Hewlett Packard
Enterprise

HPE BladeSystem Onboard Administrator User Guide

Abstract

This guide provides information on the initial setup and operation of the HPE BladeSystem Onboard Administrator. It also covers use of the Onboard Administrator GUI and enclosure Insight Display. The information in this guide applies to version 4.71 (or later) of the HPE BladeSystem Onboard Administrator.

Part Number: 695522-403
Published: September 2017
Edition: 29

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Contents

Overview

HPE BladeSystem Onboard Administrator is the enclosure management processor, subsystem, and firmware base that supports the HPE BladeSystem c-Class enclosure and all the managed devices contained within the enclosure.

Onboard Administrator provides a single point from which to perform basic management tasks on server blades or switches within the enclosure. Onboard Administrator performs configuration steps for the enclosure, enables run-time management and configuration of the enclosure components, and informs you of problems within the enclosure through email, SNMP, or the Insight Display.

Hewlett Packard Enterprise recommends that you read the specific HPE BladeSystem c3000 or c7000 Enclosure user guide for enclosure specific information before proceeding with Onboard Administrator setup.

The Onboard Administrator provides several features designed to simplify management of c-Class blades and interconnects. The BladeSystem c3000 and c7000 Enclosures can be configured with redundant Onboard Administrator modules to provide uninterrupted manageability of the entire enclosure and blades in the event of a failure of a single Onboard Administrator module. The following table indicates which Onboard Administrator feature is enhanced when the enclosure contains redundant Onboard Administrator modules. For an enclosure with only a single Onboard Administrator module, the table indicates the behavior of the enclosure if the single Onboard Administrator module has failed or is removed. Enclosure Dynamic Power Capping, introduced in Onboard Administrator firmware version 2.31, is only available in BladeSystem enclosures with redundant Onboard Administrator modules installed.

Benefits of using a redundant Onboard Administrator versus a single Onboard Administrator

Onboard Administrator feature	Single Onboard Administrator in enclosure	Single Onboard Administrator failed or removed	Redundant Onboard Administrator in enclosure
Power allocation and control for all blades and interconnects	Yes. No enclosure dynamic power capping as this requires redundant Onboard Administrators.	No. Power supplies will continue to deliver power to all blades and interconnects. No power on requests can be made for blades or interconnects.	Yes. Complete control including sustaining a failure of either Onboard Administrator. Enclosure dynamic power capping requires redundant Onboard Administrators.
Cooling for all blades and interconnects.	Yes. Complete control.	No. All enclosure fans will ramp to an un-managed higher speed to protect blades and interconnects from overheating.	Yes. Complete control, including sustaining a failure of either Onboard Administrator.
Enclosure Bay IP Addressing (EBIPA)	Yes. Complete control.	No. EBIPA IP addresses will be lost after lease timeout.	Yes. Complete control, including sustaining a failure of either Onboard Administrator.

Table Continued

Onboard Administrator feature	Single Onboard Administrator in enclosure	Single Onboard Administrator failed or removed	Redundant Onboard Administrator in enclosure
Ethernet communications to Onboard Administrator, server iLO, interconnect management processors such as Virtual Connect which use the Onboard Administrator/iLO management port	Yes. Complete control.	No Ethernet management communications including internal management traffic such as Virtual Connect Manager to other VC modules in the enclosure.	Yes. Complete control, including sustaining a failure of either Onboard Administrator.
Information and health status reporting for all blades, interconnects, fans, power supplies, Onboard Administrators, and enclosure through Onboard Administrator's GUI or CLI, alert mail, or SNMP	Yes. Complete control.	No information is available from the Onboard Administrator nor is any out-of-band information available from VCM or iLO on any server.	Yes. Complete control, including sustaining a failure of either Onboard Administrator.
Insight Display	Yes. Complete control.	No.	Yes. Complete control, including sustaining a failure of either Onboard Administrator.
Enclosure DVD (requires either c3000 DVD option, external USB DVD drive, or USB key)	Yes. Complete control.	No.	Yes. Complete control, including sustaining a failure of either Onboard Administrator.
Enclosure KVM (requires c3000 KVM option or Onboard Administrator module with VGA connector)	Yes. Complete control.	No.	Yes. Complete control. For the c3000 Enclosure, requires both c3000 KVM option and redundant Onboard Administrator option. For the c7000 Enclosure, requires two of the newer Onboard Administrator modules with VGA connector.

Stored Onboard Administrator settings and module replacement

Enclosure model	Single Onboard Administrator in enclosure	Redundant Onboard Administrator (same replacement type installed) [1]	Redundant Onboard Administrator (different replacement type installed)[1]
c3000	All enclosure settings are lost when a single module is removed and must be restored manually using Insight Display and USB key, GUI, or CLI.	All enclosure settings are retained on the remaining module and those settings are synchronized to the replaced module if the firmware versions match. [2]	When changing from the non-redundant c3000 Onboard Administrator to redundant Onboard Administrator with DDR2, the enclosure settings must be restored manually using Insight Display and USB key, GUI, or CLI.
c7000	All enclosure settings are lost when a single module is removed and must be restored manually using Insight Display and USB key, GUI, or CLI.	All enclosure settings are retained on the remaining module and those settings are synchronized to the replaced module if the firmware versions match.[2]	All enclosure settings are retained on the remaining module and those settings are synchronized to the replaced module if the firmware versions match.[2]

[1] *1 Removing a redundant Onboard Administrator module immediately results in the remaining module becoming the Active Onboard Administrator.*

[2] *If redundant Onboard Administrator firmware versions do not match, the settings are not automatically synchronized. Synchronize the firmware by using the Insight Display, GUI, or CLI command, and then the settings are automatically synchronized to the replaced Onboard Administrator module.*

Access requirements

To access Onboard Administrator web interface, you must have the Onboard Administrator IP address and a compatible web browser. You must access the application through HTTPS (HTTP packets exchanged over an SSL/TLS-encrypted session).

The Onboard Administrator web interface requires an XSLT-enabled browser with support for JavaScript 1.3 or the equivalent.

For a list of browsers supported for use with Onboard Administrator, see the latest version of the Onboard Administrator release notes.

Before running the web browser, you must enable the following browser settings:

- ActiveX (for Microsoft® Internet Explorer)
- Cookies
- JavaScript

If you receive a notice that your browser does not have the required functionality, be sure that your browser settings meet the preceding requirements, and see **Recovering the administrator password**.

If you use an installed language pack with the Onboard Administrator GUI and the browser does not display all characters correctly, make sure the operating system has the corresponding language support installed.

To access the Onboard Administrator CLI, use Onboard Administrator IP address and a terminal or terminal application. To access the CLI interface, you must use Telnet or SSH, depending on which of these protocols are enabled.

The following ports are used to access and monitor the Onboard Administrator.

Protocol	Incoming port	Outgoing port
SSH	22	—
Telnet	23	—
SMTP	—	25
Browser access	80	80
Browser access encrypted	443	443
SNMP get/set	161	—
SNMP traps	—	162
LDAP SSL	—	636
LDAP Global Catalog	—	3269
Terminal services pass-through from PC to iLO	3389	—
iLO Remote Console	17790	—
Virtual media from PC to iLO	17988	—
Remote syslog	—	514

You can change LDAP and Remote syslog port numbers.

If a protocol is disabled, then the corresponding ports are also disabled.

To use EDPC, iLO firmware 1.70 or later is required.

NOTE:

The Onboard Administrator supports multiple simultaneous login sessions, whether through the Onboard Administrator web interface or CLI, except for LDAP/Active Directory users where only one login session is allowed per user.

Onboard Administrator overview

Managing a c-Class enclosure involves multiple functions:

- Detecting component insertion and removal
- Identifying components including required connectivity
- Managing power and cooling
- Controlling components including remote control and remote consoles

Detecting component insertion and removal

Onboard Administrator provides component control in c-Class enclosures. Component management begins after the component is detected and identified. The Onboard Administrator detects components in BladeSystem c-Class enclosures through presence signals on each bay. When you insert a component into a bay, the Onboard Administrator immediately recognizes and identifies the component. When you remove a component from a bay, the Onboard Administrator deletes the information about that component.

Identifying components

To identify a component, Onboard Administrator reads a FRU EEPROM that contains specific factory information about the component such as product name, part number, and serial number. All FRU EEPROMs in c-Class enclosures are powered up, even if the component is turned off. Therefore, Onboard Administrator can identify the component before granting power. For devices such as fans, power supplies, and Insight

Display, Onboard Administrator directly reads the FRU EEPROMs. Onboard Administrator accesses server blade FRU EEPROMs through iLO management processors.

- The server blades contain several FRU EEPROMs: one on the server board, which contains server information and embedded NIC information, and one on each installed mezzanine option cards.
- Server blade control options include auto login to the iLO web interface and remote server consoles, virtual power control, and boot order control. Server blade control options also include extensive server hardware information including BIOS and iLO firmware versions, server name, NIC and option card port IDs, and port mapping.
- Onboard Administrator provides easy-to-understand port mapping information for each server blade and interconnect module in the enclosure.

The NIC and mezzanine option FRU information informs Onboard Administrator of the type of interconnects each server requires. Before power is provided to a server blade, Onboard Administrator compares this information with the FRU EEPROMs on installed interconnect modules to check for electronic keying errors. For interconnect modules, Onboard Administrator provides virtual power control, dedicated serial consoles, and management Ethernet connections.

A 16-step progress meter appears when the Active Onboard Administrator boots. Some steps might take as much as several minutes, depending on the number and types of blades, mezzanine cards, and interconnects.

NOTE:

If OA is unable to discover/identify a Gen10 or later generation of blade or its components, please ensure that "RIBCL" is enabled in the iLO of the blade.

Managing power and cooling

The most important Onboard Administrator tasks are power control and thermal management. Onboard Administrator can remotely control the power state of all components in BladeSystem c-Class enclosures. For components in device bays in the front of each enclosure, Onboard Administrator communicates with iLO to control servers, and with a microcontroller to control options such as storage blades. A separate microcontroller controls power to the interconnect modules.

