User ID you are logged in as and the other user IDs that are logged in to the console
   - Time the user ID logged in
   - Number of tasks running
   - User ID access location
   - Information about tasks that are running.

   The following information is displayed in the *Running Tasks* portion of the window:
   - Task ID number associated to the task that is running
   - Name of the task that is running
   - Object names that may be targeted for that task
   - An ID number associated with the user running the task
   - Time the task was started.

   Notes:
   - If you are assigned a user ID with access administrator roles, you can:
     - Logoff or disconnect any user from the session (click **Logoff** or **Disconnect**).
     - Terminate any task from the session (click **Terminate**).
   - You can only switch to another task in your own session.
   - You can terminate your own session.
4. You can initiate a two-way chat with another user by selecting the user name and clicking **Chat With**. You can also switch to another task that is running in your session by selecting the task and clicking **Switch To**.
5. When you have completed the task, click **Close**.

Users and Tasks

Use this task to display a list of the users that are currently logged on to the console.

User's Logged On
This table displays the following information:

Session Id
Specifies the identification number associated with the user that is logged on to the console.

User Name
Specifies the user identification that is logged on to the console.

Logon Time
Specifies the time the user logged on to the console.

Running Tasks
Specifies the number of tasks currently running for the user.

Access Location
Specifies the location the user is accessing the console from.

Notes
Contains additional and useful information pertaining to the session.

If you are assigned a user ID with Access Administrator roles you can select a user from the list and click **Logoff** or **Disconnect**.

Logoff
If you are assigned a user ID with Access Administrator roles, you can select a user from the list and click **Logoff** to log the user off of the console, otherwise this is not an option.

Disconnect
If you are assigned a user ID with Access Administrator roles, you can select a user from the list and click **Disconnect** to disconnect the user from the console, otherwise this is not an option.

Chat With

To initiate a two-way chat with the user of the selected session, click **Chat With**. The **Console Messenger Chat** window is displayed where you can begin your messaging.

If you make more than one selection from the **Users Logged On** list a separate chat window is displayed for each chat partner.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task and enable the **Console messenger** option.

Running Tasks
This table displays the tasks that are currently running and provides the following information:

Task Id
Specifies a task identification number associated to the task that is running.

Task Name
Specifies the name of the task that is running.

Targets
Specifies (if any) the object name(s) that are targeted for that task.

Session Id
Specifies the identification number associated with the user running the task.

Start Time
Specifies the time the task was started.

Switch To
To switch to another task that is running in your session, select the task from the list, then click **Switch To**.

Terminate
To end a task that is running in your session, select the task from the list, then click **Terminate**. If you are assigned a user ID with Access Administrator roles you can end tasks that are in other sessions.

Close
To end this task, click **Close**.

Help
To display help for the current window, click **Help**.

View Activation Profiles

View Activation Profiles

Use this task to view activation profiles for the central processor complex (CPC) and their images.

There are four types of activation profiles:

- Reset profile displays information to activate a CPC and its images
- Load profile displays information to load a previously activated image with a control program or operating system.
- Image profile displays information to activate an image of a CPC previously activated

- Group profile displays information in specifying the capacity of a group of logical partitions.

The following functions are also available from this window:

Cancel
To close the profile page, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Profile Tree

This lists all pages for the current profile and a list of referenced profiles and their pages.

Reset pages

The Reset activation profile, referred to also as a CPC profile, displays the CPC name and each image supported by the CPC.

Make a selection from the Profile Tree to view the Reset Profile pages:

General
Displays the selected reset profile and its purpose, and identifies the Input/Output (I/O) configuration and operating mode established for the CPC by the profile.

Storage
Displays the storage configuration established for the CPC by the profile.

Dynamic
Displays information that controls whether the Input/Output (I/O) configuration established for the CPC activated by the profile.

Options
Displays options and information for enabling or disabling global input/output (I/O) priority queuing and customizing options for error handling and recovery for the CPC activated by the profile.

CP/SAP
Indicates the number of Central Processors (CPs) and System Assist Processors (SAPs) configured for the CPC.

Fenced
Displays the number of available processors when a book is fenced and the processor assignments.

Partitions
Displays a list of logical partitions activated, and the order in which they were activated, on the CPC activated by the profile.

The window includes a section of image pages for each logical partition listed on the **Partitions** page. The information in each section is used to activate the multiple images supported by the CPC.

General

Displays information that describes the selected profile and its purpose and identifies the Input/Output (I/O) configuration and operating mode established for the Central Processor Complex (CPC) activated by the profile.

Profile name
Displays the name of the reset profile selected.

Description
Displays information that describes the contents or purpose of the profile.

IOCDS table
Identifies the Input/Output Configuration Data Set (IOCDS) used during activation to define the Input/Output (I/O) configuration for the Central Processor Complex (CPC).

The I/O configuration is the set of all I/O devices and channel paths available to the CPC.

Input/Output Configuration Data Set
Displays the data set identifier and name of the IOCDS.

Type
Identifies the operating mode supported by the IOCDS.

Note: Activation will fail if a mismatch exists between an IOCDS and mode.

Allow Dynamic I/O
Indicates whether the IOCDS defines an I/O configuration that supports dynamic changes.

Partitions
This column displays the names of logical partitions supported by the IOCDS.

Mode
Identifies the operating mode established during activation to support the number and type of control programs that can operate on the Central Processor Complex (CPC).

Load delay for power sequencing
Specifies the amount of time delayed between completing power-on reset and performing a load.

Storage

This window displays the storage available for allocating to the CPC's logical partitions. The **Mode** list in **General** of this reset profile identifies the operating mode you selected for activating the CPC.

Installed storage
Displays the CPC's amount of installed storage in megabytes.

Customer storage
Displays the storage amount available for allocating to the Central Processor Complex's (CPC) logical partitions.

Dynamic

This window displays information that controls whether the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) activated by the profile can be dynamically changed.

This window displays the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) activated by the profile.

Indicates activating this profile establishes an I/O definition that can be dynamically changed. That is, dynamic I/O will be enabled. Otherwise, this indicates the I/O definition cannot be changed dynamically. That is, dynamic I/O will not be enabled.

The input/output (I/O) definition is the set of all I/O devices and channel paths available to a central processor complex (CPC). An input/output configuration data set (IOCDS) is used during power-on reset as the source of the I/O definition.

Ordinarily, changing the I/O definition requires performing a power-on reset with a modified or different IOCDS. Dynamically changing the I/O definition does not require a power-on reset.

Dynamically changing the I/O definition requires support from the selected IOCDS and from the Hardware Configuration Definition (HCD) feature of a Multiple Virtual Storage (MVS) operating system.

Options

This window displays options and information that enable or disable the global input/output (I/O) priority queueing and options for error handling and recovery for the Central Processor Complex (CPC) activated by the profile.

Enable global input/output (I/O) priority queuing
Indicates whether global I/O priority is enabled or disabled after initial microcode load (IML).

Global I/O priority queuing allows the operating system to specify a priority to be associated with an I/O request at Start Subchannel time. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

Automatic input/output (I/O) interface reset
Indicates whether the I/O interface is reset automatically when any condition occurs that causes shared control units to hold reserves on their devices

- A machine check places the Central Processor Complex (CPC) in a check stopped state.
- A control program places a logical partition in a non-restartable wait state.

Indicates the I/O interface is reset automatically if any of the listed conditions occurs. Otherwise, this indicates the I/O interface is not reset automatically.

In a multiple CPC environment, several objects, which can be CPCs or logical partition, may share the control units, channel paths, and I/O devices included in their I/O interfaces.

Each condition listed above causes shared control units to hold reserves on their devices for the object affected by the condition. Holding reserves provides the affected object with exclusive use of devices, preventing them from being used by other objects that share the control units.

Resetting the I/O interface releases reserves held by shared control units assigned to an object. Their devices become available to other objects.

System recovery time

Indicates whether there is a limit on the amount of time the Central Processor Complex (CPC) is allowed to spend on error handling and recovery.

Limit system recovery time
If selected, recovery time is limited. Otherwise, there is no limit on the amount of time the CPC is allowed to spend on error handler recovery.

When recovery time is limited, error handling and recovery must complete within the specified time limit, otherwise the CPC is put into a checkstop state.

When there is no time limit, the CPC uses as much time as necessary to handle errors. But this does not imply that all errors will be resolved, regardless of how much time the CPC spends on them.

Note: The limit specified for recovery time also determines the type of recovery that is attempted.

Time limit
If recovery time is limited, displays the amount of time the Central Processor Complex (CPC) allowed to spend on error handling and recovery before it is put into a checkstop state.

Note: This field is applicable only when **Limit system recovery time** is selected. Otherwise, this field is unavailable.

The amount of time determines the type of recovery that is attempted. If recovery time is not limited, then all types of recovery are attempted.

Processor running time

Indicates how processor running time is determined.

Processor running time is the amount of continuous time allowed for logical processors to perform jobs on shared processors. The amount of continuous time is also referred to as a timeslice.

Dynamically determined by the system
Indicates the running time whenever the number of active logical processors changes.

Determined by the user
Indicates the constant running time.

Running time
Indicates the constant amount of running time set for logical processors to perform jobs on shared processors in the **Running time** field.

The running time specified is assigned to all logical processors shared by logical partitions activated without dedicated processing resources. Each logical partition has control of shared processor

resources for the specified running time. Control passes to the next logical partition when the running time interval expires.

Do not end the timeslice if a partition enters a wait state (HMC Version 2.13.1 and earlier)
Displays the processor running time determined by the user to indicate whether logical processors lose their share of running time when their logical partition enters a wait state.

Indicates logical processors do not lose their share of running time when the logical partition enters a wait state. Instead, if the logical partition enters a wait state, processor resources allocated to it are idle until the end of the wait state, or the end of the running time. Otherwise, it indicates logical processors lose their share of running time when the logical partition enters a wait state. That is, idle processor resources are allowed to be used by another logical processor immediately. The share of running time ends for the logical partition that enters the wait state, and a new timeslice begins for another logical partition.

Display fenced book page
Indicates whether or not to display the fenced page.

CP/SAP

Note: This page is available on the Hardware Management Console Version 2.13.1 and earlier.

This window displays the number of Central Processors (CPs) and System Assist Processors (SAPs) to configure for the Central Processor Complex (CPC).

The window lists the configurations of CPs and SAPs that can be established. The machine type and model of the CPC determine its possible configurations:

- All CPCs have a default configuration.
- Some CPCs have additional configurations available. That is, some CPC's allow configuring one or more CPs as additional SAPs.

The CPC's default configuration is listed first, followed by its additional configurations, if any.

CP/SAP table

CPs
Displays the number of central processors (CPs) in each configuration.

SAPs
Displays the number of SAPs in each configuration.

The physical processor units installed in a central processor complex (CPC) are used either as central processors (CPs) or system assist processors (SAPs). The model of your machine determines its default configuration of CPs and SAPs. The SAPs are used exclusively for input/output (I/O) instruction processing.

Some CPC machine types and models allow configuring one or more CPs as additional SAPs. If other CP/SAP configurations are available, selecting a configuration that configures one or more CPs as additional SAPs may improve the performance of some types of applications (applications that have greater needs for I/O instruction processing, for example). But this reduces the default number of CPs available which may affect how the CPC can be activated.

Internal coupling facility processors (ICFs)
Displays the number of internal coupling facility processors (ICFs).

Integrated facilities for Linux (IFLs)
Displays the number of integrated facilities for Linux (IFLs).

IBM zEnterprise Application Assist Processors (zAAPs)
Displays the number of IBM zEnterprise Application Assist Processors (zAAPs).

IBM z Integrated Information Processors (zIIPs)
Displays the number of IBM z Integrated Information Processors (zIIPs).

Defective processing units
Displays the number of defective processing units.

Fenced Book

This window displays the available system processors assigned when a hardware problem occurs with one of the system books that caused that book to be fenced or become unavailable for use.

- **Number of available processors for Licensed Internal Code** indicates the number of processors that are available in your system.
- **Number of available processors when a book is fenced** indicates the number of processors that your system can use when one book is fenced from use.
- **Number of available processors when a XX processors book is fenced** XX indicates the number of processors that your system can use when the specified processors book is fenced from use.

Processor assignment controls
Displays the processor assignment option.

Determined by the system
Displays if you selected the system to determine how to assign all available processors when a book is fenced from use in your system.

Determined by the user
Displays if you selected to manually assign the processors to your system when a book is fenced from use.

Processor assignments

Displays the processor assignment when a XX processors book is fenced
The XX indicates the number of processors fenced from use.

Processor type
Displays the physical processor assigned to the logical partitions logical processors

LICCC Definition
Displays the amount of licensed internal code installed in your system

Value Used when Book is Fenced
Indicates how many processors have been assigned to the specified processor types.

Partitions

Displays a list of logical partitions to be activated and the order in which they are activated on the Central Processor Complex (CPC) activated by the profile.

Partition
Displays the names of the logical partitions to activate.

Order
Displays the numeric positions of the logical partitions in the activation order.

For each logical partition to be activated, information for activating it in its corresponding set of image pages displays. To display the image pages for a logical partition, select its pages from the profile tree view on the left side of the window.

Load

This window displays information that controls loading a control program for the logical partition activated by the profile.

Profile name
Specifies the name of the profile currently displayed.

Description
Displays information about the contents or the purpose of the profile.

Load type
Indicates the type of load to perform for the logical partition. You would use the SCSI or NVMe dump option to do a standalone dump to a SCSI device or NVMe adapter.

Standard load
Indicates to perform the load on the logical partition.

Note: You must select this choice if you want to perform the **Store status** function and the **Store status** clear check box must be unchecked.

SCSI load
Indicates to IPL from a device that requires a SCSI IPL.

SCSI dump
Indicates to IPL a standalone dump program from a device that requires a SCSI IPL.

NVMe load
Indicates to IPL from a device that requires a NVMe IPL.

NVMe dump
Indicates to IPL a standalone dump program from a device that requires a NVMe IPL.

Clear the main memory on this partition before loading it
Indicates to clear main memory storage on the logical partition before a load.

Note: Available when **Standard load**, **SCSI load**, or **NVMe load** are selected. Clearing partitions with larger amounts of main memory storage may take longer.

Enable Secure Boot for Linux
Indicates to verify the signature of the load program and distributor's signature match.

Load address
Displays the address of the input/output (I/O) device that provides access to the control program to load. This should contain four or five hexadecimal digits.

A load address is required to complete this page.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device may store the control program or may be used to read the control program from a data storage medium.

Use dynamically changed address
Indicates whether the load address is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition.

Load parameter
Displays the optional information, if any, to use to further control how the control program is loaded.

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Use dynamically changed parameter
Indicates whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition.

Time-out value
Indicates the amount of time to allow for the completion of the load.

If the load operation cannot be completed within the specified time, the operation is canceled.

This field is unavailable if a load type of **SCSI load** or **SCSI dump** is selected.

Store status
Indicates whether the store status function is performed before the load starts.