After components are powered, the Onboard Administrator begins thermal management with Thermal Logic. The Thermal Logic feature in BladeSystem c-Class minimizes power consumption by the enclosure fan subsystem by reading temperature sensors across the entire enclosure. Then, Thermal Logic changes fan speed in different zones in the enclosure to minimize power consumption and maximize cooling efficiency.

Controlling components

Onboard Administrator uses embedded management interfaces to provide detailed information and health status for all bays in the enclosure including presence detection signals in each bay, i2c, serial, USB, and Ethernet controllers. Onboard Administrator also offers information on firmware versions for most components in the enclosure and can be used to update those components.

Interfaces

Each c-Class enclosure has several external management interfaces that connect the user to Onboard Administrator. The RJ-45Ethernet jack is the primary interface. This interface provides network access to the Onboard Administrator and management interface on all server blades (iLO), storage blades (TBM), and interconnect modules.

A serial port on the Onboard Administrator module provides full out-of-band CLI access to the Onboard Administrator and is used for Onboard Administrator firmware flash recovery.

USB ports on Onboard Administrator are used to connect external DVD drives to support the enclosure DVD feature. In addition, you can order an optional internal DVD drive for the c3000 Enclosure. The USB port on the Onboard Administrator might have a sticker on the port, stating that it is reserved for future use. To use the USB port with Onboard Administrator firmware version 2.00 or later, remove the sticker.

All c-Class enclosures support two enclosure link connectors that provide private communications among enclosures linked with CAT5 cable. The enclosure link-up connector provides an enclosure service port that allows you to temporarily connect a laptop personal computer to any linked enclosure Onboard Administrator for local diagnostics and debugging.

The KVM Module option for the c3000 Enclosure plugs into the rear bay adjacent to interconnect module 1 and provides a VGA connector and two more USB connectors for the c3000 Enclosure. This KVM module enables the enclosure KVM feature for the c3000 Enclosure. The VGA connector attaches to an external VGA monitor and external USB keyboard and mouse to provide access to all the server video consoles or the Onboard Administrator CLI or Insight Display.

The new c7000 Onboard Administrator Module with KVM adds a VGA connector to the c7000 Onboard Administrator, enabling the Enclosure KVM feature for the c7000 Enclosure. The Active c7000 Onboard Administrator Module with KVM provides the same Enclosure KVM capabilities as the optional c3000 KVM Module. An external USB hub (not included) must be used to connect a USB DVD drive at the same time as the KVM USB for keyboard and mouse for simultaneous Enclosure KVM and Enclosure DVD functionality. The Standby Onboard Administrator Module with KVM will only provide access to the Onboard Administrator CLI login which enables the logged in user to force a takeover.

Each c-Class enclosure includes an embedded Insight Display on the front of the enclosure which provides status and information on all the bays in a c-Class enclosure and diagnostic information if the Onboard Administrator detects a problem in the enclosure. The Insight Display configures key settings in the Onboard Administrator including the IP address of the Onboard Administrator.

Onboard Administrator authentication

Security is maintained for all Onboard Administrator user interfaces through user authentication. User accounts created in Onboard Administrator are assigned one of three privilege levels and granted access to component bays at the specified privilege level. Onboard Administrator stores the passwords for local user accounts and can be configured to use LDAP authentication for user group accounts. The Insight Display can be protected by an LCD PIN code or completely disabled. An LCD PIN code protects against unauthorized access to the Insight Display and Enclosure KVM. Use of the KVM Module to access server consoles is protected by server operating system user name and passwords.

IMPORTANT:

Onboard Administrator does not support OpenLDAP.

Role-based user accounts

Onboard Administrator provides configurable user accounts that can provide complete isolation of multiple administrative roles such as server, LAN, and SAN. User accounts are configured with specific device bay or interconnect bay permissions and one of three privilege levels: administrator, operator, or user. An account with administrator privileges including Onboard Administrator bay permission can create or edit all user accounts on an enclosure. Operator privileges enable full information access and control of permitted bays. User privileges enable information access but no control capability.

Onboard Administrator requires you to log in to the web GUI or CLI with an account and password. The account can be a local account where the password is stored on Onboard Administrator or an LDAP account, where Onboard Administrator contacts the defined LDAP server to verify the user credentials. Two-Factor and CAC Authentication enables even tighter security for the user management session to Onboard Administrator. You can also configure both Two-Factor Authentication and LDAP authentication, as described in **TFA+LDAP Authentication**. Similarly you can configure CAC Authentication and LDAP Authentication , as described in **CAC + LDAP Authentication**.

Rather than requiring separate logins to multiple resources (once to each enclosure, once to every server management processor, or both), Onboard Administrator enables single point access for linked enclosures in a rack. In this way, the administrator can use single sign-on to log in to a single Onboard Administrator and use the web GUI to graphically view and manage the HPE BladeSystem c-Class components in up to seven linked enclosures. (The single sign-on requires that all the active Onboard Administrators have the same password.) For example, an IT administrator can automatically propagate management commands, such as changing the enclosure power mode, across all the linked enclosures. A valid account must be present on each linked enclosure to gain access. For more information, see **Signing in to the Onboard Administrator GUI**.

Login security

Onboard Administrator provides several login security features. No penalty is imposed after an initial failed login attempt. With all subsequent failed attempts, Onboard Administrator imposes a 10-second to 30-second delay. An information page appears during each delay. This action continues until a valid login is completed. This feature assists in defending against possible dictionary attacks.

Onboard Administrator saves a detailed log entry for all failed login attempts.

Running Onboard Administrator for the first time

Setting up a c-Class enclosure using the Onboard Administrator is simplified by using the Insight Display first time installation wizard, followed by use of the Onboard Administrator GUI First Time Wizard or Onboard Administrator CLI to complete the reset of the enclosure settings.

When operating in FIPS Mode, configure FIPS Mode before performing any other enclosure or Onboard Administrator configuration, including configuration of the Virtual Connect or First Time Setup Wizard. Enabling FIPS Mode on an Onboard Administrator module or redundant pair of modules forces the Onboard Administrator modules to be reset to factory defaults. After configuring FIPS Mode, perform the configuration steps in this section. For more information on FIPS Mode, see "**FIPS tab**."

The Onboard Administrator modules, server blade iLO management processors and many interconnect modules default to DHCP for their management IP address. If the user has DHCP and connects the Onboard Administrator management port to the DHCP server, then the Onboard Administrator modules, all iLO, and interconnect modules supporting and configured to use the Onboard Administrator internal management network will all automatically obtain DHCP addresses from the user DHCP server.

If you do not have a DHCP server for assigning IP addresses to management processors, you must configure each Onboard Administrator IP address and then all the individual device and interconnect module management IP addresses by using one of the following methods:

- Recommended Practice - configure each Onboard Administrator with a static IP address using the Insight Display. Then log in to the Onboard Administrator GUI and use the First Time Setup Wizard or log in to the Onboard Administrator CLI and configure and enable Enclosure Bay IP Addresses (EBIPA) for Device Bays and Interconnect Bays. Enabling EBIPA for a bay will allow that server or interconnect module to be replaced and the new module will automatically obtain the previously configured IP address for that bay.
- Alternatively, configure each device and interconnect module for static IP manually. For ProLiant server blades, you must connect to each server blade from SUV port (using the SUV cable included with each enclosure) and configure the iLO IP address manually during POST by pressing F8 to access the iLO Option ROM settings. For the interconnect modules with management processors that can use the Onboard Administrator management network, access and configure their IP address using either an external serial console port or the Onboard Administrator CLI serial connection to that bay. After changing the interconnect module IP address manually, the switch may require power cycling to use the new setting.

IMPORTANT:

Do not configure the IP address for any Onboard Administrator in the 169.254.x.x range.

The initial credentials to log in to a new Onboard Administrator module are printed on a label on each module. The user is Administrator and the password is unique to each module. This password must be captured by the installer and communicated to the remote Administrator for the first remote login to the Onboard Administrator GUI or Onboard Administrator CLI.

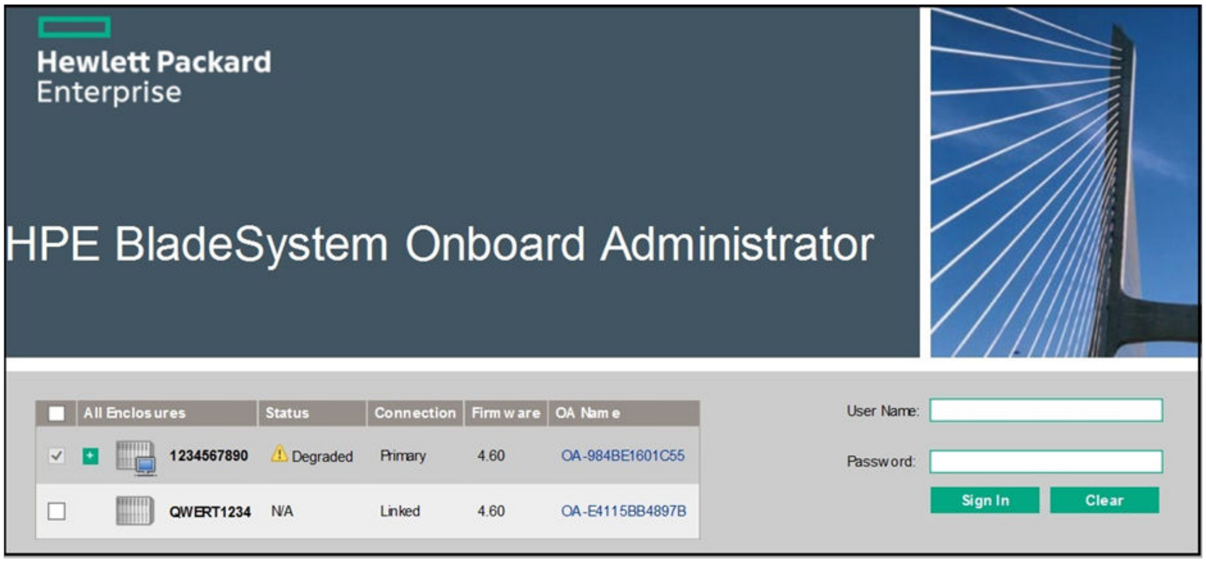
The enclosure settings can be configured manually or uploaded from a configuration script or file. The web GUI offers a First Time Setup Wizard. The CLI can be accessed from the Onboard Administrator serial port, Ethernet management port, service port, or by using the Enclosure KVM - Onboard Administrator CLI button.

An alternative to manual configuration is to upload an enclosure configuration file to the active Onboard Administrator using either the GUI or CLI with an HTTP, FTP or TFTP network location for the configuration file, or use the GUI, CLI or Insight Display to upload a configuration file from a USB key drive plugged into the active Onboard Administrator USB port.

The recommended practice to create an enclosure configuration file is to use the GUI, CLI, or Insight Display USB Key Menu to save the existing configuration to a file. The saved configuration file is a set of CLI text commands for each configuration item. The Onboard Administrator will not save user passwords when it saves a configuration file. The user can edit the configuration file and insert the password commands for each user account - or use the Administrator local account to individually update all user passwords after restoring a previously saved enclosure configuration file.

If the enclosure contains redundant Onboard Administrator modules, the remaining Onboard Administrator updates the new Onboard Administrator with all the settings.

Signing in to the Onboard Administrator GUI


Hewlett Packard Enterprise
HPE BladeSystem Onboard Administrator
Sign In
Clear

□	All Enclosures	Status	Connection	Firmware	OA Name
☑	1234567890	⚠ Degraded	Primary	4.60	OA-984BE1601C55
□	QWERT1234	N/A	Linked	4.60	OA-E4115BB4897B

User Name:

Password:

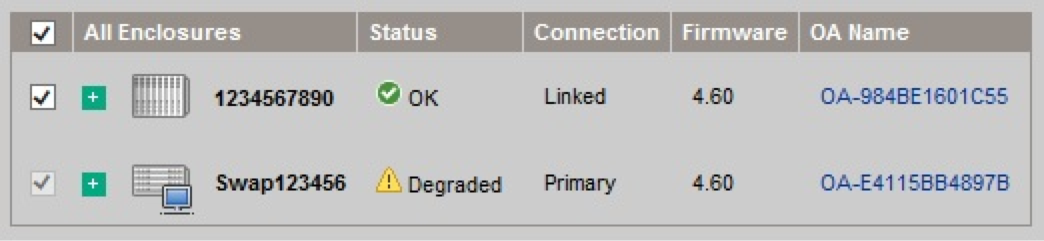
Enter the user name and initial administration password for your Onboard Administrator. The default account credentials can be found on the tag attached to the Onboard Administrator.

When signing in to the Onboard Administrator, the following issues might occur:

- You are not entering the information correctly. Passwords are case sensitive.
- The account information you are entering has not been set up for Onboard Administrator.
- The user name you are entering has been deleted, disabled, or locked out.
- The password for the account must be changed.
- You are attempting to sign in from an IP address that is not valid for the specified account.
- The password for the Administrator account has been forgotten or lost. To reset the Administrator password, see **Recovering the Administrator password**.

If you continue to have issues signing in, contact your administrator.

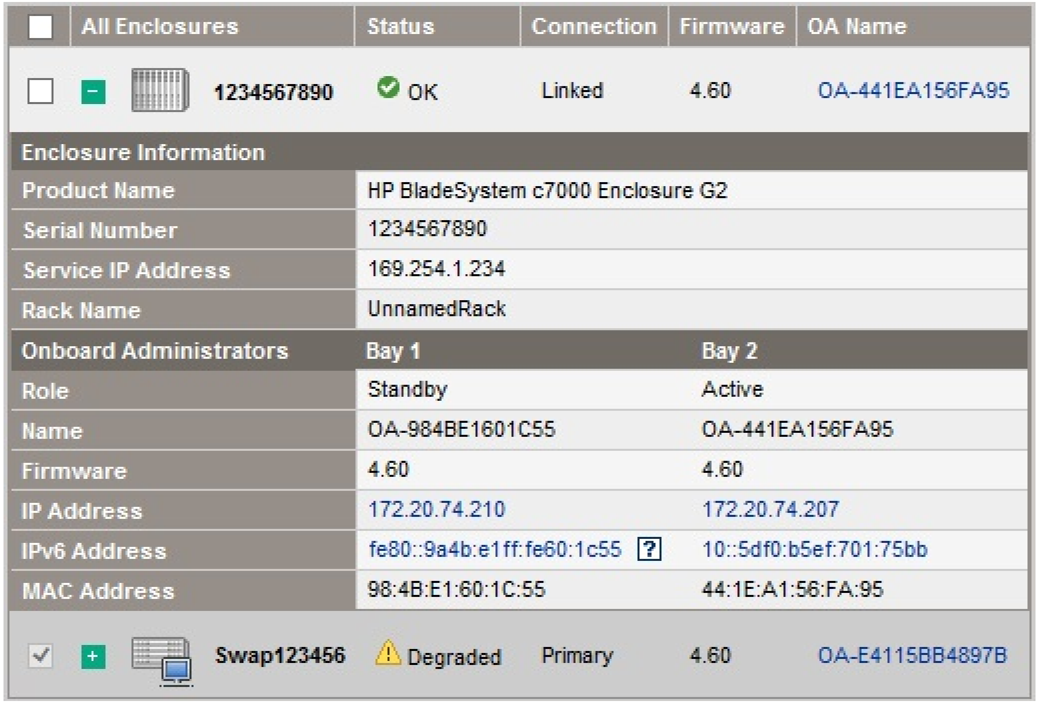
If you have the same credentials on multiple enclosures, you can use single sign-on to log in to multiple linked enclosures. Before signing in, select the box next to each of the linked enclosures listed in the table on the Sign-in page, as shown in the following table. In this scenario, you are attempting to log in to three active Onboard Administrators on the corresponding selected enclosures, using the supplied user name and password. Alternatively, to verify and log in to all the linked enclosures, select the box at the top of the check box column. If the login succeeds, then each of those enclosures is viewed in the same GUI window. The display order of each enclosure is based on the enclosure link cables. Connect the "down-link" port of the topmost enclosure to the "up-link" port of the following enclosure. Repeat until the bottom enclosure is reached. This GUI order is the same order that appears in the `SHOW TOPOLOGY` command.



☑	All Enclosures	Status	Connection	Firmware	OA Name
☑ +	1234567890	✓ OK	Linked	4.60	OA-984BE1601C55
☑ +	Swap123456	⚠ Degraded	Primary	4.60	OA-E4115BB4897B

As shown in the preceding example, the enclosure table on the Sign-in page also provides information on the enclosure status, connection, firmware version, OA name, and rack position. If extended data has been enabled on the **Network Access** page Anonymous Data tab, you can view more detailed enclosure and Onboard Administrator information by selecting the + sign to the left of the enclosure icon. The + sign appears only if extended data is enabled on that enclosure. Through Location Discovery Services, the extended data includes location information for each chassis. For more information about Location Discovery Services, see **Rack Overview screen**. Extended data is enabled by default. If extended data is disabled on an enclosure, the enclosure status appears as `N/A`.

The following figure shows the extended data for the first enclosure listed in the table.



□	All Enclosures	Status	Connection	Firmware	OA Name
□ −	1234567890	✓ OK	Linked	4.60	OA-441EA156FA95

Enclosure Information		
Product Name	HP BladeSystem c7000 Enclosure G2	
Serial Number	1234567890	
Service IP Address	169.254.1.234	
Rack Name	UnnamedRack	
Onboard Administrators	**Bay 1**	**Bay 2**
Role	Standby	Active
Name	OA-984BE1601C55	OA-441EA156FA95
Firmware	4.60	4.60
IP Address	172.20.74.210	172.20.74.207
IPv6 Address	fe80::9a4b:e1ff:fe60:1c55 ?	10::5df0:b5ef:701:75bb
MAC Address	98:4B:E1:60:1C:55	44:1E:A1:56:FA:95

☑ +	Swap123456	⚠ Degraded	Primary	4.60	OA-E4115BB4897B

Flash disaster recovery

To successfully recover an Onboard Administrator from a failed flash, you must have the following:

- Local access to the enclosure
- A DHCP server accessible by the Onboard Administrator
- A TFTP server accessible by the Onboard Administrator
- Onboard Administrator firmware (.bin file)

To recover from a failed flash, use one of the following processes:

- Flash recovering the Active OA with only one Onboard Administrator in the enclosure
- Flash recovering the Active OA with two Onboard Administrator modules in the enclosure.

Flash recovering the Active OA with one Onboard Administrator in enclosure

If you have only one Onboard Administrator in the enclosure and you want to Flash Recover the Active OA:

Procedure

1. With a null-modem cable (9600 N, 8, 1, VT100), locally connect to the Onboard Administrator.
2. Press and hold the Reset button of the Onboard Administrator for 5 seconds.
3. On the serial console, when you are prompted for Flash Recovery or Reset Password, press **F**. The Onboard Administrator obtains an IP address through DHCP.
4. At the prompt for the TFTP server IP address (where the Onboard Administrator image files are stored), enter the appropriate IP address.
5. You are prompted for the path to the Onboard Administrator firmware image. The Onboard Administrator downloads the image and flashes itself.

Upon successful completion of this process, the Onboard Administrator firmware is up to date, and any error condition is repaired.

Flash recovering the Active OA with two Onboard Administrators in the enclosure

If you have two Onboard Administrator modules in the enclosure and you want to Flash Recover the Active OA:

Procedure

1. With a null-modem cable (9600 N, 8, 1, VT100), locally connect to the Onboard Administrator.
2. Press and hold the Reset button of the Onboard Administrator for 5 seconds.