If this is not selected the store status function is not performed. Otherwise, the store status function is performed before the load starts.

The store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations.

Note: This is applicable only when the selected load type is **Standard load**. Otherwise, this selection is unavailable.

Worldwide port name
Displays the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI IPL or SCSI Dump.

This field is disabled if a load type of **Standard load** is selected.

Logical unit number
Displays the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI IPL or SCSI Dump.

This field is disabled if a load type of **Standard load** is selected.

Boot program selector
Displays the program to load from the FCP-load device. Valid range from 0 to 30.

This field is disabled if a load type of **Standard load** is selected.

Boot record logical block address
Displays the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

This field is disabled if a load type of **Standard load** is selected.

Operating system specific load parameters
Displays a variable number of characters to be used by the program that is loaded during SCSI IPL or SCSI Dump. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

This field is disabled if a load type of **Standard load** is selected.

Image pages

This window displays an activation profile for activating a logical partition as an image. The window displays the image name.

Make a selection from the Profile Tree to view the image pages in the profile:

General
Displays the image profile and its purpose, and identifies the operating mode established for the logical partition activated by the profile.

Processor
Displays information that assigns logical processors to the logical partition activated by the profile.

Security
Displays settings that determine the extent of interaction between the logical partition activated by the profile and other logical partitions activated on the CPC.

Storage
Displays the amount of storage assigned to the logical partition activated by the profile.

Options
Displays the image option for the processor values.

Load
Displays information that controls loading a control program for the logical partition activated by the profile.

Note: Not available when Coupling facility, Secure Service Container, or zAware are selected on the **General** image page.

zAware
Displays the image options for the zAware partition.

Notes:

1. The zAware mode is applicable for z13, zEC12, and zBC12.
2. Not available when Coupling facility is selected on the **General** image page.

"SSC" on page 1474
Displays the image options for the selected SSC partition.

Crypto
Displays information that controls how the logical partition activated by the profile uses the coprocessors and accelerators assigned to it.

Note: Not available when Coupling facility or zAware are selected on the **General** image page.

Time Offset
Displays the logical partition's clock using an offset from the External Time Source's time of day.

Note: Available when **Logical partition offset** is selected on the **General** image page.

General

Displays information on the image profile and its purpose and identifies the operating mode established for the logical partition activated by the profile.

Profile name
Specifies the name of the profile currently displayed.

Description
Displays additional information about the profile, such as the contents or purpose of the profile.

Note: A description is recommended, but optional is and optional profile parameter; some profiles may not have one. The person who customizes the profile provides or omits its description.

Partition identifier
Displays the number of the partition (in hexadecimal). This is used by the program that is operating in the logical partition.

The partition identifier must also be unique among the identifiers of other logical partitions activated by this profile. If necessary, check the partition identifier fields on the other **General** image pages to verify the partition identifier assigned to this image is unique.

Mode
Displays the operating mode established during activation to support the type of control program that can operate on the logical partition.

The mode determines some of the other types of information included in the image profile. Different profile information is associated with each different mode.

Clock type assignment
Identifies a time source for setting the logical partition's time-of-day (TOD) clock.

The logical partition's clock is synchronized with the central processor complex time-of-day clock (CPC TOD clock). Ordinarily, the logical partition's clock is set to the same time as the CPC's time source (either the CPC TOD clock or an external time reference, such as a Sysplex Timer or Server Time Protocol (STP). But you can use this group box to select another source for setting the logical partition's clock.

Standard time of day
Indicates the logical partition's clock is set to the same time the CPC's time source (either the CPC TOD clock or an external time reference, such as the Sysplex Timer or STP).

Logical partition time offset
Indicates the logical partition's clock is set using an offset from the External Time Source's time of day.

Processor

This window displays information that determines the allocation and management of processor resources assigned to the logical partition activated by the profile.

Displays the logical partition's logical processor assignment.

Note: The **Mode** list on the **General** image page lists the operating modes. The logical partition operates in the selected mode upon being activated with this profile. Depending on the selected mode and what processors are installed in your system will determine the allocation and management of the processor resources.

You can find more detailed help on the following elements of this window:

Group name

Displays the group profile name assigned to the logical partition, A logical partition can be assigned to only one group.

Note: If the group profile name is blank, then the logical partition is not assigned to a group.

Logical processor assignment (CPs - General and SSC modes)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned to it and, if the logical partition shares other processors.

Note: The zAware mode is applicable for z13, zEC12, and zBC12.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates a central processor is dedicated to each logical processor.

Not dedicated central processors
Indicates the logical processors share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when the logical partition is activated).

Logical processor assignment (CPs/zAAPs/zIIPs - General mode)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned and if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates a central processor is dedicated to each logical processor.

Dedicated zEnterprise Application Assist Processors (zAAPs)
Indicates zEnterprise Application Assist Processors (zAAPs) are assigned to each logical processor.

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

Dedicated z Integrated Information Processors (zIIPs)
Indicates the selected z Integrated Information Processors (zIIPs) are assigned to each logical processor.

Not dedicated central processors
Indicates the logical processors share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when the logical partition is activated).

Not dedicated zEnterprise Application Assist Processors (zAAPs)
Indicates the logical processors share not dedicated zEnterprise Application Assist Processors (zAAPs) (zAAPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

Not dedicated z Integrated Information Processors (zIIPs)
Indicates the logical processors share not dedicated z Integrated Information Processors (zIIPs) (zIIPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Logical processor assignment (CPs/ICFs - Coupling facility mode)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned to it and, if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates that a central processor is dedicated to each logical processor.

Dedicated internal coupling facility processors
Indicates *Dedicated internal coupling facility processors* are dedicated to each logical processor.

Not dedicated central processors
Indicates the logical processors share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated internal coupling facility processors
Indicates the logical processors share *not dedicated internal coupling facility processors* (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Dedicated internal coupling facility processors and not dedicated central processors
Indicates the selected *Dedicated internal coupling facility processors* and *not dedicated central processors* are assigned to the logical partition.

Dedicated and not dedicated internal coupling facility processors
Indicates the selected *Dedicated and not dedicated internal coupling facility processors* and *not dedicated central processors* are assigned the logical partition

Logical processor assignment (CPs/IFLs - Linux only mode)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned to it and, if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates the selected central processor is dedicated to each logical processor.

Dedicated integrated facility for Linux
Indicates the selected *Dedicated integrated facility for Linux* processors are dedicated to each logical processor.

Not dedicated central processors
Indicates the selected logical processors share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated integrated facilities for Linux
Indicates the selected logical processors share *not dedicated integrated facilities for Linux* (Integrated Facilities for Linux (IFL) that are not already dedicated to other activated logical partitions when this logical partition is activated).

Logical processor assignment (CPs/zAAPs/zIIPs/ICFs/IFLs - z/VM mode)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned to it and, if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates the selected central processor is dedicated to each logical processor.

Dedicated zEnterprise Application Assist Processors (zAAPs)
Indicates the selected IBM zEnterprise Application Assist Processors (zAAPs) are assigned to each logical processor.

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

Dedicated z Integrated Information Processors (zIIPs)
Indicates the selected z Integrated Information Processors (zIIPs) are assigned to each logical processor.

Dedicated internal coupling facility processors
Indicates the selected *internal coupling facility processors* are assigned to each logical processor.

Dedicated integrated facilities for Linux
Indicates the selected *integrated facilities for Linux* are assigned to each logical processor.

Not dedicated central processors
Indicates the selected logical processors share *not dedicated central processor*s (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated zEnterprise Application Assist Processors (zAAPs)
Indicates the selected logical processors share not dedicated IBM zEnterprise Application Assist Processors (zAAPs) (zAAPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.

Not dedicated z Integrated Information Processors (zIIPs)
Indicates the selected logical processors share not dedicated z Integrated Information Processors (zIIPs) (zIIPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated internal coupling facility processors
Indicates the selected logical processors share *not dedicated internal coupling facility processors* (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated integrated facilities for Linux
Indicates the selected logical processors share *not dedicated integrated facilities for Linux* (integrated facilities for Linux that are not already dedicated to other activated logical partitions when this logical partition is activated).

Number of processors (General, Coupling facility, Linux only, and SSC modes)

Displays the number of processors that are used each time you activate a partition.

Note: The zAware mode is applicable for z13, zEC12, and zBC12.

A *logical processor* is the processor resource defined to operate in a logical partition as a physical processor. A logical partition's control program uses its logical processors to perform jobs for the logical partition.

Initial
Indicates the number of logical processors to assign to the logical partition.

The number of processors can be from one to the maximum number of physical processors available to the logical partition. The maximum number of processors available is limited by:

- The number of physical processors configured an available.
- The number of processors supported by the operating mode selected on the **General** image page.

- The number of processors that are not already dedicated to another active logical partition at the time of the next activation.
- The number of processors supported by the control program at the time of the next activation.

Reserved
Indicates the number of reserved processors available that you want assigned to the logical partition.

Reserved processors can be configured online at a later time. Reserved processors can be defined at partition activation time, but are not used during partition activation. Instead, they are configured offline during activation automatically, and can be manually configured online. The reserved processor may or may not be available when the system is activated. If it is not available when the system is activated, it can become available during concurrent upgrade.

The ability to add and remove dedicated processors does not require deactivating/activating the partitions. This support is not restricted to concurrent upgrade purposes.

Note: This field is application only when the following selection is made:

- **Dedicated central processors**
- **Not dedicated central processors**
- **Dedicated internal coupling facility processors**
- **Not dedicated internal coupling facility processors**
- **Dedicated integrated facility for Linux**
- **Not dedicated integrated facility for Linux**

Processor type (General, z/VM, and Coupling facility modes)

Displays the number of processors that are used each time you activate a partition.

A *logical processor* is the processor resource defined to operate in a logical partition as a physical processor. A logical partition's control program uses its logical processors to perform jobs for the logical partition.

Initial
Displays the number of logical processors to assign to the logical partition.

The number of processors can be from one to the maximum number of physical processors available to the logical partition. The maximum number of processors available is limited by:

- The number of physical processors configured an available.
- The number of processors supported by the operating mode selected on the **General** image page.
- The number of processors that are not already dedicated to another active logical partition at the time of the next activation.
- The number of processors supported by the control program at the time of the next activation.

Reserved
Displays the number of reserved processors available that you want assigned to the logical partition.

Reserved processors can be configured online at a later time. Reserved processors can be defined at partition activation time, but are not used during partition activation. Instead, they are configured offline during activation automatically, and can be manually configured online. The reserved processor may or may not be available when the system is activated. If it is not available when the system is activated, it can become available during concurrent upgrade.

The ability to add and remove dedicated processors does not require deactivating/activating the partitions. This support is not restricted to concurrent upgrade purposes.

Note: This field is application only when the following selection is made:

- **Dedicated internal coupling facility processors and not dedicated central processors**
- **Dedicated and not dedicated internal coupling facility processors**

Not dedicated processor details (General, Coupling facility, Linux only, z/VM, and SSC modes)

Displays the initial processing weight, minimum and maximum processing weight, whether initial capping and workload manager are enabled, and absolute capping.

Note: The zAware mode is applicable for z13, zEC12, and zBC12.

Initial processing weight

Displays the logical partition's processing weight for sharing the not dedicated processors.

The *not dedicated* processors are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *processing weight* is its share of the not dedicated processors. The processing weight can be from 1 to 999.

The exact percentage of the not dedicated processors allocated to the logical partition depends upon the processing weights of other logical partitions defined and activated on the same Central Processor Complex (CPC). That percentage is calculated by dividing the logical partition processing weight by the sum of the processing weights of all active logical partitions on the CPC.

A processing weight is a target, not a limit. It represents the share of the not dedicated processor resources guaranteed to a logical partition when all the resources are in use. When resources are available, this logical partition can borrow them if necessary. When this logical partition is not using its share of the resources, other logical partitions can use those resources.

Notes:

1. While excess resources are available, processing weights have no effect on how those resources are used. Weights take effect when the number of logical processors requiring a timeslice is greater than the number of not central processors.
2. This field is available only when either of the following selections are made:
   - **Not dedicated central processors**
   - **Not dedicated internal coupling facility processors**
   - **Dedicated internal coupling facility processors and not dedicated central processors**

     Note: This option is only available on the console for Version 2.10.2 and earlier.
   - **Not dedicated integrated facility for Linux**
   - **zEnterprise Application Assist Processors (zAAPs)**

     Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
   - **Not dedicated z Integrated Information Processors (zIIPs)**

   Otherwise, this field is unavailable.

Initial capping

Indicates the logical partition is prevented from using the not dedicated processors in excess of its processing weight.

Indicates logical partition *cannot* use the not dedicated processors in excess of its processing weight. That is, the processing weight is capped.

Otherwise, it indicates it can use the not dedicated processors in excess of its processing weight when the resources are not in use by another logical partition. That is, the processing weight is not capped.

The *Not dedicated processors* are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *processing weight* is its share of the not dedicated processors. Ordinarily, a processing weight is a target, not a limit. When the processing weight is *capped*, it is a limit.

Note: If this logical partition's share of the not dedicated processors is capped, it does not affect the shares set for other activated logical partitions.

This field is available only when either of the following selections are made:

- **Not dedicated central processors**
- **Not dedicated integrated coupling facility processors**
- **Dedicated integrated coupling facility processors and not dedicated central processors**

  Note: This option is only available on the console for Version 2.10.2 and earlier.
- **Dedicated and not dedicated internal coupling facility processors**

  Note: This option is only available on the console for Version 2.10.2 and earlier.
- **Not dedicated Integrated Facility for Linux**
- **Not dedicated zEnterprise Application Assist Processors (zAAPs)**

  Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
- **Not dedicated z Integrated Information Processors (zIIPs)**. Otherwise, this field is unavailable.

Otherwise, this field is unavailable.

Enable workload manager

Indicates either **Enable workload manager** or **Initial capping** is enabled, but not both.

Displays the minimum and maximum processing weights.

This field is available only when either of the following selections are made:

- **Not dedicated integrated facility for Linux**
- **Not dedicated central processors**
- **zEnterprise Application Assist Processors (zAAPs)**

  Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
- **Not dedicated z Integrated Information Processors (zIIPs)**

Otherwise, this field is unavailable.

Absolute Capping

Indicates the logical partition *can* use the not dedicated processors absolute capping number to limit the logical partition's activity. The absolute capping value is either None or a number of processors value from 0.01 to 255.0 specified.

Otherwise, it indicates the logical partition *cannot* use the not dedicated processors absolute capping when the resources are in use by another logical partition. That is, the processing absolute number is not capped.

The *Not dedicated processors* are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *absolute capping* is its share of the not dedicated processors. When the absolute processing value is *capped*, it is a limit.

Notes:

- If this logical partition's share of the not dedicated processors is capped, it does not affect the shares set for other activated logical partitions.
- This field is available only when either of the following selections are made:
  - **Not dedicated central processors**
  - **Not dedicated integrated coupling facility processors**
  - **Not dedicated integrated facility for Linux**
  - **Not dedicated zEnterprise Application Assist Processors (zAAPs)**

    Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
  - **Not dedicated z Integrated Information Processors (zIIPs)**

  Otherwise, this field is unavailable.