   On the serial console, when you are prompted for Flash Recovery or Reset Password, do not type anything. Wait at least 2 minutes or more to let the Standby OA to become the Active OA before proceeding to the next step.
3. When the OA to be flashed has become the Standby OA, press and hold the Reset button a second time on the same OA as in step b.
4. On the serial console, when you are prompted for Flash Recovery or Reset Password, press **F**. The Onboard Administrator obtains an IP address through DHCP.
5. At the prompt for the TFTP server IP address (where the Onboard Administrator image files are stored), enter the appropriate IP address.

   You are prompted for the path to the Onboard Administrator firmware image. The Onboard Administrator downloads the image and flashes itself.

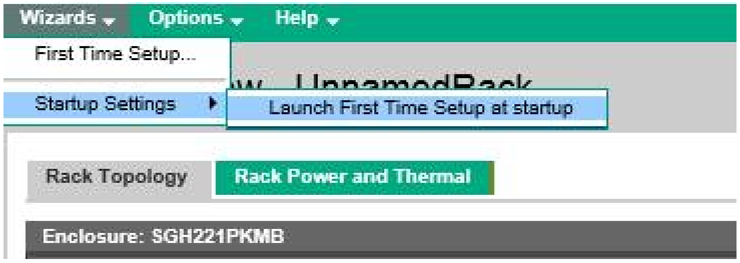
Upon successful completion of this process, the Onboard Administrator firmware is up-to-date, and any error condition is repaired.

NOTE:

Onboard Administrator with firmware version 4.50 or later will not support Flash Disaster Recovery to a version of firmware 4.50 or later. If using firmware version 4.50 or later, Flash Recover to a version prior to 4.50 and then update your firmware to the intended version (4.50 or later).

Running the setup wizard

To run the setup wizard, sign in to Onboard Administrator. The First Time Setup Wizard starts automatically when you sign in to Onboard Administrator for the first time. This wizard assists you in setting up all of the functions of the Onboard Administrator. You can access the setup wizard at any time after initial setup by clicking the **Wizards** link on the top left of the center screen.

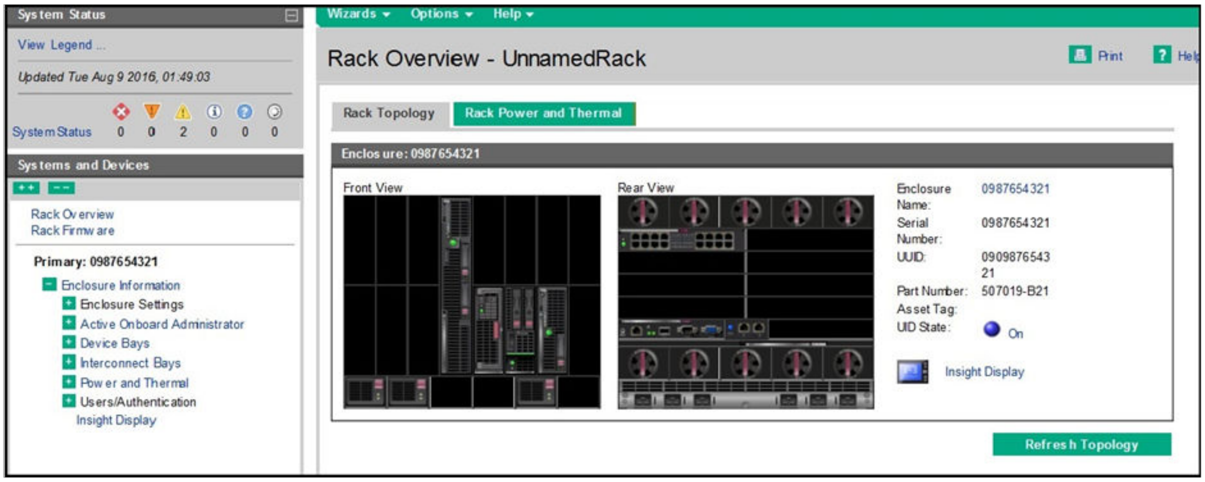


Enclosure: SGH221PKMB

For detailed information, see **First Time Setup wizard**.

Using online help

To access online help, click the green box with the white question mark or **Help** located on the top right of the screen under the header bar. Online help displays information related to the section of Onboard Administrator in which you are navigating.



Updated Tue Aug 9 2016, 01:49:03

System Status 0 0 2 0 0 0

Primary: 0987654321

Rack Overview - UnnamedRack

Enclosure: 0987654321

Enclosure Name:	0987654321
Serial Number:	0987654321
UUID:	090987654321
Part Number:	507019-B21
Asset Tag:	
UID State:	● On

Changing enclosure and device configurations

After you have completed the First Time Setup Wizard, you can return to the Onboard Administrator GUI to make configuration changes at any time. For information that will help you make changes to enclosure and device configuration, user setup, and LDAP server settings and LDAP groups, see **Configuring HPE BladeSystem enclosures and enclosure devices**.

For information about enclosure power settings, see **Enclosure Power Management**.

Recovering the administrator password

If the Administrator password has been lost, you can reset the administrator password to the factory default that shipped on the tag with the Onboard Administrator module. The Onboard Administrator resets a lost password to Lost Password/Flash Disaster Recovery (LP/FDR) mode. To reset the administrator password to the factory default:

1. Connect a computer to the serial port of the Active Onboard Administrator using a null-modem cable.
2. With a null-modem cable (9600 N, 8, 1, VT100) locally connect to the Onboard Administrator.
3. Open a suitable terminal window utility (Windows or Linux), and connect to the Active Onboard Administrator.
4. Press and hold in the Onboard Administrator reset button for 5 seconds.
5. To boot the system into Lost Password modem Press **L**. The password appears as the system reboots.

Alternatively, to reset a password on the Onboard Administrator, select the Insight Display (LCD panel) USB Menu option. This option restores a configuration script using command line interface commands stored on a USB key.

NOTE:

If the Insight Display USB menu buttons are locked, then the serial port method must be used. If the LCD panel is locked, then a large “lock” symbol appears on the screen.

In this example, the OA Administrator password is set to `Password123`.

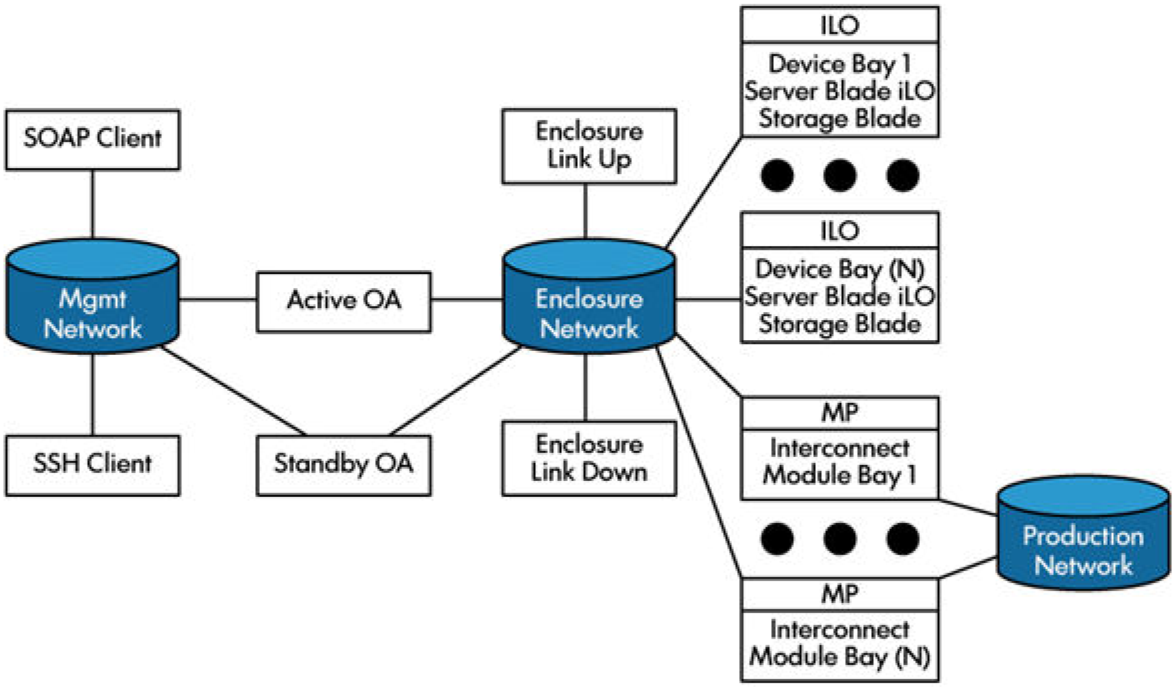
1. Create a text file named `reset_password.cfg` with the one line command: `SET USER PASSWORD` “Administrator” “Password123”
2. Insert the flash drive with `reset_password.cfg` file into the USB port of the active Onboard Administrator. The LED on the Onboard Administrator indicates which OA is active.
3. Using the Onboard Administrator Insight Display, navigate to the main menu, select USB Key Menu, and then click **OK**.
4. If Insight Display PIN Protection is enabled, you are prompted to enter the PIN. Select **Accept,** and then click **OK**.
5. Select **Restore Configuration**, then click **OK.** The USB flash drive in the Onboard Administrator is scanned and the available .cfg files are listed.
6. Select the `reset_password.cfg` file, and then click **OK**.
7. The Confirm Operation screen appears, click **OK**.
8. Log in to the Onboard Administrator with the user ID and password specified in step 1.

Security considerations

This section documents the architecture and best practice security recommendations to be considered when configuring the Onboard Administrator and compares default settings with the previous versions.

BladeSystem network architecture overview

All device bays, interconnect modules, and Onboard Administrator modules are connected to an internal enclosure network that is managed by the active Onboard Administrator. Network traffic from business applications running on server blades is routed through interconnect switch modules and onto the production network.