Security

Displays settings that determine the extent of interaction between the logical partition activated by the profile and other logical partitions activated on the same Central Processor Complex (CPC).

Partition security options

Displays the security options for the logical partitions activated by the profile.

Global performance data control
Indicates whether the logical partition can be used to view the processing unit activity data for all other logical partitions activated on the same CPC.

Input/output (I/O) configuration control
Indicates whether the logical partition can be used to read and write any Input/Output Configuration Data Set (IOCDS) in the configuration.

This option indicates the logical partition can also be used to change the input/output (I/O) configuration dynamically and controls whether or not a logical partition can enter configuration mode.

Cross partition authority
Indicates whether the logical partition can be used to issue control program instructions that reset or deactivate other logical.

Logical partition isolation
Indicates whether reconfigurable channel paths assigned to the logical partition are reserved for its exclusive use.

When selected, channel paths are configured off; they will not become available to other logical partitions.

When not selected, reconfigurable channel paths assigned to this logical partition are not reserved for its exclusive use. Its channel paths can be configured off and reassigned to other logical partitions.

Counter facility security options

Displays the security options for the logical partitions activated by the profile.

Basic counter set authorization control
Indicates whether authorization is allowed to use the basic counter set. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

Problem state counter set authorization control
Indicates whether authorization is allowed to use the problem-state counter set. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

Crypto activity counter set authorization control
Indicates whether authorization is allowed to use the crypto-activity counter set. The set can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

Extended counter set authorization control
Indicates whether authorization is allowed to use the extended counter set, The counters of this set are model dependent.

Coprocessor group counter sets authorization control
Indicates whether authorization is allowed to use the coprocessor-group counter sets. This set can be used to count the crypto activities of a coprocessor.

Note: This option is available on the Hardware Management Console Version 2.11.1 and earlier.

Sampling facility security options

Specifies the sampling facility security options for the logical partitions activated by the profile.

Basic sampling authorization control
Indicates whether authorization is allowed to use the basic-sampling function. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

CP assist for cryptographic functions

Specifies the CP Assist Cryptographic Functions (CPACF) for the logical partitions activated by the profile.

Permit AES key import functions
Displays the current AES key import functions setting for CPACF when the logical partition is activated.

Permit DEA key import functions
Displays the current DEA key import functions setting for CPACF when the logical partition is activated.

Permit ECC key import functions
Displays the current Elliptical Curve Cryptography (ECC) key import functions setting for CPACF when the logical partition is activated.

Storage

Displays the amount of storage assigned to the logical partition activated by the profile. Logical partition storage allocation is composed of central storage assignments and expanded storage assignments.

Central storage

Central storage is the amount of storage that is available to allocate for main storage.

Amount in
Displays the amount of storage that is installed in the selected partition.

Initial
Displays the amount of central storage to allocate to the logical partition upon activation.

Initial storage is allocated to a logical partition in a contiguous block of one Gigabyte (GB) units. The logical partition has exclusive use of its initial storage. That is, it is not shared with other active logical partitions.

You must allocate at least 64MB of initial storage when the logical partition will operate in coupling facility mode. Otherwise, for any other operating mode, you must allocate at least 1 MB of initial storage.

Reserved
Displays the amount of central storage that can be reconfigured dynamically to the logical partition after activation. This field is only active if the operating mode selected on the **General** image page is **General**, **LINUX only**, or **z/VM** mode. It is not available in coupling facility mode.

Reserved storage is allocated to a logical partition in a contiguous block of one Gigabyte (GB) units, and is contiguous to an located above its initial storage. But, unlike its initial storage, the logical partition does not have exclusive use of its reserved storage. The reserved storage provides the logical partition wit an additional amount of storage to use only if it is not already being used by another active logical partition.

The is no minimum for reserved storage. Zero gigabytes (0 GB) is a valid amount of reserved storage.

Storage origin
Displays how the central storage origin is determined.

Determined by the system
Displays the Central Processor Complex (CPC) determine the central storage origin.

The CPC allocates central storage, wherever sufficient, contiguous space is available.

Determined by the user
Indicates the selected central storage origin is established in this profile.

Origin
Displays the megabyte where storage allocation begins when the central storage origin is determined by the user through this profile.

When this profile is used to activate a logical partition, sufficient and contiguous space must be available from the origin for the amount of central storage specified. Logical partition activation fails if sufficient storage is not available from the origin, regardless of whether the origin is determined by the system or by the user through this profile.

Virtual Flash Memory

Displays the amount and Virtual Flash Memory storage allocated to the logical partition. The virtual memory increments in 16 GB amounts with a maximum of 6144 GB.

Initial
Displays the initial amount of virtual flash memory for the selected partition in 16 GB increments.

Maximum
Displays the maximum amount of virtual flash memory to a allow for the selected partition.

Options

Displays the image options for the processor values on this window:

Minimum and Maximum I/O priority values can be specified at a partition level. These minimum and maximum I/O priority values can both be set at partition activation time or dynamically (post partition activation).

Minimum I/O priority
The minimum value must be less than or equal to the maximum value entered. This value can range from 0 to the maximum I/O priority allowed for that processor.

The minimum default is a priority value of 0.

Maximum I/O priority
This maximum processor I/O priority is obtained from new System Information support.

The maximum default is a priority value of 0.

Defined capacity
The measure of processor resource consumption for a logical partition, expressed in millions of service units (MSU) per hour.

CP management cluster name
The name specified for the CP management cluster.

zAware

Displays the zAware network configuration settings for the selected zAware logical partition.

Note: This tab is only applicable for z13, zEC12, and zBC12.

The zAware configuration settings are:

Master user ID
Specifies the master user ID for the selected zAware logical partition.

Master password
Specifies the master password for the selected zAware logical partition.

Host name
Specifies the host name for the selected zAware logical partition.

Default gateway
Specifies the default gateway IPv4 or IPv6 address.

You can find more detailed help on the following elements of this window:

Network Adapters

The Network Adapters table displays the IP address and details settings for the zAware logical partition. You can use the **Select Action** list from the table tool bar to display table views.

CHPID
Displays the CHPID for the selected zAware logical partition.

VLAN
Displays the VLAN for the selected zAware logical partition.

IP address
Displays the IPv4 or IPv6 address for the selected zAware logical partition. Also, indicates DHCP or Link Local if that is the specific IP address type.

Mask/Prefix
Displays the Mask/Prefix for the IPv4 or IPv6 address specified.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions in the Network Adapters table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

DNS Servers

The DNS Servers table displays the IPv4 or IPv6 address for the selected zAware logical partition. You can use the **Select Action** list from the table tool bar to display table views.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.jkltoys.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all host names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

IP address
Displays the current IPv4 or IPv6 address for the selected zAware logical partition.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions in the DNS Servers table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

SSC

This window displays the configuration settings for the selected logical partition in IBM Secure Service Container (Secure Service Container) mode.

Note: Cryptographic (CRYPTO) options can be selected for the Secure Service Container partition.

The Secure Service Container configuration settings include the following:

Boot selection
Displays the Boot selection for the selected Secure Service Container partition.

Secure Service Container installer
Displays until the Secure Service Container partition is restarted and the input fields contain information that was previously defined.

Secure Service Container
Displays after the Secure Service Container partition is restarted. The **Reset Logon Settings** and **Reset Network Settings** can be updated after the restart.

Master user ID
Displays the master user ID for the selected Secure Service Container logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or embedded blanks. Valid characters for a master user ID name are numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Displays the master password for the master user ID you specified.

A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Displays again the same master password you specified in the **Master password** field.

Host name
Displays the host name for the selected Secure Service Container logical partition.

A host name can be from one to 32 characters long. It cannot have special characters or embedded blanks. Valid characters for a host name are alphanumeric characters, periods (.), colons (:), and hyphens (-).

IPv4 gateway
Displays the default gateway IPv4 address for the selected Secure Service Container logical partition.

IPv6 gateway
Displays the default gateway IPv6 address for the selected Secure Service Container logical partition.

Network Adapters

The Network Adapters table displays the IP address and details settings for the Secure Service Container logical partition.

CHPID
Displays the CHPID for the selected Secure Service Container logical partition.

VLAN
Displays the VLAN for the selected Secure Service Container logical partition.

Port
Displays the Port 0/1 parameter for the selected Secure Service Container logical partition.

IP address
Displays the IPv4 or IPv6 address for the selected Secure Service Container logical partition. Also, indicates DHCP or Link Local if that is the specific IP address type.

Mask/Prefix
Displays the Mask/Prefix for the IPv4 or IPv6 address specified.

DNS Servers

The DNS Servers table displays the IPv4 or IPv6 address for the selected Secure Service Container logical partition.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.jkltoys.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all host names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

IP address
Displays the current IPv4 or IPv6 address for the selected Secure Service Container logical partition.

Load

Displays information that controls loading a control program for the logical partition activated by the profile.

Note: The image pages do not include this additional page if the operating mode selected on the **General** image page is coupling facility mode.

Load during activation
Indicates whether the load is performed during activation.

If it has been selected it indicates a load is performed. The other information on the window is used to perform the load. Otherwise, a load is not performed.

Load type
Indicates the type of load to perform for the logical partition. You would use the SCSI dump option to do a standalone dump to a SCSI device.

Standard load
Indicates to perform the load on the logical partition.

SCSI load
Indicates to IPL from a device that requires a SCSI.

SCSI dump
Indicates to IPL a standalone dump program from a device that requires a SCSI IPL.

NVMe load
Indicates to IPL from a device that requires a NVMe IPL.

NVMe dump
Indicates to IPL a standalone dump program from a device that requires a NVMe IPL.

Enable Secure Boot for Linux
Indicates to verify the signature of the load program and distributor's signature match.

Load address
Displays the address of the input/output (I/O) device that provides access to the control program to load. Contains four or five hexadecimal digits.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device can store the control program or can be used to read the control program from a data storage medium.

Use dynamically changed address
Indicates whether the load address is dynamically determined by changes to the channel subsystem Input/Output definition (I/O).

Load parameter
Displays the optional information, if any, to use to further control how the control program is loaded during activation.

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Use dynamically changed parameter
Indicates whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition.

Time-out value
Displays the amount of time to allow for the completion of the load.

The time-out value can be from 60 to 600 seconds. If the load operation cannot be completed within the specified time, the operation is canceled.

This field is unavailable if a load type of **SCSI load** or **SCSI dump** is selected.

Worldwide port name
Indicates the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI IPL or SCSI Dump.

If the selected load type is **Standard load** this field is unavailable.

Logical unit number
Indicates the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI IPL or SCSI Dump.

If the selected load type is **Standard load**, this field is unavailable.

Boot program selector
Displays the program to load from the FCP-load device. Valid range from 0 to 30.

If the selected load type is **Standard load**, this field is unavailable.

Boot record logical block address
Displays the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

If the selected load type is **Standard load**, this field is unavailable.

Operating system specific load parameters
Indicates a variable number of characters to be used by the program that is loaded during SCSI IPL or SCSI Dump. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

If the selected load type is **Standard load**, this field is unavailable.

Crypto

This window displays information that controls how the logical partition activated by the profile uses the coprocessors and accelerators assigned to it. The settings are referred to here as *cryptographic controls*, and apply to the logical partition only if it is customized for using coprocessors and accelerators.

Control domain index
Displays the cryptographic domain index (CDX) numbers of one or more control domains for the logical partition.

A logical partition's *control domains* are those cryptographic domains for which remote secure administration functions can be established and administered from this logical partition.

But a logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), select at least one control domain and matching usage domain. Refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Control and Usage domain index
Displays the cryptographic domain index (CDX) numbers of one or more usage domains for the logical partition.

A logical partition's *control and usage domains* are domains in the cryptos that can be used for cryptographic functions. The usage domains cannot be removed if they are online.

A logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Cryptographic candidate list
Identifies which coprocessors from the candidate and online list will be assigned to the logical partition at the next activation.

Cryptographic online list
Identifies which coprocessors from the candidate and online list will be brought online at the next activation.

The logical partition must be activated to bring the coprocessors or accelerators online.

Time Offset

This window displays the Central Processor (CPC) External Time Source settings and how it is applied when the logical partition's clock is set.

Note: The image profile includes this window only if the clock type selected on the **General** page of the logical partition's image profile is **Logical partition time offset**.

Offset
Indicates the number of days, hours, and minutes you want to set for the offset from the External Time Source's time of day. You can set an offset within the following range:

- 0 to 999 days
- 0 to 23 hours
- 0, 15, 30, or 45 minutes

days
Indicates the number of days, from 0 to 999, that you want to set for the offset from the External Time Source's time of day.

hours
Indicates the number of hours, from 0 to 23, that you want to set for the offset from the External Time Source's time of day.

minutes
Indicates the number of minutes, 0, 15, 30, or 45, that you want to set for the offset from the External Time Source's time of day.

Decrease system time value by the amount shown
Displays the logical partition's clock *back* setting from the External Time Source's time of day by the number of days, hours, and minutes in the offset.

Increase system time value by the amount shown
Displays the logical partition's clock *ahead* setting of the External Time Source's time of day by the number of days, hours, and minutes in the offset.

Help
To display help for the current window, click **Help**.

Group page

This window displays a group profile name, group description, and group capacity value used in determining the allocation and management of processor resources assigned to the logical partition in the group.

Make a selection from the Profile tree to view the group pages in the profile.

Group name
Displays a group name for logical partition(s) in the group.

Group description
Indicates information that describes the contents or purpose of the profile.

View Console Events

Accessing the View Console Events task

This task enables you to view a record of system events occurring on the Hardware Management Console. System events are individual activities that indicate when processes occur, begin and end, succeed or fail.

When an event occurs, the date and time it occurs and a brief description of the event are recorded in the **Console Event Log**.

To view the console events:

1. Open the **View Console Events** task. The View Console Events window is displayed.

   Initially, all events in the table are displayed in descending order, from the most recent event to the oldest event. You can work with the table by using the table icons from the table toolbar. If you place

your cursor over an icon a description of the icon is displayed. The icons perform the following functions:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** found under a column title to define a filter for that column. This limits the entries in the table. Tables can be filtered to show only those entries most important to you. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

Clear All Filters
Returns the table back to the complete listing.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Quick Filter
Allows you to select a filter category to apply to the filter. By default, all columns are filtered, showing only rows containing a cell whose value includes the filter text. When you click the drop-down arrow, a menu is displayed that allows you to restrict the columns to which the filter is applied.

2. When you have finished reviewing the console events, click **Cancel**.

View Console Events

This task displays console events logged by the console.

The console automatically keeps a log of significant operations and activities, referred to as *console events*, that occur while the application is running.

This window initially displays all console events currently logged and lists them in reverse order of occurrence (from the most recent event to the oldest event).

A filter task bar appears above the table that allows you to change the information that you want displayed, such as, changing the number of events listed or the order of the events.

Events table

This table initially displays the console events in descending order with the following information:

Date
Displays the date and time when the console event occurred. Use the up or down arrow to display the table in ascending or descending order by the date.

Events
Describes the console event logged by the console. Use the up or down arrow to display the table in alphabetical order or reverse alphabetical order by the console event.

You can work with the table by using the filter icons on the task bar above the table. If you place your cursor over an icon the icon description appears.

Filter task bar

The filter task bar includes table filter icons that perform the following functions:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** found under a column title to define a filter for that column. This limits the entries in the table. Tables can be filtered to show only those entries most important to you.

Note: As you are filtering, the information on the bottom of the table indicates the total number of items you are working with and the number of items filtered and displayed.

The filter conditions on **Date** include the following:

All Dates
Displays all events for all dates.

Dates until
Displays only those events up to the date and time you selected.

Dates from
Displays only those events from the current date to the date and time you selected.

Dates between
Displays only those events within the beginning and ending dates and times you selected.

The filter conditions on **Events** include the following (each condition allows you to specify text that should be sorted on and whether or not to match the case of the text being sorted on):

Contains
Displays only those events that includes the **Text** that you specified.

Does not contain
Displays only those events that does not include the **Text** that you specified.

Starts with
Displays only those events that have an event name that begins with the **Text** that you specified.

Ends with
Displays only those events that have an event name that ends with the **Text** that you specified.

Matches
Displays only those events that exactly matches the complete event name that you specified.

Is empty
No events are displayed in the table.

Is not empty
All events are displayed in the table.

Click **OK** when you have defined your filter. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

Clear All Filters
Returns the table back to the complete listing.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Quick Filter
Allows you to select a filter category to apply to the filter. By default, all the columns are filtered, showing only rows containing a cell whose value includes the filter text. When you click the drop-down arrow, a menu is displayed that allows you to restrict the columns to which the filter is applied.

Max page size

Specify the number of entries in the input field that you want displayed at one time in the table, then press Enter. If the total number of events exceed the number that appear in the table you can specify a page number in the entry field to see more entries or click the forward or backward arrows to page through the additional entries. The amount of entries that are displayed is the number you specified in the **Max Page Size** input field.

Note: The maximum page size allowed is 999.

Additional functions from this window include:

Cancel
To close this window when you are done viewing this information, click **Cancel**.

Refresh
To update the table with the most recent events and restore the table defaults, click **Refresh**.

Help
To display help for the current window, click **Help**.

View Console Information

Accessing the View Console Information task

This task displays information about the Hardware Management Console and its licensed internal code. The machine information could include:

- Engineering Change (EC) number
- Machine type
- Version of the Hardware Management Console
- Licensed Internal Code (LIC) control level
- Machine model number
- Engineering Changes AROM
- Machine serial number
- Bundle level of the Hardware Management Console

Licensed internal code controls many of the operations available on the Hardware Management Console. Internal code changes may provide new operations, or correct or improve existing operations.

Product support assigns the EC number to a set of licensed internal code. The number identifies the licensed internal code and its purpose.

If a set of licensed internal code is modified, its EC number is supplemented with a state level. A state level distinguishes between different versions of the same set of licensed internal code.

To view the console information:

1. Open the **View Console Information** task. The View Console Information window is displayed.
2. Select a licensed internal code from the list.
3. Click **EC Details...** to view the additional information about internal code state levels.
4. Click **OK** when you are done viewing the information.

Accessing the System Information task

This task displays information about a selected CPC (server) and its licensed internal code. The machine information could include:

- Engineering Change (EC) number
- Machine type
- Version of the Support Element
- Licensed Internal Code (LIC) control level
- Machine model number
- Engineering Changes AROM or Concurrent Engineering Changes
- Machine serial number
- Driver level of the Support Element
- Bundle level of the Support Element

The internal code changes information includes the engineering change (EC) number, the state levels of each set of licensed internal code associated with the Support Element, and a description.

Licensed internal code controls many of the operations available on the Support Element. Internal code changes may provide new operations, or correct or improve existing operations.

The part number and EC number are assigned to a set of licensed internal code by product support. The numbers identify the licensed internal code and its purpose.

If a set of licensed internal code is modified, its EC number is supplemented with a state level. A state level distinguishes between different versions of the same set of licensed internal code.

To view the system information:

1. Select one or more CPCs (servers).
2. Open the **System Information** task. The System Information window is displayed.
3. Select the internal code information you want to view.
   - To view the additional information about this internal code, click **EC Details...**.
   - To display information about further actions that may need to be taken, click **Query Additional Actions...**.

     Note: This option is available only if the selected CPC is at Version 2.10.0 or later.
4. Click **OK** when you have completed this task.

View Console Information/System Information

Use the **View Console Information** task to display information about the internal code changes stored on the console.

Use the **System Information** task to display information about the internal code changes stored on the Support Element of the selected systems.

Licensed internal code, also referred to as internal code, controls many of the operations available on the console or on the systems and their Support Elements. Internal code changes may provide new internal code, or correct or improve existing internal code.

A console or a systems Support Element automatically keeps records of information about the internal code changes stored on it. The record-keeping begins when changes are retrieved from their source to the console. For each internal code change the information identifies:

- Its Engineering Change (EC) number and description
- The change level most recently retrieved
- The highest retrieved internal code change level that can be installed and activated concurrently
- The change level most recently activated
- The change level most recently accepted
- Additional details include the most recent date and time each task was performed.

The information may assist you with planning and managing the internal code change process. For example, review the information to either:

- Determine whether the console or system is operating with your latest available levels of internal code changes.
- Determine which tasks you must perform next to make the console or system operate with the latest available levels of internal code changes.

Note: Service representatives will provide assistance applying and managing internal code changes.

Machine Information

EC number
Displays the Engineering Change (EC) number of the Hardware Management Console or selected systems where the internal code changes are applied.

Type
Displays the machine type of the Hardware Management Console or selected systems where the internal code changes are applied.

Version
Displays the version of the Hardware Management Console or selected systems where the internal code changes are applied.

LIC control level
Displays the Licensed Internal Code level of the Hardware Management Console or selected systems where the internal code changes are applied.

Model number
Displays the machine model number of the Hardware Management Console or selected systems where the internal code changes are applied.

Engineering Changes AROM
This label is displayed when the system is preloaded for disruptive activation of a new Engineering Changes (ECs) level.

Serial number
Displays the machine serial number of the Hardware Management Console or selected systems where the internal code changes are applied.

Driver
Displays the driver level of the Hardware Management Console or selected systems where the internal code changes are applied.

Note: The Driver information only appears if you are using this task with a user ID definition that is based on the *Service Representative* task roles.

Bundle level
Displays the bundle level of the Hardware Management Console or selected systems where the internal code changes are applied.

Note: This information is not available for IBM zEnterprise 196 and IBM zEnterprise 114 machines and earlier.

Internal Code Change Information

For additional information about an internal code change, select an EC number, then click **EC Details...**.

EC Number
Displays the engineering change (EC) number of the internal code change.

Retrieved Level
Displays the internal code change level that was most recently copied to the console or Support Elements of the systems, making it available for installation.

Installable Concurrent
Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for this console or for the systems, from the current installed level up to and including the installable concurrent level, without disrupting the operations of the systems defined to this console or the operations of the selected systems.

Activated Level
Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the console or selected systems.

Accepted Level
Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the console or selected systems.

Description
Displays a brief description of the internal code change.

Additional functions are available from this window:

EC Details...
To display detailed information for the selected internal code change, click **EC Details...**.

Query Additional Actions...

Note: This option is only available if the selected object is at Version 2.10.0 or later.

To display information for additional actions that are pending, click **Query Additional Actions...**. The **System Information Query Additional Actions** window is displayed. If further actions are required, instructions are provided, otherwise **NO** appears. Click **OK** to close the window.

OK
To close this window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Retrieved Level

This field displays the internal code change level that was most recently copied for an object, making it available for installation.

Compare the number in this field with the number displayed for the **installed level** to determine whether your latest available change level has been installed:

- If the retrieved level is higher than the installed level, then the change level has been retrieved, but has not been installed.

  The object, when activated, will operate without your latest available level of the internal code change.
- If the retrieved level is equal to the installed level, then the change level has been retrieved and installed.

  The object, when activated, will operate with your latest available level of the internal code change.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Installable Concurrent

This field displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for an object, from the current installed level up to and including the installable concurrent level, without disrupting the operations of the console or the operations of the selected system.

Compare the number in this field with the number displayed for the **installed level** to determine whether one or more retrieved change levels can be installed and activated concurrently:

- If the installable concurrent level is blank, then none of the retrieved change levels from the current installed level up to and including the current retrieved level can be installed and activated concurrently.
- If the installable concurrent level is equal to the installed level, then all of the retrieved change levels that can be installed and activated concurrently are already installed.

  Note: Compare the installable concurrent level with the **activated level**. If they are equal, then the installed concurrent change levels are also already activated. Otherwise, you can use console tasks for changing internal code to activate concurrent internal code changes for the object.

- If the installable concurrent level is higher than the installed level, then all retrieved change levels from the current installed level up to and including the installable concurrent level can be installed and activated concurrently.

  Note: You can use console tasks for changing internal code to install and activate concurrent internal code changes for the object.

  For example, when:

  – The **Installed Level** is: 002.

  – And the **Installable Concurrent Level** is: 004.

  Then you can use console tasks for changing internal code to install change levels: 003 and 004, and then activate them without disrupting the operations of the console or selected system.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Activated Level

This field displays the internal code change level that was most recently activated as a working part of the licensed internal code of an object.

Compare the number in this field with the number displayed for the **installed level** to determine whether a more recent change level has been installed:

- If the installed level is higher than the activated level, then a more recent change level has been installed, but has not been activated.

  The object is operating without your latest available level of the internal code change.
- If the installed level is equal to the activated level, then the change level has been installed and activated.

  Note: Compare the installed level with the **retrieved level** to determine whether the object is operating with your latest available level of the internal code change.

If the retrieved change level is installed and activated, compare the number in this field with the number displayed for the **accepted level** to determine whether your latest available change level has been accepted:

- If the activated level is higher than the accepted level, then the change level has been activated, but has not been accepted.

  The object is operating with your latest available level of the internal code change, but it is not yet a permanent working part of the licensed internal code of the object.
- If the activated level is equal to the accepted level, then the change level has been activated and accepted.

  Your latest available level of the internal code change is a permanent working part of the licensed internal code of the object.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Accepted Level

This field displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the object.

Compare the number in this field with the number displayed for the **activated level** to determine whether a more recent change level has been activated:

- If the activated level is higher than the accepted level, then a more recent change level is currently activated, but it is not yet a permanent working part of the licensed internal code of the object.
- If the accepted level is equal to the activated level, then the change level currently activated is a permanent working part of the licensed internal code of the object.

  Note: Check the **retrieved level** and **installed level** to determine whether the object is operating with your latest available level of the internal code change.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

System Information

Use this task to display information about the internal code changes stored on the Support Element of the selected systems.

Licensed internal code, also referred to as internal code, controls many of the operations available on the console or on the systems and their Support Elements. Internal code changes may provide new internal code, or correct or improve existing internal code.

A console or a systems Support Element automatically keeps records of information about the internal code changes stored on it. The record-keeping begins when changes are retrieved from their source to the console or a systems Support Element. For each internal code change the information identifies:

- Its part number and Engineering Change (EC) number, type, and description
- The change level most recently retrieved
- The highest retrieved internal code change level that can be installed and activated concurrently
- The change level most recently activated
- The change level most recently accepted
- Additional details include the most recent date and time each task was performed.

The information may assist you with planning and managing the internal code change process. For example, review the information to either:

- Determine whether the console or system is operating with your latest available levels of internal code changes.
- Determine which tasks you must perform next to make the console or system operate with the latest available levels of internal code changes.

Note: A service representative will provide assistance applying and managing internal code changes.

Machine Information

EC number
Displays the Engineering Change (EC) number of the Hardware Management Console or selected systems where the internal code changes are applied.

Type
Displays the machine type of the Hardware Management Console or selected systems where the internal code changes are applied.

Version
Displays the version of the Hardware Management Console or selected systems where the internal code changes are applied.

LIC control level
Displays the Licensed Internal Code level of the Hardware Management Console or selected systems where the internal code changes are applied.

Model number
Displays the machine model number of the Hardware Management Console or selected systems where the internal code changes are applied.

Engineering Changes AROM
This label is displayed when the system is preloaded for disruptive activation of a new Engineering Changes (ECs) level.

Serial number
Displays the machine serial number of the Hardware Management Console or selected systems where the internal code changes are applied.

Driver
Displays the driver level of the Hardware Management Console or selected systems where the internal code changes are applied.

Note: The Driver information only appears if you are using this task with a user ID definition that is based on the *Service Representative* task roles.

Bundle level
Displays the bundle level of the Hardware Management Console or selected systems where the internal code changes are applied.

Note: This information is not available for IBM zEnterprise 196 and IBM zEnterprise 114 machines and earlier.

Internal Code Change Information

For additional information about an internal code change, select an EC number, then click **EC Details...**.

EC Number
Displays the engineering change (EC) number of the internal code change.

Retrieved Level
Displays the internal code change level that was most recently copied to the console or Support Elements of the systems, making it available for installation.

Installable Concurrent
Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for this console or for the systems, from the current installed level up to and including the installable concurrent level, without disrupting the operations of the systems defined to this console or the operations of the selected systems.

Activated Level
Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the console selected systems.

Accepted Level
Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the console selected systems.

Description
Displays a brief description of the internal code change.

Additional functions are available from this window:

EC Details...
To display detailed information for the selected internal code change, click **EC Details...**.

Query Additional Actions...

Note: This option is only available if the selected object is at Version 2.10.0 or later.

To display information for additional actions that are pending, click **Query Additional Actions...**. The **System Information Query Additional Actions** window is displayed. If further actions are required, instructions are provided, otherwise **NO** appears. Click **OK** to close the window.

OK
To close this window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Retrieved Level

This field displays the internal code change level that was most recently copied for an object, making it available for installation.

Compare the number in this field with the number displayed for the **installed level** to determine whether your latest available change level has been installed:

- If the retrieved level is higher than the installed level, then the change level has been retrieved, but has not been installed.

  The console, when activated, will operate without your latest available level of the internal code change.
- If the retrieved level is equal to the installed level, then the change level has been retrieved and installed.

  The console, when activated, will operate with your latest available level of the internal code change.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Installable Concurrent

This field displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for an object, from the current installed level up to and including the installable concurrent level, without disrupting the operations of the console or the operations of the selected systems.

Compare the number in this field with the number displayed for the **installed level** to determine whether one or more retrieved change levels can be installed and activated concurrently:

- If the installable concurrent level is blank, then none of the retrieved change levels from the current installed level up to and including the current retrieved level can be installed and activated concurrently.
- If the installable concurrent level is equal to the installed level, then all of the retrieved change levels that can be installed and activated concurrently are already installed.