Although it is possible for the management and production networks to be connected, the management network should be isolated from production traffic and the intranet. From a security perspective, this reduces access and ability to attack the management interfaces. From an efficiency standpoint, separate networks keep production traffic off the management network.

Recommended security best practices

In addition to the best practices, note these additional considerations.

Physical presence considerations

Physical access to a system often implies administrator privilege. The Onboard Administrator is no exception. For more information on how to configure the Onboard Administrator, see **Configuring HPE BladeSystem enclosures and enclosure devices**.

- Verifying physical cabling

  The BladeSystem enclosure can have many cables attached to the enclosure. Cables connected to the interconnect switch modules are generally for production network traffic. All other cables and ports are generally for enclosure management network traffic and should be carefully inspected.

  - Ensure that enclosure link ports are connected only to enclosure link ports on other enclosures.
  - Inspect Onboard Administrator serial ports for unauthorized connections.
  - Inspect Onboard Administrator USB ports for unauthorized connections.
- Securing the Insight Display LCD panel

  The Insight Display LCD panel allows for configuration and monitoring of key Onboard Administrator settings: network address configuration and power up/down of server blade bays to name a few critical BladeSystem functions. Hewlett Packard Enterprise recommends securing the Insight Display LCD panel with a PIN, particularly in a multi-tenant datacenter. Furthermore, certain regulatory or industry standards, such as PCI, might require that all interfaces be secured with a PIN/password, regardless of requiring physical access.

  The Insight Display LCD panel buttons are locked by default in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug. For more information, see **FIPS tab**.

Set factory defaults before hardware redeployment

The very nature of redundant hardware is to ensure that all settings are present so that if a failure occurs on the Active Onboard Administrator, the Standby Onboard Administrator can take over the active role. This means that local user account information is duplicated on the Standby Onboard Administrator. If Enclosure IP mode is configured, then the private key used for SSL communications is also stored on the Standby Onboard Administrator. (Enclosure IP mode is not configured by default.) Depending on the security requirements for the datacenter, critical security parameters should be cleared from the hardware before decommissioning or reprovisioning an enclosure or components inside the enclosure, such as the Onboard Administrator, VC, and iLO for BladeSystem.

To ensure all critical security parameters are cleared, SET FACTORY defaults. Additionally, the Administrator password can be set to factory “toe-tag” value by manually changing the password or connecting a serial cable and invoking the lost password recovery procedure. For instructions, see **Recovering the administrator password**.

Isolate the management network

No matter how secure a device might appear to be, there will always be some sort of new attack or vulnerability. As a preventative measure and to follow industry best practices, Hewlett Packard Enterprise strongly recommends that the management network be separate from the production network. Furthermore, do not place the management network on the open internet or firewall DMZ without requiring additional access authentication, such as using a VPN/tunnel.

Network ports

For more information on ports, see **Access requirements**.

For more information on managing Hewlett Packard Enterprise software through a firewall, see the *Managing Hewlett Packard Enterprise Servers Through Firewalls with Insight Management White Paper*. This document may be downloaded from the **HPE Insight Management Information Library**.

Cryptographic security capabilities and defaults

Beginning with version 3.71, Onboard Administrator significantly upgrades the Onboard Administrator cryptographic capabilities by adding a new FIPS Mode of operation called FIPS Mode ON. Beginning with version 4.70, Onboard Administrator adds another new set of cryptography required by CNSA under a new FIPS Mode of operation called Top-Secret mode. FIPS Mode enforces a number of requirements that differ significantly from non-FIPS settings and prior releases. The security improvements remove weak algorithms and generally follow FIPS 140-2 and CNSA guidance. FIPS mode DEBUG will no longer be a separate FIPS mode. Instead, DEBUG option can be enabled or disabled by an OA administrator when switching between FIPS Modes ON and Top-Secret. For more information, see the following table. A list of supported SSH ciphers, SSH key exchange algorithms, and SSH Message Authentication Code algorithms follows the table.

The OA Administrator can modify FIPS Mode settings and enable or disable cryptographic protocols and ciphers by using the **Enclosure Settings > Network Access > FIPS tab**.

NOTE:

When running a version of Onboard Administrator firmware earlier than version 3.71 with Strong Encryption mode enabled, if you update the firmware to version 3.71 or later and earlier than 4.40, an entry might be logged to the Onboard Administrator syslog indicating that the Onboard Administrator is operating in FIPS Mode. This syslog entry ("`FIPS: OA is operating in FIPS Mode On`") is incorrect and can be ignored.

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01-OA 4.02 FIPS Mode OFF	OA 4.01-OA 4.02 FIPS Mode ON	OA 4.11-OA 4.22 FIPS Mode OFF	OA 4.11-OA 4.22 FIPS Mode ON	OA 4.30-OA 4.70 FIPS Mode OFF	OA 4.30-OA 4.70 FIPS Mode ON	OA 4.70 FIPS Mode Top-Secret
General Security Items									
CSPs Zeroization	NO	YES	NO	YES	NO	YES	NO	YES	YES
Known Answer Tests (KATs)	NO	YES	NO	YES	NO	YES	NO	YES	YES
Power-up tests	NO	YES	NO	YES	YES	YES	YES	YES	YES
Continuous PRNG testing	NO	YES	NO	YES	YES	YES	YES	YES	YES
Minimum Password Length required	3	8	3	8	3	8	3	8	8
Require Password Complexity (upper, lower, symbols)	NO	YES	NO	YES	NO	YES	NO	YES	YES
FIPS compatible PRNG [1]	YES	YES	YES	YES	YES	YES	YES	YES	YES
Telnet service disabled	YES[2]	YES	NO [2]	YES	YES[2]	YES	YES [2]	YES[2]	YES[2]
Enclosure IP Mode disabled	NO	YES	NO	YES	NO	YES	NO	YES	YES
Support Dump disabled	NO	YES	NO	YES	NO	YES	NO	YES	YES
SNMPv1 and SNMPv2 services disabled	NO	YES	NO	YES	NO	YES	NO	YES	YES

Table Continued

	OA 3.71 FIPS Mode OFF	**OA 3.71 FIPS Mode ON**	**OA 4.01-OA 4.02 FIPS Mode OFF**	**OA 4.01-OA 4.02 FIPS Mode ON**	**OA 4.11-OA 4.22 FIPS Mode OFF**	**OA 4.11-OA 4.22 FIPS Mode ON**	**OA 4.30-OA 4.70 FIPS Mode OFF**	**OA 4.30-OA 4.70 FIPS Mode ON**	**OA 4.70 FIPS Mode Top-Secret**
SNMPv3 service disabled	NO	NO	NO	NO	NO	NO	NO	NO	YES
Partition Integrity Checking	YES	YES	YES	YES	YES	YES	YES	YES	YES
Requires Insight Display LCD PIN	NO	YES	NO	YES	NO	YES	NO	YES	YES
SSL Encryption									
Default SSL Key Type and Size	RSA 2048 bits	RSA 2048 bits	RSA 2048 bits	RSA 2048 bits	RSA 2048 bits	RSA 2048 bits	RSA 2048 bits	RSA 2048 bits	384(ECDSA)
Default self-signed certificate Hash Signature algorithm	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256	SHA384
Configurable SSL Hash signature algorithms on self signed certificate	YES	YES	YES	YES	YES	YES	YES	YES	NO
SSL/TLS Protocols	SSLv3 TLSv1	TLSv1	SSLv3 TLSv1	TLSv1	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2	TLSv1.2
Reject Certificates with non FIPS Hash Signature Algorithms[3]	NO	YES	NO	YES	NO	YES	NO	YES	YES

Table Continued

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01-OA 4.02 FIPS Mode OFF	OA 4.01-OA 4.02 FIPS Mode ON	OA 4.11-OA 4.22 FIPS Mode OFF	OA 4.11-OA 4.22 FIPS Mode ON	OA 4.30-OA 4.70 FIPS Mode OFF	OA 4.30-OA 4.70 FIPS Mode ON	OA 4.70 FIPS Mode Top-Secret
Permitted Certificate Signature Hash Algorithms	md5, sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	md5, sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha384, sha512
DES	NO	NO	NO	NO	NO	NO	NO	NO	NO
CAST5	NO	NO	NO	NO	NO	NO	NO	NO	NO
Blowfish	NO	NO	NO	NO	NO	NO	NO	NO	NO
ARC4	NO	NO	NO	NO	NO	NO	NO	NO	NO
3DES	YES	YES	YES	YES	YES	YES	YES	YES	NO
AES 128-SHA	YES	YES	YES	YES	YES	YES	YES	YES	NO
DHE-RSA-AES256-SHA	YES	YES	YES	YES	YES	YES	YES	YES - 4.30 NO - 4.40 and later	NO
AES256-SHA	YES	YES	YES	YES	YES	YES	YES	YES	NO
DHE-RSA-AES128-SHA	YES	YES	YES	YES	YES	YES	YES	YES - 4.30 NO - 4.40 and later	NO
EDH-RSA-DES-CBC3-SHA	YES	YES	YES	YES	YES	YES	YES	YES	NO
DES-CBC3-SHA	YES	YES	YES	YES	YES	YES	NO	NO	NO
AES128-GCM-SHA256	NO	NO	NO	NO	NO	NO	YES	YES	NO