  Note: Compare the installable concurrent level with the **activated level**. If they are equal, then the installed concurrent change levels are also already activated. Otherwise, you can use console tasks for changing internal code to activate concurrent internal code changes for the object.
- If the installable concurrent level is higher than the installed level, then all retrieved change levels from the current installed level up to and including the installable concurrent level can be installed and activated concurrently.

  Note: You can use console tasks for changing internal code to install and activate concurrent internal code changes for the object.

  For example, when:

  – The **Installed Level** is: 002.

  – And the **Installable Concurrent Level** is: 004.

  Then you can use console tasks for changing internal code to install change levels: 003 and 004, and then activate them without disrupting the operations of the console or selected systems.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.

- Each system selected when you start a system task.

Activated Level

This field displays the internal code change level that was most recently activated as a working part of the licensed internal code of an object.

Compare the number in this field with the number displayed for the **installed level** to determine whether a more recent change level has been installed:

- If the installed level is higher than the activated level, then a more recent change level has been installed, but has not been activated.

  The object is operating without your latest available level of the internal code change.
- If the installed level is equal to the activated level, then the change level has been installed and activated.

  Note: Compare the installed level with the **retrieved level** to determine whether the object the object is operating with your latest available level of the internal code change.

If the retrieved change level is installed and activated, compare the number in this field with the number displayed for the **accepted level** to determine whether your latest available change level has been accepted:

- If the activated level is higher than the accepted level, then the change level has been activated, but has not been accepted.

  The objectis operating with your latest available level of the internal code change, but it is not yet a permanent working part of the licensed internal code of the object.
- If the activated level is equal to the accepted level, then the change level has been activated and accepted.

  Your latest available level of the internal code change is a permanent working part of the licensed internal code of the object.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Accepted Level

This field displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the object.

Compare the number in this field with the number displayed for the **activated level** to determine whether a more recent change level has been activated:

- If the activated level is higher than the accepted level, then a more recent change level is currently activated, but it is not yet a permanent working part of the licensed internal code of the object.
- If the accepted level is equal to the activated level, then the change level currently activated is a permanent working part of the licensed internal code of the object.

  Note: Check the **retrieved level** and **installed level** to determine whether the object is operating with your latest available level of the internal code change.

Note: The term *object* is the target of a task and can be either:

- The Hardware Management Console when you perform a console task.
- Each system selected when you start a system task.

Internal Code Change Details

This window displays details for an internal code change.

Attention: A service representative will provide new internal code changes and manage their initial use.

For internal code changes already retrieved, you should manage these changes only under the supervision of a service representative or with the assistance of the support system.

Selected Internal Code Change Item

Part number
Displays the part number of the internal code change.

Engineering change number
Displays the engineering change (EC) number of the internal code change.

Engineering change type
Identifies the type of internal code affected by the internal code change.

Base ECs
Indicates the internal code change affects the base internal code of the system.

National language EC
Indicates the internal code change affects the internal code for a specific national language.

Other optional EC
Indicates the internal code change affects internal code other than base or national language internal code.

Engineering change description
Displays a brief description of the internal code change.

Internal Code Change State Details

Type
Identifies the internal code change states of an internal code change.

Level
Displays the change level of the selected internal code change in the state.

Date
Displays the date the change level was put in the state.

Time
Displays the time the change level was put in the state.

Additional functions are available from this window:

OK
To close this window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

System Information Error

An error occurred when attempting to retrieve the system information for the objects listed below.

Use this window to view system information retrieval error details.

Select an object, click **Error Details...** to view the cause for this error.

OK
To close this window, click **OK**.

Error Details...
To view the cause for the selected error, click **Error Details...**.

Help
To display help for the current window, click **Help**.

View Console Service History

Accessing the Perform Problem Analysis task

This task manually calls Problem Analysis, which analyzes stored data that is collected from various parts of a processor at the time of an error and determines the type of problem. Problem Analysis then informs the user of the steps that are necessary to resolve the problem.

Problems that are considered to be *hard* errors start Problem Analysis automatically. An example of a hard error is a processor card failure. Results from automatic Problem Analysis are stored under **Hardware Messages**.

The icon of the CPC that had the hard error and the icon of any group that contains the CPC icon will have a blue background indicating that Problem Analysis results were reported for that CPC.

Problems that can be considered to be *soft* errors require the operator to start Problem Analysis manually, usually after the operating system reports a problem. An example of a soft error is an interface control check (IFCC).

To perform a manual problem analysis:

1. Select one or more CPCs (servers).
2. Open the **Perform Problem Analysis** task. The Problem Analysis window is displayed. This window displays the last 50 IFCCs that occurred.
3. You can select a specific problem, then click **View Selected Errors...**. The Problem Analysis window is displayed listing a description of the errors for the problem you previously selected.
4. You can continue to analyze the problems or click **Cancel** to return to the previous window.

Accessing the View Service History task

This task displays a list of current problems for selected CPCs or a selected group of CPCs. The problems may be opened or closed and will be displayed with the most recent entry at the top of the list.

To display the service history:

1. Select one or more CPCs (servers).
2. Open the **View Service History** task. The Service History window is displayed.
3. From the menu bar you can:
   - Select **View** for the following choices:

     Problem Summary
     Displays detailed information about the selected problem including machine type, model, and serial number information.

     Problem Analysis Panels
     Redisplays the Problem Analysis (PA) windows that were created when the selected problem was originally reported.

     Repair Information
     Displays repair information for the selected problem.

     Exit
     Ends the task.
   - Select **Close** for the following choices:

     Selected Problem
     Changes the current status of the selected problem to closed.

     All Problems
     Changes the current status of all open problems to closed.
   - Select **Sort** for the following choices:

By Date
Lists problems in the order of the dates on which problems occurred, starting with the most recent problem.

By System Name
Lists problems by the alphabetical order of the names of the objects on which they occurred.

By Status
Lists all open problems, followed by all closed problems.

- Select **Help** to display additional task information.

4. When you have completed this task, select **View**, **Exit** to return to the Hardware Management Console workplace.

Accessing the View Console Service History task

This task displays the service history log for the Hardware Management Console. The service history is a record of problems occurring on the Hardware Management Console. Service history information is recorded by *Problem Analysis* that starts automatically and identifies the source of a Hardware Management Console problem. Service history entries are displayed with the most recent entry at the top of the record.

To view the console service history:

1. Open the **View Console Service History** task. The View Console Service History window is displayed.
2. A table is displayed that lists the problems. Select a problem, then use the options from the menu bar for additional information or sorting preferences.
3. Click **View**, **Exit** from the menu bar when you have completed this task.

Service History

Use this window to review or close problems discovered by Problem Analysis, or reported using Problem Analysis, for one or more objects.

A problem is *opened* when either:

- Problem Analysis determines service is required to correct a problem detected by the object
- A console operator uses the **Report a Problem** task to report a suspected problem not detected by the object.

Each record of a problem includes detailed information about the problem, and indicates whether the service required to correct the problem is still pending (an *opened* problem), or is already completed or no longer needed (a *closed* problem).

Collectively, the problem and service records are referred to as the *service history* of the object. Upon viewing the object's service history, you can:

- Redisplay the Problem Analysis windows that were displayed when a problem was originally reported.
- Display detailed information about a problem.
- Manually close open problems.

Click **View** on the menu bar, then select the following:

- **Problem Summary...** to display additional information that further describes the selected problem and the object it occurred on, and lists actions performed to diagnose and correct the problem.
- **Problem Analysis Panels...** to display Problem Analysis panels that were shown to report the selected problem when it occurred.
- **Repair Information...** to display the repair information for the selected problem.
- **Exit** to end this task and return to the console workplace.

Click **Close** on the menu bar, then select the following:

- **Selected Problem** to change the status of selected *open* problems to *closed*.

- **All Problems** to change the status of all *open* problems to *closed*.

Click **Sort** on the menu bar, then select the following:

- **By Date** to list problems in order of the dates on which they occurred, from the most recent problem to the oldest problem.
- **By System Name** to list problems in alphabetical order of the names of the objects on which they occurred.
- **By Status** to list all *open* problems, followed by all *closed* problems.

Click **Help** to display help for the current window.

Service History table

This list displays the most recent problems that were automatically detected by Problem Analysis, or reported manually using Problem Analysis, for all selected objects.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

System name
Displays the name of the object on which the problem occurred.

Problem Number
Displays the number assigned by Problem Analysis and used to identify and track the problem.

Status
Indicates whether the problem is *open* or *closed*.

Description
Displays a brief explanation of the problem.

Service History Problem State

This window displays information that identifies an object, describes a specific problem that occurred on it, and lists actions performed to diagnose and correct the problem.

System name
Displays the name of the object on which the problem occurred.

Machine type
Displays the machine type of the object.

Machine model
Displays the model number of the object.

Machine serial number
Displays the serial number of the object.

Problem management hardware (PMH) number
Displays the number assigned to the problem by the support system.

Problem number
Displays the number assigned to the problem by Problem Analysis.

Problem type
Identifies the type of problem reported to the support system by Problem Analysis, and indicates the type of service required to correct it.

Problem data
Displays additional information provided by Problem Analysis specifically for this problem.

The information may be part numbers of parts needed to repair the problem, or reference codes needed to perform additional problem determination.

Problem State table

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

“Problem States” on page 1494
Displays the problem state of the object on which the problem occurred.

Problem States

Descriptions of the problem states or their effects on the problem:

Additional problem information
Indicates a service representative, while performing a repair procedure, manually edited the service history log to further describe the problem or its repair.

Continued in printed information
Indicates a repair procedure instructed a service representative to continue the repair using a printed repair procedure.

Customer notified
Indicates Problem Analysis displayed a panel to report the problem.

Duplicate problem closed
Indicates Problem Analysis closed the problem because it was a duplicate of another open problem.

Inactive problem closed
Indicates Service History closed the problem because of inactivity.

Problem closed
Indicates Problem Analysis could no longer detect the problem after a service representative completed a repair procedure.

Problem closed by the user
Indicates the console operator used the Service History task to close the problem.

Problem detected
Indicates Problem Analysis detected the problem automatically.

Problem reopened
Indicates Problem Analysis detected the problem occurred again after it was repaired and closed.

Repair closed
Indicates a problem was closed when the repair was completed.

Repair ended
Indicates a service representative completed a repair procedure.

Repair resumed
Indicates a service representative started using a previously suspended repair procedure.

Repair started
Indicates a service representative began a repair procedure.

Repair suspended
Indicates a service representative temporarily stopped using a repair procedure before completing the repair.

Returned from printed information
Indicates a service representative resumed using a repair procedure to acknowledge completing a printed repair procedure.

Service authorization complete
Indicates Problem Analysis successfully transmitted problem information and requested service through a Remote Support Facility (RSF) connection to the support system.

Service authorization delayed
Indicates Problem Analysis reported the problem, but the console operator did not request service.

Service authorization failed
Indicates Problem Analysis could not successfully transmit problem information or request service through a Remote Support Facility (RSF) connection to the support system.

Service authorized electronically
Indicates Problem Analysis used the Remote Support Facility (RSF) to connect to the support system to transmit problem information and request service.

Service requested via telephone
Indicates Problem Analysis displayed problem information and instructed the console operator to call a service representative, describe the problem, and request service.

Additional functions are available from this window:

OK

To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Service History Part Replacement

This window displays part replacement information including part descriptions as well as how many parts were replaced.

Part Location
Displays the machine location of the object on which the problem occurred.

Part Number
Displays the actual part number of the object.

Serial Number
Displays the serial number of the object.

Fix description
The description from Service History of how to correct the problem.

OK

to return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem description)

This window displays the following information about a problem discovered by automatic Problem Analysis:

System name
Displays the name of the object on which the problem occurred.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

Depending on the information that was provided for a problem, the following information could also appear in this window:

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the Interface Control Code (IFCC) occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Use the following information to determine whether to request service, then take the appropriate action:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Impact of Repair
Describes what system resources will be affected.

Additional functions are available from this window:

Request Service...
To request service to correct the problem, click **Request Service...**.

I/O Trace...
To display Input/Output (I/O) trace information, click **I/O Trace...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Display Sense Data
To display additional specific problem failure information, click **Display Sense Data**.

Detail Problem Description...
To view a more detailed description of the problem, click **Detail Problem Description...**.

Delete
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Tag-in control lines

This field displays a two-digit, hexadecimal value that identifies the inbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-in is active.
- The value for a bit is 0 when its tag-in is not active.

Bit	Tag-In
0	Operational
1	Address
2	Status
3	Select
4	Request
5	Service or Data (see Note)
6	Data or Mark (see Note)
7	Disconnect

Note: The values for bits 5 and 6 indicate whether the following tags-in are active:

```
Bit 5    Bit 6          Data In       Service       Mark
-----    -----          -------       -------       ----
 1        1              On            Off           Off
 1        0              Off           On            Off
 0        1              Off           Off           On
 0        0              Off           Off           Off
```

For example, a tag-in value of 86 indicates that Operational In and Data In are both active.

Tag-out control lines

This field displays a two-digit, hexadecimal value that identifies the outbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-out is active.
- The value for a bit is 0 when its tag-out is not active.

Bit	Tag-In
0	Operational
1	Address
2	Select/Hold

Bit	Tag-In
3	Data streaming
4	Service
5	Data
6	Suppress
7	Command

For example, a tag-out value of 84 indicates that Operational Out and Data Out are both active.

Problem Analysis (sense data details)

This window displays sense data details and additional problem failure information.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (operation/outcome)

This window displays information about an automatic Problem Analysis operation on an object. The information identifies the operation and describes its outcome.

Review the information, then take the appropriate action.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information)

This window displays information about a problem discovered by automatic Problem Analysis.

Use the information provided to determine whether to request service, then take the appropriate action.

System name
Displays the name of the object that had the channel path configured on when the IFCC occurred.

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the IFCC occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Additional functions are available from this window:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Request Service...
To request service to correct the problem, click **Request Service...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (contact)

Use this window to identify a person that can be contacted about the problem, and to specify how to service will be requested.

Provide the following information, then click **Request Service...**:

Customer name
Specify the name of the person that can be contacted about the problem.

Customer phone
Specify the telephone number of the person that can be contacted about the problem.

Transmission Type
Select how to request service, through automatic transmission or manually by telephone.

Select a transmission type, then click **Request Service...**.

Electronic transmission
To automatically transmit the service request and problem information, select **Electronic transmission**.

Voice transmission
To manually request service and report problem information by telephone, select **Voice transmission**.

Note: The telephone number and problem information are provided on a subsequent window.

Additional functions are available from this window:

Request Service...
To authorize service for this problem and initiate the transmission type by electronic or by voice, select click **Request Service...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information/contact)

This window displays information about a problem discovered by automatic Problem Analysis. Use this information to request service and describe the problem.

1. Be ready to provide the problem information when you call.
2. Dial the telephone number to speak with a service representative.
3. Request service.
4. Provide the problem information to the service representative.