Table Continued

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01-OA 4.02 FIPS Mode OFF	OA 4.01-OA 4.02 FIPS Mode ON	OA 4.11-OA 4.22 FIPS Mode OFF	OA 4.11-OA 4.22 FIPS Mode ON	OA 4.30-OA 4.70 FIPS Mode OFF	OA 4.30-OA 4.70 FIPS Mode ON	OA 4.70 FIPS Mode Top-Secret
AES256-GCM-SHA384	NO	NO	NO	NO	NO	NO	YES	YES	NO
AES128-SHA256	NO	NO	NO	NO	NO	NO	YES	YES	NO
AES256-SHA256	NO	NO	NO	NO	NO	NO	YES	YES	NO
ECDHE-ECDSA-AES256-GCM-SHA384	NO	NO	NO	NO	NO	NO	NO	NO	YES
ECDHE-ECDSA-AES256-SHA384	NO	NO	NO	NO	NO	NO	NO	NO	YES
ECDHE-RSA-AES256-GCM-SHA384	NO	NO	NO	NO	NO	NO	NO	NO	YES
ECDHE-RSA-AES256-SHA384	NO	NO	NO	NO	NO	NO	NO	NO	YES
DHE-RSA-AES256-GCM-SHA384	NO	NO	NO	NO	NO	NO	YES	YES	YES
DHE-RSA-AES128-GCM-SHA256	NO	NO	NO	NO	NO	NO	YES	YES	NO
SSH Interface									
Default SSH key type and size	DSA 2048	DSA 1024	DSA 2048	DSA 1024	RSA 2048	RSA 2048	RSA 2048	RSA 2048	ECDSA 384
HMAC-MD5	NO	NO	NO	NO	NO	NO	NO	NO	NO

Table Continued

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01- OA 4.02 FIPS Mode OFF	OA 4.01- OA 4.02 FIPS Mode ON	OA 4.11- OA 4.22 FIPS Mode OFF	OA 4.11- OA 4.22 FIPS Mode ON	OA 4.30- OA 4.70 FIPS Mode OFF	OA 4.30- OA 4.70 FIPS Mode ON	OA 4.70 FIPS Mode Top-Secret
HMAC-SHA1-96	NO	NO	NO	NO	NO	NO	NO	NO	NO
HMAC-SHA1	YES	YES	YES	YES	YES	YES	YES	YES	NO
HMAC-SHA256	NO	NO	NO	NO	YES	YES	YES	YES	NO
HMAC-SHA512	NO	NO	NO	NO	YES	YES	YES	YES	NO
Insight Display KVM									
RC4 Encryption	YES	NO	YES	NO	YES	NO	YES	NO	NO
AES Support for LCD KVM	YES	YES	YES	NO	YES	YES	YES	YES	YES

[1] *X9.31 was used in OA 3.71 and OA 4.01-4.02. From OA 4.11 onward, the SP800-90A compatible AES CTR-DRBG is used.*

[2] *Telnet is disabled by default in Onboard Administrator 3.70 and later. When in FIPS Mode, Telnet cannot be enabled.*

[3] *Default certificate hash algorithm changed from SHA1 to SHA256 in Onboard Administrator 3.70. You can select different key sizes and hash algorithms with the GENERATE KEY command.*

Onboard Administrator 4.40 modifies the display name of supported TLS ciphers and introduces a strict order to be followed by enabled TLS ciphers. The list of supported TLS ciphers and their order is given in the following table.

TLS cipher suites	OA 4.40 - 4.70 FIPS Mode OFF	OA 4.40 - 4.70 FIPS Mode ON	OA 4.70 FIPS Top Secret
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	YES	YES	NO
TLS_RSA_WITH_AES_128_CBC_SHA	YES	YES	NO
TLS_RSA_WITH_AES_256_CBC_SHA	YES	YES	NO
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	YES	NO	NO
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	YES	NO	NO
TLS_RSA_WITH_AES_128_GCM_SHA256	YES	YES	NO
TLS_RSA_WITH_AES_256_GCM_SHA384	YES	YES	NO
TLS_RSA_WITH_AES_128_CBC_SHA256	YES	YES	NO
TLS_RSA_WITH_AES_256_CBC_SHA256	YES	YES	NO

Table Continued

TLS cipher suites	OA 4.40 - 4.70 FIPS Mode OFF	OA 4.40 - 4.70 FIPS Mode ON	OA 4.70 FIPS Top Secret
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	YES	YES	NO
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	NO	NO	YES
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	NO	NO	YES
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	NO	NO	YES
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	NO	NO	YES
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	YES	YES	YES

SSH ciphers

The supported SSH ciphers are the same for FIPS Mode ON and FIPS Mode OFF, and for Onboard Administrator 3.71, 4.01 - 4.02, 4.11 - 4.22, and 4.30 - 4.70:

- `aes128-ctr`
- `aes192-ctr`
- `aes256-ctr`
- `aes128-cbc`
- `3des-cbc`
- `aes192-cbc`
- `aes256-cbc`
- `rijndael-cbc@lysator.liu.se`

Supported SSH cipher for FIPS mode TOP Secret and Onboard Administrator 4.70

`aes256-gcm@openssh.com`

SSH key exchange algorithms

- OA 4.30 - 4.70

  `ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`
- OA 4.11 - 4.22

  `diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`
- OA 4.01 - 4.02

  `diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1`
- OA 3.71

  `diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`
- OA 4.01 and later versions include an option to enable/disable

  `diffie-hellman-group1-sha1.`
- OA 4.01 and 4.02 default for `diffie-hellman-group1-sha1` is disabled.

- OA 4.11 - 4.22, and 4.30 - 4.60 default for `diffie-hellman-group1-sha1` is enabled when FIPS Mode is OFF and disabled when FIPS Mode is ON.
- OA 4.70 FIPS Mode TOP Secret key exchange algorithm

  `ecdh-sha2-nistp384`

SSH Message Authentication Code algorithms

The supported SSH Message Authentication Code is the same for FIPS Mode ON and FIPS Mode OFF. Onboard Administrator 3.70 and later no longer supports HMAC-MD5 and HMAC-SHA-96 for SSH2 message authentication.

- OA 4.11 - 4.22, and 4.30 - 4.70

  `hmac-sha2-256`

  `hmac-sha2-512`

  `hmac-sha1`
- OA 4.01 - 4.02

  `hmac-sha1`
- OA 3.71

  `hmac-sha1`

FIPS Top-Secret - After AES-GCM is selected, the exchanged MAC algorithms are ignored.

HPE BladeSystem c3000/c7000 Enclosure hardware installation

Installing Onboard Administrator modules

The BladeSystem c3000 and BladeSystem c7000 Enclosure ship with one Onboard Administrator module installed and can support up to two Onboard Administrator modules. Install Onboard Administrator modules based on the total number ordered:

- One Onboard Administrator module: Bay 1
- Two Onboard Administrator modules: Bays 1 and 2

Install an Onboard Administrator blank in an unused Onboard Administrator bay.

NOTE:

When two Onboard Administrator modules are installed, the module installed in Bay 1 is active and the module installed in Bay 2 is redundant.

Instructions for installing an Onboard Administrator module are available in the following documents accessible from the **BladeSystem Information Library**:

- HPE BladeSystem c3000 Enclosure Setup and Installation Guide
- HPE BladeSystem c7000 Enclosure Setup and Installation Guide

Onboard Administrator cabling

Instructions for cabling an Onboard Administrator module are available in the following documents accessible from the **BladeSystem Information Library**:

- BladeSystem c3000 Enclosure Setup and Installation Guide
- BladeSystem c7000 Enclosure Setup and Installation Guide

If the Onboard Administrator management Ethernet port is connected to a management LAN that also connects to server ports, be sure that the server applications do not overload the Onboard Administrator management port with broadcast packets. The Onboard Administrator management port forwards all broadcast packets from the management network to all the devices inside the enclosure, and the Onboard Administrator records network packet flooding messages to the active Onboard Administrator syslog when it detects a high rate of packets. If the server connections are 1GB, and the Onboard Administrator connection is 100 MB, the server broadcast packets can easily overwhelm the port on the network switch connected to the Onboard Administrator. If the network packet flooding persists, the Onboard Administrator performance is impacted with a possibility of Onboard Administrator restart if the packet flooding overwhelms the Onboard Administrator capacity. This condition occurs is because Onboard Administrator must inspect all packets from the network it is connected to so the Onboard Administrator can act as the management conduit for internal enclosure devices, such as iLOs or Virtual Connect management interfaces. While an Onboard Administrator restart does not cause direct customer traffic outage, this action can cause unnecessary inconvenience, especially in configurations with Virtual Connect.

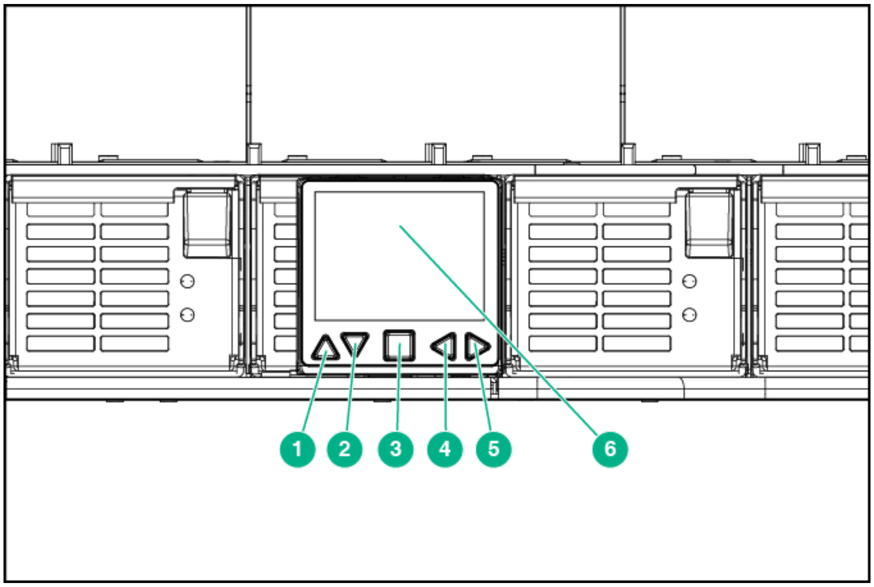
If the Onboard Administrator is connected to a network with a DHCP server when you power up the enclosure, the Onboard Administrator and each iLO (one for each server blade) consumes a DHCP lease.