Request service when:

- Service is required.
- Service may be required, and you have verified all possible causes of the problem do not exist.

It is recommended you do not request service when:

- Service is not required.
- Service may be required, but you have verified one or more possible causes of the problem exist, and you will attempt to correct the problem.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (action to take)

This window displays information about a problem discovered by automatic Problem Analysis.

Review the information, then take the appropriate action.

Problem Data
Provides specific information about the selected problem.

Parts List

- Part Location - the physical location of the part.
- Part Number - the number of the part.
- Fix Percentage - the percentage of accuracy for correcting the problem.
- Serial Number - the serial number of the part.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (channel path errors)

This window displays the unreported errors that occurred on a specific channel path of a Central Processor Complex (CPC).

Use this window to select an error when you want to display detailed information from Problem Analysis that describes the error.

Select one error from the list, then click **Analyze Error...** to display details about the error.

System name
Displays the name of the CPC that had the channel path configured on when the error occurred.

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Interface location
Identifies the physical location of the channel card and port that supports the channel path on which the error occurred.

Additional functions are available from this window:

Error table

Date
Displays the date the error occurred.

Time
Displays the time the error occurred.

Description
Displays a brief description of the error.

Analyze Error...
Select an error from the list, then click **Analyze Error...** to display details about the selected error.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (unreported errors)

This window summarizes the unreported errors that occurred on the selected Central Processor Complexes (CPCs). The summary identifies the problem areas where errors occurred, and displays the number of errors that occurred in each area.

Use this window to select a problem area when you want to display more information about the unreported errors that occurred in the area.

Problem areas for a CPC include the processors and its channels paths.

An unreported error is an error that is analyzed, but is not reported by Problem Analysis. Errors are not reported when automatic recovery operations succeed, and when service is not needed for the CPC to continue operating.

Select a problem area for a CPC from the list, then click **View Selected Errors...** to display a summary of unreported errors that occurred in that area.

Beginning time
Displays the time and date when the least recent unreported error occurred.

All unreported errors occurred at or after this time.

Ending time
Displays the time and date when the most recent unreported error occurred.

All unreported errors occurred before or at this time.

Error table

System Name
Displays the name of the CPC where the unreported errors occurred.

Problem Area
Indicates whether the unreported errors occurred on a processor in the CPC, or on a particular channel path.

Number of Errors
Indicates the number of unreported errors that occurred in the problem area during the time range.

View All Errors...
To view details about all errors shown in the list, click **View All Errors...**.

View Selected Errors...
To view details about one error in the list, click **View Selected Errors...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

View Console Tasks Performed

Accessing the View Console Tasks Performed task

This task allows the support system to review the tasks that have been performed on a Hardware Management Console. This can be very helpful when working with an operator to determine what happened if a problem occurs.

To view the console tasks performed:

1. Open the **View Console Tasks Performed** task. The View Console Tasks Performed window is displayed.
2. A table of information that includes the last 2000 tasks performed on the Hardware Management Console is displayed. The table includes the task name, user ID that accessed the task, and the user interface style that was used.
3. Click **OK** when you are done viewing the information.

View Frame Layout

Accessing the View Frame Layout task

This task provides a graphic view of the physical location of the hardware objects that are defined to this Hardware Management Console. Each object is shown with its frame designation and position within the frame. By opening (double-clicking on) the object, additional information is provided:

- Machine type
- Model
- Serial number
- Device location

Objects can be added, removed, or moved by a user with service representative roles using the **Edit Frame Layout** task.

To view the physical location of hardware objects that are defined to the Hardware Management Console:

1. Select a CPC (server).
2. Open the **View Frame Layout** task. The View Frame Layout window is displayed.

   Note: If you select more than one object, the Object Selection window is displayed prompting you to select a single CPC on which to perform the task.
3. Click **OK** when you are done viewing the frame layout.

View Frame Layout

This window graphically displays the physical location of the hardware objects that are defined to this Hardware Management Console. Each object is shown with its frame designation and position within the frame.

Additional information includes:

- Machine type
- Model
- Serial number
- Device location

Use the mouse to select graphics and to display pop-up menus of views you can use on the selected graphic. The possible menu choices available for viewing include:

- Device details
- Support element details

If you are assigned a user ID with service representative task roles, you can add, remove, or move objects by using the **Edit Frame Layout** task.

Additional functions are available from this window:

OK
To close the window, click **Cancel**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Device/CPC Details

Use this window to view device/CPC details. Detailed hardware configuration information for a selected device is displayed.

To change the device details, specify the device serial number and select the associated CPC, then click **Change Device Details**.

Device
Displays the name or type of the device.

Description
Displays a brief description of the device.

Location
Identifies the location of the device.

Serial number
Displays the serial number of the device.

Associated CPC
Displays the name and location of the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the support elements of its CPCs. A Support Element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

OK

When you are done reviewing the information in this window, click **OK**.

Help
To display help for the current window, click **Help**.

Support Element Details

Use this window to confirm the Support Elements listed by description, serial number, and location and associated with a specific CPC.

This is the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the Support Elements of its CPCs. A support element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

To confirm the Support Elements, click **OK**.

OK
When you are done reviewing the information in this window, click **OK**.

Help
To display help for the current window, click **Help**.

View Internal Code Changes Summary

Accessing View Internal Code Changes Summary task

To view a summary of internal code changes, open the **View Internal Code Changes Summary** task. The View Internal Code Change Summary window is displayed.

View Internal Code Changes Summary

You can use this task to view a summary of internal code changes pending conditions that would otherwise require running the separate tasks to obtain the information. The following areas indicate whether a pending condition displays and a link to the specific task:

Close
To close this window and exit this task, click **Close**.

Refresh
To update the displayed internal code change summary information with the information, click **Refresh**.

Help
To display help for the current window, click **Help**.

View Licenses

Accessing the View Licenses task

This task allows you to view the Licensed Internal Code (LIC) that you have agreed to for this Hardware Management Console.

To view the licenses:

1. Open the **View Licenses** task. The View Licenses window is displayed.
2. A list of the licenses is displayed, click on any of the license links for more information.

   Note: This list does not include programs and code provided under separate license agreements.
3. Click **OK** when you are done viewing this information.

View LPAR Cryptographic Controls

Accessing the View LPAR Cryptographic Controls task

You can use this task to review information about the active logical partitions that use the Crypto Express features assigned to them. You can review:

- A summary tab page of information on all active logical partitions.
- Individual tab pages for each logical partition's cryptographic controls.

To review the logical partition's cryptographic controls:

1. Open the **View LPAR Cryptographic Controls** task.

   The View LPAR Cryptographic Controls window displays. The window includes a summarized view tab for cryptos on all partitions and individual tabs for each logical partition's cryptographic controls.
2. Click **OK** when you have finished.

View LPAR Cryptographic Controls

Use the **View LPAR Cryptographic Controls** task to review the cryptographic candidate list and usage domain index assignments for the logical partitions that use the Crypto Express feature.

Click the tab along the right hand side of the window to display:

- A summary page of cryptographic candidate list and usage domain index assignments for all logical partitions.
- An individual page for each active logical partition that describes the assignment of the control domain index, the usage domain index, the cryptographic candidate list, and the cryptographic online list from the activation profile.

Additional functions on this window include:

Close
To close the window, and return to the window from which you selected the task, click **Close**.

Refresh
To update the current window with the new changes, click **Refresh**.

Help
To display help for the current window, click **Help**.

Conflicts

This window displays a list of the inactive partitions that will create conflicts with activated partitions if they become activated. The inactive partitions listed could be in conflict with other inactive partitions in the list if they become activated.

Crypto numbers in conflict
Displays the inactive crypto numbers that will create conflicts with the activated partitions.

Usage domains in conflict
Displays the inactive usage domain numbers that will create conflicts with the activated partitions.

Close
To exit the current window, click **Close**

Help
To display help for the current window, click **Help**.

Summary page

The summary page displays the installed cryptos and cryptographic settings for all logical partitions. The cryptographic settings on the summary page include the cryptographic candidate list and usage domain index assignments. For active partitions, the cryptographic settings currently in effect are displayed. For inactive partitions, the cryptographic settings in the activation profile are displayed. Select the “Conflicts” on page 1506 link to display the inactive partitions that will be in conflict when activated with existing activated partitions.

You can work with the table by using the table icon or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Individual pages

Each page of the View LPAR Cryptographic Controls displays the cryptographic settings for an active logical partition. The page tab displays the active logical partition's name.

The cryptographic controls on each page indicate the current settings of each active logical partition's cryptographic controls. You can find more detailed help on the following elements of this window:

Control domain index

Displays the cryptographic domain number the active logical partition uses for remote secure administration functions.

A logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), there is at least one control domain and matching usage domain. Refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Usage domain index

Displays the usage domain number the active logical partition uses for Public Key Algorithm (PKA) and cryptographic functions.

If you are using the Integrated Cryptographic Service Facility (ICSF), there is at least one control domain and matching usage domain. Refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Cryptographic candidate list

The candidate list identifies which coprocessors will be assigned to the partition at the next activation. For each selected coprocessor in the candidate list, there is a corresponding coprocessor selected in the online list.

Cryptographic online list

The online list identifies which coprocessors will be configured online at the next activation of the logical partition, as specified in the activation profile. For each selected coprocessor in the online list, there is a corresponding coprocessor selected in the candidate list.

You must activate the partition to bring the coprocessors or accelerators online.

View Partition Resource Assignments

Accessing the View Partition Resource Assignments task

You can use the console to view the mapping of active logical partitions and associated processor information.

Note: Use this task under the direction of product support.

To view the resource assignments for partitions:

1. Select a system.
2. Open the **View Partition Resource Assignments** task. The View Partition Resource Assignments window displays.
3. The window displays the active logical partitions and physical processors associated with each active logical partition.

View Partition Resource Assignments

Use this task, under the direction of product support, to view the mapping of active logical partitions and associated processor information.

You can work with the table by using the table icons or **Actions** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar:

Spare 

Select this icon toggle to display or hide shared, unassigned, and spare physical processor assignments.

Note: If you selected an IBM z13 or IBM z14 system then only the spare physical processor assignments are displayed or hidden.

Pause/Resume  /
image icon of pause and resume button

Select these icons to dynamically pause or resume the current view of the logical partition resource assignments.

Export 

Select this option from the **Actions** list or click **Export** icon.

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print 

Select this option from the **Actions** list or click **Print** icon.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Expand All
Expands the Node and Chip view and displays physical processor type details for each Chip assigned to the active logical partitions. The core ID is identified with each Chip.

Collapse All
Collapses the Node and Chip details view for the active logical partitions. Displays the Chip summary view of processor types assigned to the active logical partitions. This is the default.

Partition Resource Assignment table

Use the Partition Resource Assignment table, under the direction of product support, to view processor allocations to partitions in your system. The active logical partitions are identified at the top of the table. The Node and Chip numbers associated with each active logical partition are identified on the left. You can view the Node and Chips assignments using the **Expand All** and **Collapse All** icons to view or hide sections.

To view the resource assignments for partitions:

Logical partition name

Displays the active logical partition and if Hyperdispatch (HD) is enabled.

Node

Displays the processor Node number in your system.

Chip

Displays the processor Chip number associated with the Node and lists the processor types associated with each active logical partitions. The Chip **Collapse All** icon displays a summary view. The following physical processor types are:

- General processors (G)
- Coupling facility processors (C)
- Integrated Facilities for Linux (IFLs) (I).
- z Integrated Information Processors (zIIPs) (Z).
- Integrated Firmware Processor (IFPs) (F

The physical processor types may have some of the following conditions:

- Indicates the physical processor types are shared (SH).
- Indicates the physical processor is dedicated (D).
- Indicates the vertical polarity for the physical processor types (H/M/L).

Additional functions on this window include:

Close

To exit the current window, click **Close**.

Help

To display help for the current window, click **Help**.

View PMV Records

Accessing the View PMV Records task

To view a PMV record:

1. Open the **View PMV Record**s task for the console or after selecting one or more CPCs (servers). The View PMV Records window is displayed.
2. Click **Yes** to retrieve a list of the most recent records, otherwise click **No** to get a list of records without the latest updates. The View PMV Records message window is displayed. It indicates the PMV records that are being retrieved from the support system. This process can take a long time. You can click **Cancel** to stop the process and exit the task at any time.
3. When the records have been retrieved, the View PMV Records window displays a listing of the PMV records and corresponding machine.
4. Select a PMV record to view, click **OK**. A message is displayed indicating the retrieval of the PMV record. The View PMV Records window is displayed. From this window the following options are available:
   - To add a comment to the PMV record, click **Add Comment**. The View PMV Records window is displayed with a text input area. Provide a comment in the text input area and click **OK**.
   - To refresh the details of the PMV record, click **Refresh**. The PMV record displays the most current information.
   - To supply a screen capture of the problem in the PMV record, click **Add Attachment**.
   - To view existing screen captures (files) available for download, click **Download Attachments**.

- To view the attachments associated with this PMV record, click **View Attachments**.
- To return to the list of PMV records, click **Close**.

5. To stop processing an action on a PMV record or to exit the task, click **Cancel** at any time.

View PMV Records

Use this task to obtain Problem Management Viewable (PMV) records issued to the support system for the Hardware Management Console or selected servers (CPCs). These problems are typically sent to the support system where errors are not recorded by the console. You are able to view and edit the PMV records on the console and you have the ability for an interactive dialog with a service representative. A PMV record is initially created from the **Report a Problem** task specifying a problem type of **Type V Viewable PMH(PMV)**.

Note: To cancel processing at any time during the retrieval of the PMV records, click **Cancel**. The processing can take some time.

You can work with the table by using the table icons or the **Select Action** list from the table toolbar. If you place your cursor over the icon, the icon description appears. The toolbar performs the following functions:

Edit Sort
The **Edit Sort** icon allows you to perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
The **Clear All Sorts** icon allows you to return to the default ordering.

Configure Columns
The **Configure Columns** icon allows to you arrange the columns in the table in the order you want or hide certain columns from view. All available columns are listed in the Columns list by their column name. Select the columns you want displayed or hidden by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified.

Following are descriptions for the columns displayed in the table:

Select
Use this column to make selections. No rows are selected when the table is first displayed. You can select any number of rows.

PMV
Specifies the PMV record number assigned from the support system.

Machine
Specifies the machine type and serial number the problem is written against.

Additional functions are available from this window:

OK
To display the details of the selected PMV record, click **OK**.

Cancel
To end the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

PMV Details

Use this window to view the information of the PMV records you selected.

Add Comment
To provide a comment or additional information about the PMV record, click **Add Comment**. A text input area is displayed where you can specify information about the PMV record.

Refresh
To display the most current details of the PMV record, click **Refresh**. The window displays the most current information PMV record.

Add Attachment
To add a screen capture of the problem to the PMV record, click **Add Attachment**. A list of screen captures you created using the "Manage Print Screen Files" on page 987 task are displayed. You can select one or more of these files and upload them to the PMV record, click **OK** to proceed or **Cancel** to return to the previous window.