Onboard Administrator ports

Port type	Description	Usage guidelines
OA/ILO	Ethernet 1000BaseT RJ45 connector	• Provides Ethernet access to the OA and to the iLO on each blade. • Supports interconnect modules with management processors configured to use the enclosure management network. • Autonegotiates 1000/100/10 or can be configured to force 100Mb or 10Mb full duplex.
USB	USB 2.0 Type A connector	For connecting USB devices such as DVD drives, USB key drives, or a keyboard or mouse for enclosure KVM use. The OA supports USB devices of 4GB or less.
Serial connector	Serial RS232 DB-9 connector with PC standard pinout.	Provides direct access to the OA, using a null-modem serial cable. Provides a two-way communication channel. • Useful when the OA is not reachable on the network. • Connect a computer to the OA command line interface (CLI). For example, the two-way communication channel allows users to execute diagnostic commands or to display information about the enclosure status. • Access the OA without requiring credentials or knowledge of an IP address. If your OA Administrator credentials have been forgotten, you can connect to the OA through the serial port and reset the password (see **Recovering the administrator password**).
VGA connector	VGA DB-15 connector with PC standard pinout. The c3000 Enclosure VGA ports are present on a separate module (the KVM module) in the rear of the enclosure.	Similar to serial port but additionally provides access to the rack KVM and the server blades iLO. However, this only provides a display; OA diagnostics cannot be run via the KVM connection. For accessing the enclosure KVM menu, connect a rack KVM monitor. For accessing the OA CLI, connect a VGA monitor.
Enclosure link-down port	Connects to the enclosure link-up port on the enclosure below with a CAT5 patch cable.	Used for connecting different enclosures and for creating a cluster of enclosures. By linking enclosures, only the base enclosure IP address must be known to access the group of enclosures.
Enclosure link-up port and service port	Connects to the enclosure link-down port on the enclosure above with a CAT5 patch cable.	Same usage as enclosure link-down port. On a stand-alone enclosure or the top enclosure in a series of linked enclosures, the top enclosure link-up port functions as a service port.

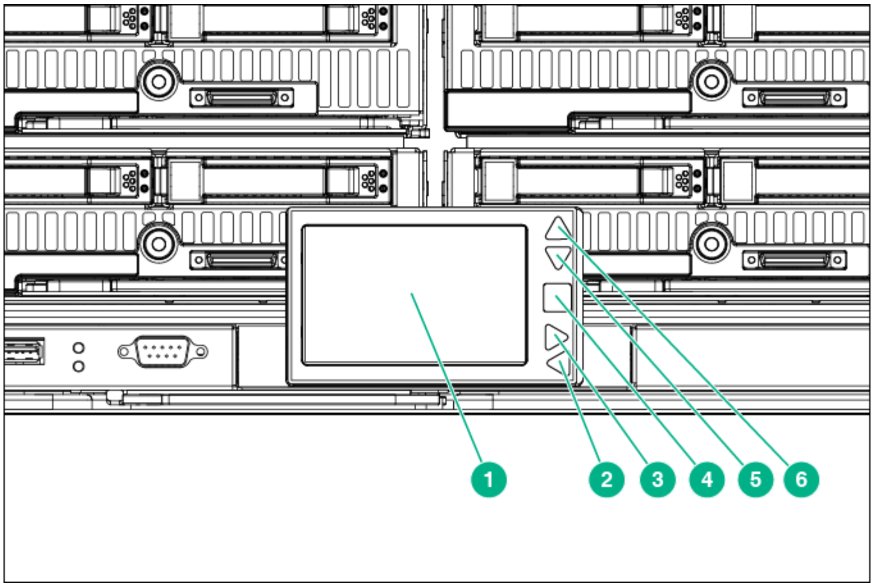
HPE BladeSystem Insight Display

HPE BladeSystem c7000 2-inch Insight Display components



Item	Description	Function
1	Up arrow button	Moves the menu selection up one position
2	Down arrow button	Moves the menu selection down one position
3	OK button	Accepts the highlighted selection and navigates to the selected menu
4	Left arrow button	Moves the menu or navigation bar selection left one position
5	Right arrow button	Moves the menu or navigation bar selection right one position
6	Insight Display screen	Displays Main Menu error messages and instructions

HPE BladeSystem c3000 and c7000 3-inch Insight Display components



Item	Description	Function
1	Insight Display screen	Displays Main Menu error messages and instructions
2	Left arrow button	Moves the menu or navigation bar selection left one position
3	Right arrow button	Moves the menu or navigation bar selection right one position
4	OK button	Accepts the highlighted selection and navigates to the selected menu
5	Down arrow button	Moves the menu selection down one position
6	Up arrow button	Moves the menu selection up one position

Insight Display overview

The Insight Display enables the rack technician to initially configure the enclosure. It also provides information about the health and operation of the enclosure. The color of the Insight Display varies with the condition of the enclosure health:

- Blue—The Insight Display illuminates blue when the enclosure UID is active. The enclosure UID is automatically turned on when the enclosure is powered up for the first time, and can be turned by selecting Turn Enclosure UID On from the Main Menu or by pressing the enclosure UID button on the management interposer.

  When the enclosure UID is on, the Insight Display flashes after two minutes of inactivity. Pressing any button on the Insight Display stops the blinking and reactivates the screen.
- Green—The Insight Display illuminates green when no error or alert conditions exist, and the enclosure is operating normally. After two minutes of inactivity, the Insight Display light turns off. Pressing any button on the Insight Display reactivates the screen.
- Amber—The Insight Display illuminates amber when the Onboard Administrator detects an error or alert condition. The details of the condition display on the screen.

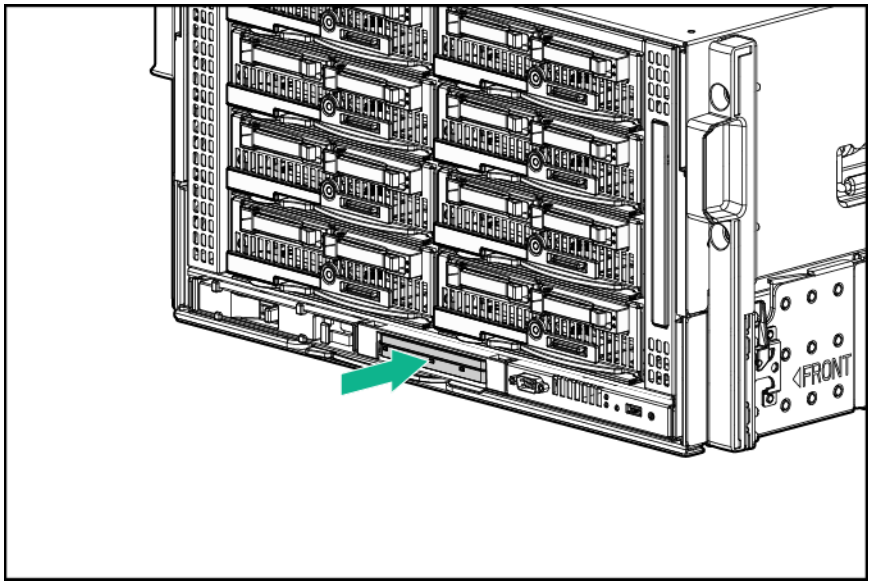
After two minutes of inactivity, the Insight Display flashes amber indicating an error or alert condition exists. If the enclosure UID is on and an error or alert condition exists, the Insight Display illuminates blue as the enclosure UID takes priority over the alert. Pressing any button on the Insight Display reactivates the screen.

- Dark (no power)—The Insight Display has a two-minute inactivity period. If no action is taken and no alert condition exists, the screen light turns off after two minutes. Hitting any button on the Insight Display will reactivate the screen.

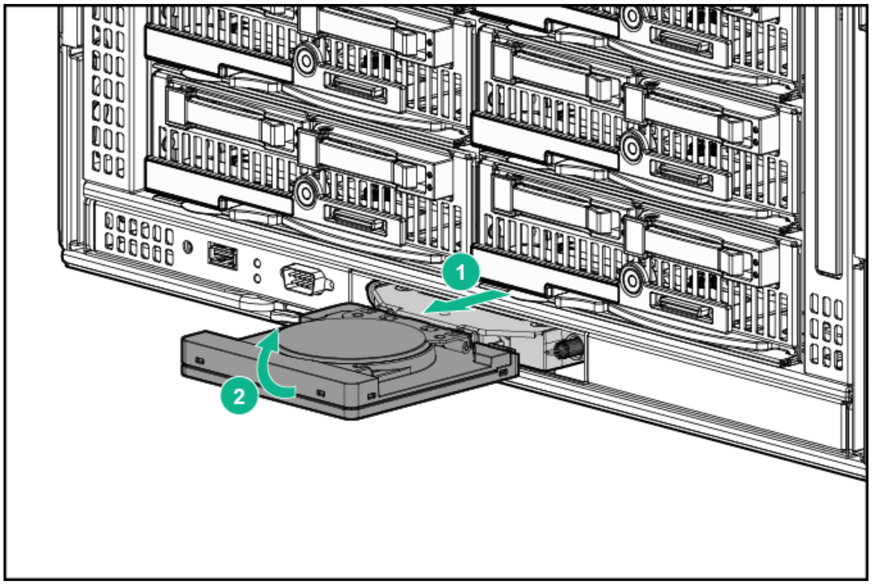
The Enclosure Health icon is located on the bottom left corner of every screen, indicating the condition of the enclosure health. Navigate the cursor to the Enclosure Health icon and pressing OK to access the Health Summary screen from any Insight Display screen.

Accessing the HPE BladeSystem c3000 Insight Display

1. To access the Insight Display, push on the exposed end.



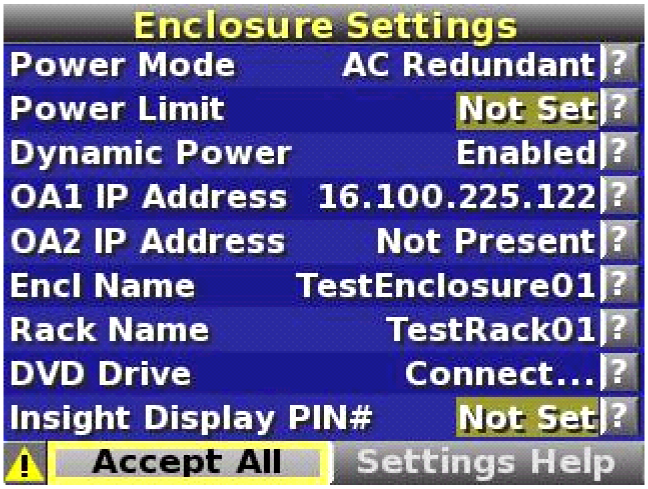
2. Pull the Insight Display out of the chassis to lock it into place, and then tilt it up.