Note: Once a file has been uploaded you cannot upload it again to the same PMV record unless it has a different file name.

Download Attachments
To view existing screen captures (files) available for download, click **Download Attachments**. A list of attachments is displayed that can be downloaded from the PMV record.

View Attachments
To view the attachments that are associated with this PMV record, click **View Attachments**. A list of the files that have been uploaded for the PMV record are displayed.

Close
To return to the list of PMV records, click **Close**.

Help
To display help for the current window, click **Help**.

Add Comment to PMV Record

Use this window to specify a comment or information pertaining to the PMV record in the input area.

OK
To submit your comment or information for the PVM record, click **OK**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Files to Upload

Use this window to upload one or more files. You can use the "Manage Print Screen Files" on page 987 task to create, manage, or view the files. The table displays the screen captures you created along with the assigned file name. Select one or more to upload to the PVM record.

OK
To upload the files selected, click **OK**.

Cancel
To return to the previous window and do not upload any files, click **Cancel**.

Help
To display help for the current window, click **Help**.

Download Attachments

Use this window to download attachments associated with the PMV record. Select one or more attachments, then click **OK** to proceed or click **Cancel** to return to the previous window.

OK
To download the attachment selected, click **OK**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

View Image

This window displays the files that are associated with this PMV record. Select a file to view, then click **OK** to proceed or click **Cancel** to return to the previous window.

OK
To view the selected attachment, click **OK**.

The file you selected to view is displayed. You can click **Close** to return to the previous window. If you are viewing a large print file, use the scroll bars on the right to navigate through the file.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

View Security Logs

Accessing the View Security Logs task

This task allows you to view the security events logged for the Hardware Management Console or a server (CPC). A security event occurs when an object's operational state, status, or settings change or involves user access to tasks, actions, and objects.

To view a security log:

1. Open the **View Security Logs** task. The View Security Logs window is displayed.
2. From the menu bar you have the following options for viewing information:
   - To open security logs, click **File**, then one of the following options:
     - To open an archived security log from a USB flash memory drive (whose capacity is 1 GB or greater) or an FTP server, select **Open Security Log**, **New**.
     - To open the Hardware Management Console's default security log, select **Open Security Log**, **Default**).
     - To close the window and end the task, select **Exit**.
   - To search the security log that is currently open, click **Search By**, then one of the following options:
     - To search events by the time and date they occurred, select **Date**.
     - To search for an event by its description, select **Event**.
     - To search for events by a certain group, select **Category**.
     - To search for events by user ID, select **User**.
   - To view or alter the security log options, click **Options**, then one of the following options:
     - To enable the creation of a hardware message when the security log is approaching the maximum size, select **Create hardware message when approaching maximum**, **On**.
     - To disable the creation of a hardware message when the security log is approaching the maximum size, select **Create hardware message when approaching maximum**, **Off**.
     - To enable the creation of a security log event when the underlying network firewall denies a network connection, select **Log security event for network denial events**, **On**.
     - To disable the creation of a security log event when the underlying network firewall denies a network connection, select **Log security event for network denial events**, **Off**.
   - To display help for the current window, click **Help**.
3. When you are done viewing the security log and ready to exit the task, click **File**, **Exit**.

View Security Logs

Use this task to view the:

- Console's default security log
- Archived security logs.

The console automatically keeps a *default security log* of security events that occur while the console application is running. A *security event* occurs when a task is performed that either:

- Changes an object's operational state, status, or settings. For example, activating a CPC, customizing an activation profile, and loading a CPC image.
- Or involves user access to console tasks, actions, and objects. For example, logging on and off, changing a user profile, and defining an undefined CPC.

On the menu bar:

- Click **File** to open security logs, then select the following:
  - **Open Security Log, New** to open an archived security log from a USB flash memory drive or from an FTP server. The Retrieve from Removable Media or FTP Server window is displayed.

    Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.
  - **Open Security Log, Default** to open the console's default security log (the log in which it currently logs security events).
  - **Exit** to close the window and end the task.
- Click **Search By** to search the security log that is currently open, then select the following:
  - Date to search for events by the time and date they occurred.
  - Event to search for an event by its description.
  - Category to search for events by a certain category.
  - User to search for events by a user ID.
- Click **Options** to view or alter the security log options, then select the following:
  - **Create hardware message when approaching maximum size, On** to enable the creation of a hardware message when the security log is approaching the maximum size.
  - **Create hardware message when approaching maximum size, Off** to disable the creation of a hardware message when the security log is approaching the maximum size.
  - **Log security event for network denial events, On** to enable the creation of a security log event when the underlying network firewall denies a network connection.
  - **Log security event for network denial events, Off** to disable the creation of a security log event when the underlying network firewall denies a network connection.
- Click **Help** to display help for the current window.

Security Logs table

When you open a security log, the window lists the most recent (latest) security events. The events are listed in order of occurrence (from the most recent event to the oldest event). Only a subset of the events is listed; click **Show Earlier Events** or **Show Later Events** to navigate to other subsets of events.

User
Displays the user ID from which the security event occurred.

Date
Displays the date and time the event occurred.

Security Event
Displays a description of the event.

Additional information is available for events marked with an asterisk (*). Click **Details...** to display the information.

Additionally, you can perform the following actions from the table:

Details...
To display additional information about a selected event, click **Details...**. The Security Log Details window is displayed. To close the window, click **OK**.

Authentication Data...
To display authentication data for the selected event, click **Authentication Data...**. The Authentication Data window is displayed. To close the window, click **OK**.

Show Earlier Events
To display events that occurred *before* the events currently displayed (use it to navigate to older events in the security log), click **Show Earlier Events**.

Note: This option is available only when earlier events are available. Otherwise, it is unavailable.

Show Later Events
To display events that occurred *after* the events currently displayed (use it to navigate to more recent events in the security log), click **Show Later Events**.

Note: This option is available only when later events are available. Otherwise, it is unavailable.

Retrieve from Removable Media or FTP Server

Use this window to open a security log from a USB flash memory drive or from an FTP server.

Hardware Management Console USB flash memory drive
To retrieve a security log from a Hardware Management Console USB flash memory drive, select **Hardware Management Console USB flash memory drive**. A table is displayed which includes the available USB flash memory drives. To make sure you have the available USB flash memory drive, click **Refresh**.

Note: If you're using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP Server
To retrieve a security log from an FTP server, select **FTP Server**. The following input areas are displayed.

Host name:
Specify the host name address or destination. This is a required field.

User name:
Specify the user name for the target FTP destination. This is a required field.

Password:
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol:

Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)
- **SFTP** (SSH File Transfer Protocol)

File path
When you have selected either a USB flash memory drive or an FTP server the security log is to be saved to, you must provide the path name in the input area or click **Browse**. Once you make your directory selection it is displayed in the input area.

If you do not provide a file path for a USB flash memory drive, then the default is to the media mount point. If you do not provide a file path for an FTP selection, then the default is to the home directory of the FTP server.

Note: The file path has a maximum length of 2048 characters.

OK
To proceed with your selection, click **OK**.

Cancel
To exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Search by Date

Use this window to set a time and date for locating events in the security log that are currently open:

1. Use the **Desired Time** field to set the time. Specify the hours, minutes, and seconds (hh:mm:ss.SSS). Initially, the current time appears in this field.
2. Use the **Desired Date** field to set the date. Specify the month, day, and year (mm/dd/yyyy). Initially, the current date appears in this field.
3. Click **Find Event** to begin the search.

The search begins with the first event in the log and proceeds in order of event occurrence (from the most recent event to the oldest event).

Upon locating events that occurred at or before the specified desired time and date, the **View Security Logs** window is displayed again with the events listed in order of occurrence.

Additionally, the Search by Date window includes the following:

Newest Time
Specifies the time of the most recent security log in the list.

Oldest Time
Specifies the time of the oldest security log in the list.

Newest Date
Specifies the date of the most recent security log in the list.

Oldest Date
Specifies the date of the oldest security log in the list.

Cancel
Exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Search by Event

Use this window to select an event description to search for in the security log currently open:

1. Select an event description from the list.
2. Click **OK** to display the list of security logs matching the selected event type.

   The view security logs window is displayed again with the matching events.

   Note: The **Find Earlier Event** and **Find Later Event** options are disabled if there are fewer than 500 events.

Event description list
This list displays the security log event descriptions that you can select. When an event is selected (highlighted), click **Find Earlier Event** or **Find Later Event** to search for the next event. The sorting of the events depends on which option you selected.

Find Earlier Event
To search the security log for an event that is older than the currently displayed events, click **Find Earlier Event**.

Find Later Event
To search the security log for an event that is more recent than the currently displayed events, click **Find Later Event**.

Full Text
To view the entire event description, select the event, then click **Full Text**.

The **Full Text of Security Event** window is displayed, click **OK** when you are done viewing the window.

Cancel
To exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Search By Event Categories

Use this window to select the subset of security events (defined by the appropriate category) you want to view.

OK
After selecting a category, click **OK** to view the security logs that pertain to that category.

Cancel
To exit this window, click **Cancel**.

Category Content
To determine which events are in a selected category, click **Category Content**.

The **Category Content** window is displayed, click **OK** when you are done viewing this window.

Help
To display help for the current window, click **Help**.

Search by User Name

Use this window to provide a user ID that is associated with the events you want to view.

User
Specify a user name in the text input area.

OK
To proceed with the user ID you have entered, click **OK**.

Cancel
To return to the previous window without searching for a specified user ID, click **Cancel**.

Help
To display help for the current window, click **Help**.

View Service History

Accessing the Perform Problem Analysis task

This task manually calls Problem Analysis, which analyzes stored data that is collected from various parts of a processor at the time of an error and determines the type of problem. Problem Analysis then informs the user of the steps that are necessary to resolve the problem.

Problems that are considered to be *hard* errors start Problem Analysis automatically. An example of a hard error is a processor card failure. Results from automatic Problem Analysis are stored under **Hardware Messages**.

The icon of the CPC that had the hard error and the icon of any group that contains the CPC icon will have a blue background indicating that Problem Analysis results were reported for that CPC.

Problems that can be considered to be *soft* errors require the operator to start Problem Analysis manually, usually after the operating system reports a problem. An example of a soft error is an interface control check (IFCC).

To perform a manual problem analysis:

1. Select one or more CPCs (servers).
2. Open the **Perform Problem Analysis** task. The Problem Analysis window is displayed. This window displays the last 50 IFCCs that occurred.
3. You can select a specific problem, then click **View Selected Errors...**. The Problem Analysis window is displayed listing a description of the errors for the problem you previously selected.
4. You can continue to analyze the problems or click **Cancel** to return to the previous window.

Accessing the View Service History task

This task displays a list of current problems for selected CPCs or a selected group of CPCs. The problems may be opened or closed and will be displayed with the most recent entry at the top of the list.

To display the service history:

1. Select one or more CPCs (servers).
2. Open the **View Service History** task. The Service History window is displayed.
3. From the menu bar you can:
   - Select **View** for the following choices:

     Problem Summary
     Displays detailed information about the selected problem including machine type, model, and serial number information.

     Problem Analysis Panels
     Redisplays the Problem Analysis (PA) windows that were created when the selected problem was originally reported.

     Repair Information
     Displays repair information for the selected problem.

     Exit
     Ends the task.
   - Select **Close** for the following choices:

     Selected Problem
     Changes the current status of the selected problem to closed.

     All Problems
     Changes the current status of all open problems to closed.
   - Select **Sort** for the following choices:

     By Date
     Lists problems in the order of the dates on which problems occurred, starting with the most recent problem.

     By System Name
     Lists problems by the alphabetical order of the names of the objects on which they occurred.

     By Status
     Lists all open problems, followed by all closed problems.
   - Select **Help** to display additional task information.
4. When you have completed this task, select **View**, **Exit** to return to the Hardware Management Console workplace.

Accessing the View Console Service History task

This task displays the service history log for the Hardware Management Console. The service history is a record of problems occurring on the Hardware Management Console. Service history information is recorded by *Problem Analysis* that starts automatically and identifies the source of a Hardware Management Console problem. Service history entries are displayed with the most recent entry at the top of the record.

To view the console service history:

1. Open the **View Console Service History** task. The View Console Service History window is displayed.
2. A table is displayed that lists the problems. Select a problem, then use the options from the menu bar for additional information or sorting preferences.
3. Click **View**, **Exit** from the menu bar when you have completed this task.

Service History

Use this window to review or close problems discovered by Problem Analysis, or reported using Problem Analysis, for one or more objects.

A problem is *opened* when either:

- Problem Analysis determines service is required to correct a problem detected by the object
- A console operator uses the **Report a Problem** task to report a suspected problem not detected by the object.

Each record of a problem includes detailed information about the problem, and indicates whether the service required to correct the problem is still pending (an *opened* problem), or is already completed or no longer needed (a *closed* problem).

Collectively, the problem and service records are referred to as the *service history* of the object. Upon viewing the object's service history, you can:

- Redisplay the Problem Analysis windows that were displayed when a problem was originally reported.
- Display detailed information about a problem.
- Manually close open problems.

Click **View** on the menu bar, then select the following:

- **Problem Summary...** to display additional information that further describes the selected problem and the object it occurred on, and lists actions performed to diagnose and correct the problem.
- **Problem Analysis Panels...** to display Problem Analysis panels that were shown to report the selected problem when it occurred.
- **Repair Information...** to display the repair information for the selected problem.
- **Exit** to end this task and return to the console workplace.

Click **Close** on the menu bar, then select the following:

- **Selected Problem** to change the status of selected *open* problems to *closed*.
- **All Problems** to change the status of all *open* problems to *closed*.

Click **Sort** on the menu bar, then select the following:

- **By Date** to list problems in order of the dates on which they occurred, from the most recent problem to the oldest problem.
- **By System Name** to list problems in alphabetical order of the names of the objects on which they occurred.
- **By Status** to list all *open* problems, followed by all *closed* problems.

Click **Help** to display help for the current window.

Service History table

This list displays the most recent problems that were automatically detected by Problem Analysis, or reported manually using Problem Analysis, for all selected objects.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

System name
Displays the name of the object on which the problem occurred.

Problem Number
Displays the number assigned by Problem Analysis and used to identify and track the problem.

Status
Indicates whether the problem is *open* or *closed*.

Description
Displays a brief explanation of the problem.

Service History Problem State

This window displays information that identifies an object, describes a specific problem that occurred on it, and lists actions performed to diagnose and correct the problem.

System name
Displays the name of the object on which the problem occurred.

Machine type
Displays the machine type of the object.

Machine model
Displays the model number of the object.

Machine serial number
Displays the serial number of the object.

Problem management hardware (PMH) number
Displays the number assigned to the problem by the support system.

Problem number
Displays the number assigned to the problem by Problem Analysis.

Problem type
Identifies the type of problem reported to the support system by Problem Analysis, and indicates the type of service required to correct it.

Problem data
Displays additional information provided by Problem Analysis specifically for this problem.

The information may be part numbers of parts needed to repair the problem, or reference codes needed to perform additional problem determination.

Problem State table

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

“Problem States” on page 1520
Displays the problem state of the object on which the problem occurred.

Problem States

Descriptions of the problem states or their effects on the problem:

Additional problem information
Indicates a service representative, while performing a repair procedure, manually edited the service history log to further describe the problem or its repair.

Continued in printed information
Indicates a repair procedure instructed a service representative to continue the repair using a printed repair procedure.

Customer notified
Indicates Problem Analysis displayed a panel to report the problem.

Duplicate problem closed
Indicates Problem Analysis closed the problem because it was a duplicate of another open problem.

Inactive problem closed
Indicates Service History closed the problem because of inactivity.

Problem closed
Indicates Problem Analysis could no longer detect the problem after a service representative completed a repair procedure.

Problem closed by the user
Indicates the console operator used the Service History task to close the problem.

Problem detected
Indicates Problem Analysis detected the problem automatically.

Problem reopened
Indicates Problem Analysis detected the problem occurred again after it was repaired and closed.

Repair closed
Indicates a problem was closed when the repair was completed.

Repair ended
Indicates a service representative completed a repair procedure.

Repair resumed
Indicates a service representative started using a previously suspended repair procedure.

Repair started
Indicates a service representative began a repair procedure.

Repair suspended
Indicates a service representative temporarily stopped using a repair procedure before completing the repair.

Returned from printed information
Indicates a service representative resumed using a repair procedure to acknowledge completing a printed repair procedure.

Service authorization complete
Indicates Problem Analysis successfully transmitted problem information and requested service through a Remote Support Facility (RSF) connection to the support system.

Service authorization delayed
Indicates Problem Analysis reported the problem, but the console operator did not request service.

Service authorization failed
Indicates Problem Analysis could not successfully transmit problem information or request service through a Remote Support Facility (RSF) connection to the support system.

Service authorized electronically
Indicates Problem Analysis used the Remote Support Facility (RSF) to connect to the support system to transmit problem information and request service.

Service requested via telephone
Indicates Problem Analysis displayed problem information and instructed the console operator to call a service representative, describe the problem, and request service.

Additional functions are available from this window:

OK

To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Service History Part Replacement

This window displays part replacement information including part descriptions as well as how many parts were replaced.

Part Location
Displays the machine location of the object on which the problem occurred.

Part Number
Displays the actual part number of the object.

Serial Number
Displays the serial number of the object.

Fix description
The description from Service History of how to correct the problem.

OK

to return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem description)

This window displays the following information about a problem discovered by automatic Problem Analysis:

System name
Displays the name of the object on which the problem occurred.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

Depending on the information that was provided for a problem, the following information could also appear in this window:

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the Interface Control Code (IFCC) occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Use the following information to determine whether to request service, then take the appropriate action:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Impact of Repair
Describes what system resources will be affected.

Additional functions are available from this window:

Request Service...
To request service to correct the problem, click **Request Service...**.

I/O Trace...
To display Input/Output (I/O) trace information, click **I/O Trace...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Display Sense Data
To display additional specific problem failure information, click **Display Sense Data**.

Detail Problem Description...
To view a more detailed description of the problem, click **Detail Problem Description...**.

Delete
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Tag-in control lines

This field displays a two-digit, hexadecimal value that identifies the inbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.

- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-in is active.
- The value for a bit is 0 when its tag-in is not active.

Bit	Tag-In
0	Operational
1	Address
2	Status
3	Select
4	Request
5	Service or Data (see Note)
6	Data or Mark (see Note)
7	Disconnect

Note: The values for bits 5 and 6 indicate whether the following tags-in are active:

```
Bit 5    Bit 6          Data In       Service       Mark
-----    -----          -------       -------       ----
 1        1              On            Off           Off
 1        0              Off           On            Off
 0        1              Off           Off           On
 0        0              Off           Off           Off
```

For example, a tag-in value of 86 indicates that Operational In and Data In are both active.

Tag-out control lines

This field displays a two-digit, hexadecimal value that identifies the outbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-out is active.
- The value for a bit is 0 when its tag-out is not active.

Bit	Tag-In
0	Operational
1	Address
2	Select/Hold
3	Data streaming
4	Service
5	Data
6	Suppress
7	Command

For example, a tag-out value of 84 indicates that Operational Out and Data Out are both active.

Problem Analysis (sense data details)

This window displays sense data details and additional problem failure information.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (operation/outcome)

This window displays information about an automatic Problem Analysis operation on an object. The information identifies the operation and describes its outcome.

Review the information, then take the appropriate action.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information)

This window displays information about a problem discovered by automatic Problem Analysis.

Use the information provided to determine whether to request service, then take the appropriate action.

System name
Displays the name of the object that had the channel path configured on when the IFCC occurred.

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the IFCC occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Additional functions are available from this window:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Request Service...
To request service to correct the problem, click **Request Service...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (contact)

Use this window to identify a person that can be contacted about the problem, and to specify how to service will be requested.

Provide the following information, then click **Request Service...**:

Customer name
Specify the name of the person that can be contacted about the problem.

Customer phone
Specify the telephone number of the person that can be contacted about the problem.

Transmission Type
Select how to request service, through automatic transmission or manually by telephone.

Select a transmission type, then click **Request Service...**.

Electronic transmission
To automatically transmit the service request and problem information, select **Electronic transmission**.

Voice transmission
To manually request service and report problem information by telephone, select **Voice transmission**.

Note: The telephone number and problem information are provided on a subsequent window.

Additional functions are available from this window:

Request Service...
To authorize service for this problem and initiate the transmission type by electronic or by voice, select click **Request Service...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information/contact)

This window displays information about a problem discovered by automatic Problem Analysis. Use this information to request service and describe the problem.

1. Be ready to provide the problem information when you call.
2. Dial the telephone number to speak with a service representative.
3. Request service.
4. Provide the problem information to the service representative.

Request service when:

- Service is required.
- Service may be required, and you have verified all possible causes of the problem do not exist.

It is recommended you do not request service when:

- Service is not required.
- Service may be required, but you have verified one or more possible causes of the problem exist, and you will attempt to correct the problem.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (action to take)

This window displays information about a problem discovered by automatic Problem Analysis.

Review the information, then take the appropriate action.

Problem Data
Provides specific information about the selected problem.

Parts List

- Part Location - the physical location of the part.
- Part Number - the number of the part.
- Fix Percentage - the percentage of accuracy for correcting the problem.
- Serial Number - the serial number of the part.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (channel path errors)

This window displays the unreported errors that occurred on a specific channel path of a Central Processor Complex (CPC).

Use this window to select an error when you want to display detailed information from Problem Analysis that describes the error.

Select one error from the list, then click **Analyze Error...** to display details about the error.

System name
Displays the name of the CPC that had the channel path configured on when the error occurred.

Channel path
Displays the identifier of the channel path on which the error occurred.

Depending on your machine type and model, this is one of the following:

- A two-digit channel path identifier (CHPID), for example: 90, 91, or 92
- A four-digit physical channel identifier (PCHID), for example: 0131, 0132, or 0133.

Interface location
Identifies the physical location of the channel card and port that supports the channel path on which the error occurred.

Additional functions are available from this window:

Error table

Date
Displays the date the error occurred.

Time
Displays the time the error occurred.

Description
Displays a brief description of the error.

Analyze Error...
Select an error from the list, then click **Analyze Error...** to display details about the selected error.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (unreported errors)

This window summarizes the unreported errors that occurred on the selected Central Processor Complexes (CPCs). The summary identifies the problem areas where errors occurred, and displays the number of errors that occurred in each area.

Use this window to select a problem area when you want to display more information about the unreported errors that occurred in the area.

Problem areas for a CPC include the processors and its channels paths.

An unreported error is an error that is analyzed, but is not reported by Problem Analysis. Errors are not reported when automatic recovery operations succeed, and when service is not needed for the CPC to continue operating.

Select a problem area for a CPC from the list, then click **View Selected Errors...** to display a summary of unreported errors that occurred in that area.

Beginning time
Displays the time and date when the least recent unreported error occurred.

All unreported errors occurred at or after this time.

Ending time
Displays the time and date when the most recent unreported error occurred.

All unreported errors occurred before or at this time.

Error table

System Name
Displays the name of the CPC where the unreported errors occurred.

Problem Area
Indicates whether the unreported errors occurred on a processor in the CPC, or on a particular channel path.

Number of Errors
Indicates the number of unreported errors that occurred in the problem area during the time range.

View All Errors...
To view details about all errors shown in the list, click **View All Errors...**.

View Selected Errors...
To view details about one error in the list, click **View Selected Errors...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Virtual Support Element Management

Accessing the Virtual Support Element Management task

This task allows you to manage the graphical console of the Support Element from the Hardware Management Console.

To manage the Virtual Support Element Management task:

1. Open the **Virtual Support Element Management** task. The Virtual Support Element Management window is displayed.
2. Select the type of Support Element to install, then click **Start SE Virtual Machine**.

   Note: If a virtual Support Element is currently running, you will need to stop the virtual Support Element prior to installing.
3. To display a new Support Element console window, click **Show SE Console**.

Virtual Support Element Management

You can use this window to view information on the selected virtual Support Element, start or stop the virtual Support Element, or install the virtual Support Element.

Support Element Information
Displays information on the targeted virtual Support Element.

Status
Displays the status of the virtual Support Element: Running or Shutdown

Name
Displays the targeted virtual Support Element

Type
Displays the type of Support Element that is hosted: Primary, Alternate, or Unavailable if not known.

Peer HMC

Displays the name of the peer HMC if known or Unavailable if not known.

Start/Stop Support Element Virtual Machine
To start or stop the virtual Support Element, click **Start SE Virtual Machine** or **Stop SE Virtual Machine**.

Support Element Console
To launch the virtual Support Element window, click **Show SE Console**.

Install Support Element
To install a virtual Support Element locally (not available remotely), select the media type, then click **Install SE**.

Note: If the virtual Support Element status indicates running, you will need to stop the virtual Support Element to perform an install.

- USB

  Note: To install a virtual Support Element, USB needs to be in Port 2.
- Network - LAN Interface 1
- Network - LAN Interface 2

Additional functions on this window include:

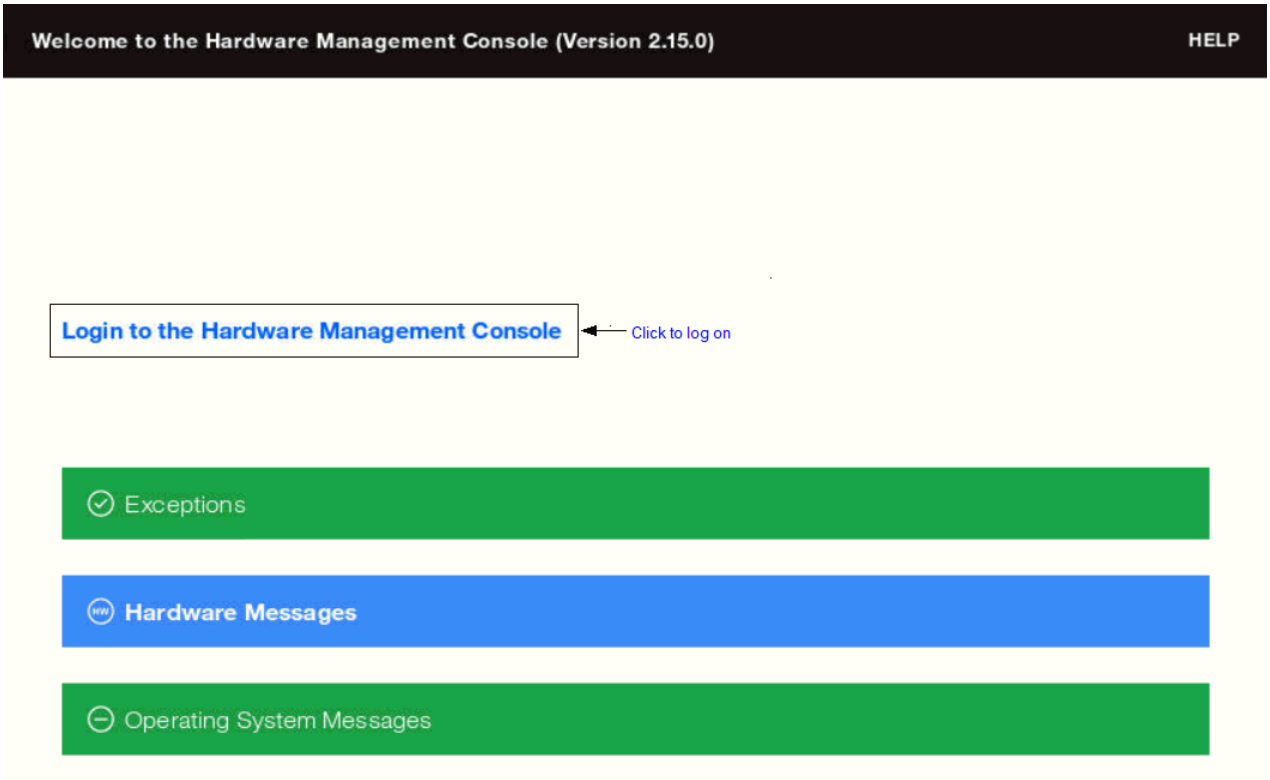
Cancel
To exit this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Welcome

Welcome to the Hardware Management Console

Use this window to log on and start the console and see an overview of the system status.



The elements of this window allow you to do the following:

- View the online help
- Learn the status of the console

Log On

To log on to the console, select the **Login to the Hardware Management Console** link.

This takes you to the logon window where you provide your user ID and password.

Online Help

To view the online help for the console, click **HELP** found in the upper right corner of the window.

Status overview

The status overview area of this window indicates the system status of the objects.

Exceptions

When no objects exist with unacceptable status, then the **Exceptions** bar is green to convey a positive status. If there are objects that have exceptions, then the bar is red. To view the exceptions and log on to the Hardware Management Console, select the **Exceptions** link.

Hardware Messages

When no objects exist with hardware messages, then the **Hardware Messages** bar is green to convey a positive status. If there are objects that exist with hardware messages, then the bar is blue. To view the hardware messages and log on to the Hardware Management Console, select the **Hardware Messages** link.

Operating System Messages

When no objects exist with operating system messages, then the **Operating System Messages** bar is green to convey a positive status. If there are objects that exist with operating system messages, then the bar is purple. To view the operating system messages and log on to the Hardware Management Console, select the **Operating System Messages** link.

What's New

Accessing the What's New task

This task is a link to a description of the new features for this version of the Hardware Management Console.

To view this information:

1. Open the **What's New** task. A summary of the new content is displayed. For more detailed information on the changes, you can click the individual topics that are listed.
2. When you are done viewing the information, you can click the X in the upper right corner of the window.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z