Running the Insight Display installation

To identify the enclosure, the rear enclosure UID light and the background of the Insight Display are illuminated blue when the enclosure is powered on initially. When the enclosure is powered up for the first time, the Insight Display launches an installation wizard to guide you through the configuration process. At the beginning of the installation, the wizard automatically powers on the enclosure UID. After the installation is complete, the wizard powers off the enclosureUID. After configuring the enclosure, the Insight Display verifies that there are no installation or configuration errors. If errors are present, the Insight Display guides you through the process of correcting the errors.

The Enclosure Settings screen is the first screen to appear.



Power Mode	AC Redundant
Power Limit	Not Set
Dynamic Power	Enabled
OA1 IP Address	16.100.225.122
OA2 IP Address	Not Present
Encl Name	TestEnclosure01
Rack Name	TestRack01
DVD Drive	Connect...
Insight Display PIN#	Not Set

1. Review each setting on the **Enclosure Settings screen** for accuracy.
2. To change any value, move the cursor to the menu option to be edited and press the **OK** button.
3. Change the setting to the appropriate value, move the cursor to **Accept,** and press **OK** to return to the Enclosure Settings menu. Repeat this step until all options on the Enclosure Settings menu are accurate.

TIP:

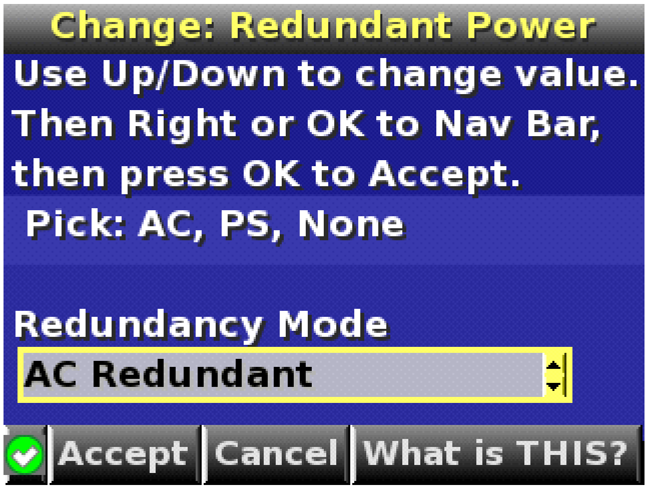
Select the ? icon to access detailed help information about each setting or topic.

Within any menu option, navigate the cursor to **What is This,** and press the **OK** button to view additional information about each setting, option, or alert.

4. When all settings on the Enclosure Settings menu are accurate, move the cursor to **Accept All,** and press **OK** to accept the current settings.

   You can change the following options in the Enclosure Settings screen:

   - **Power Mode—**The default setting is AC Redundant. The following selections are valid:
     - AC Redundant
     - Power Supply Redundant
     - None



Change: Redundant Power

Use Up/Down to change value. Then Right or OK to Nav Bar, then press OK to Accept.

Pick: AC, PS, None

Redundancy Mode: AC Redundant

- **Power Limit—**The default setting is Not Set. You can change the limit by increments of 50 Watts.

CAUTION:

When calculating the Power Limit Watts AC value, derate the circuit to 80% of the maximum to prevent tripping the circuit breaker (United States only).

If your facility cannot support the calculated peak Watts AC, set the Power Watts AC value to match the capability of your facility.

- **Dynamic Power—**The default setting is Disabled. The following selections are valid:
    - **Enabled—**Some power supplies can be placed on standby to automatically increase overall enclosure power subsystem efficiency.
    - **Disabled—**All power supplies share the load. The power subsystem efficiency varies based on load.

NOTE:

Dynamic Power is supported with all c3000 power supplies. It is supported with all c7000 power supplies except those operating with low-line input voltage (nominal 100-120V AC).

- **OA1 IP Addr—**The default setting is DHCP. If no IP address is received, the IP address is 0.0.0.0. The IP address, mask, and gateway are set within this option.
- **OA2 IP Addr—**If this module is present, the default setting is DHCP. If no IP address is received, the IP address is 0.0.0.0. If only one Onboard Administrator module is installed, the screen displays "Not Present."
- **Enclosure Name—**The default setting is a unique factory-assigned name. The accepted character values are 0–9, A–Z, a–z, -, _ and □. The □ symbol is used to signal the end of the name.

NOTE:

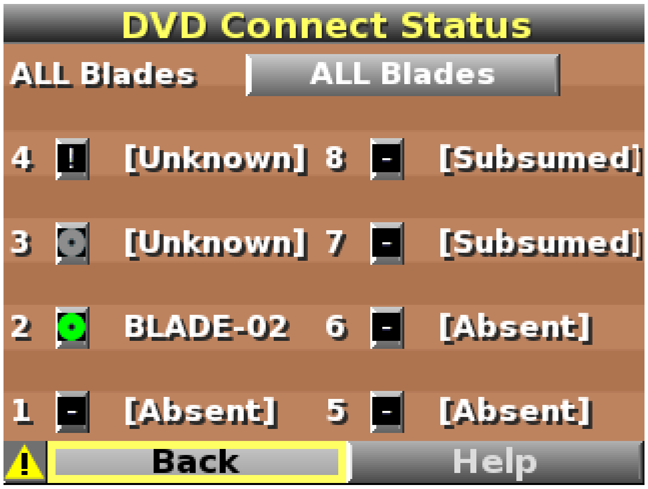
Do not use the □ symbol in the middle of a text field. Entries in text fields will be truncated to the last character before the □ symbol.

TIP:

Select **Clear** from the navigation bar to quickly clear entries in text fields up to the □ symbol.

- **Rack Name—**The default setting is UnnamedRack. The accepted character values are 0–9, A–Z, a–z, -, _ and □. The □ symbol is used to signal the end of the name.
- **DVD Drive—**The default setting is Disconnected on all blades. The DVD Connect Status menu displays the current DVD connection status with an icon.

  To navigate to the Blade DVD Connection menu, select a DVD icon on the DVD Connect menu.



DVD Connect Status

ALL Blades | ALL Blades

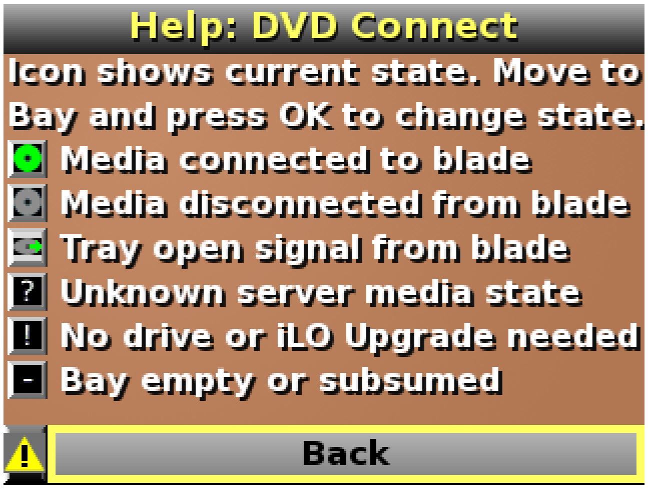
4 ! [Unknown] 8 - [Subsumed]

3 ○ [Unknown] 7 - [Subsumed]

2 ● BLADE-02 6 - [Absent]

1 - [Absent] 5 - [Absent]

To view the various DVD Connect icons and their meanings, click Help.



Help: DVD Connect

Icon shows current state. Move to Bay and press OK to change state.

● Media connected to blade

○ Media disconnected from blade

Tray open signal from blade

? Unknown server media state

! No drive or iLO Upgrade needed

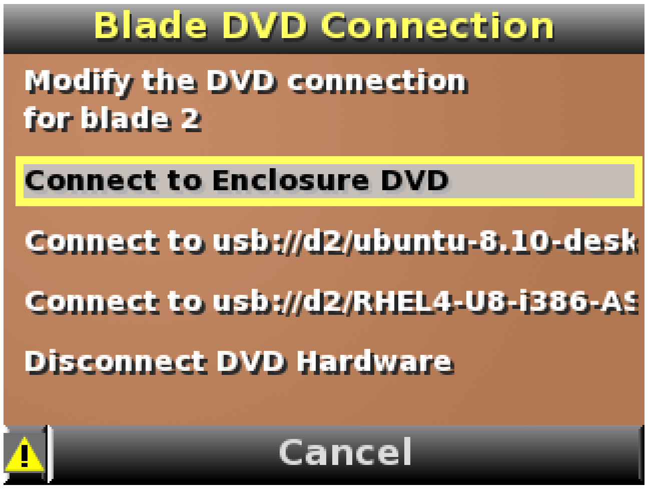
- Bay empty or subsumed

If the Insight Display PIN# is set, the DVD Drive menu is LCD PIN protected. To view or change the Enclosure DVD settings, you must enter the correct PIN at the LCD.

To connect any blade to a CD, DVD, or ISO file, navigate to either an individual server DVD icon or to the **All Blades** button and press **OK.**

The Blade DVD Connection menu indicates whether an Enclosure DVD or ISO file on a USB key is available to connect to the selected servers on the DVD Connect Status menu. If multiple ISO files are found on the USB key, you might see more than one page of options. To view the next page of connection options, select the **Next Page** button.

- **Connect to—**Select one of the currently available options and click **OK** to select that option and navigate to the **Connect: Blade DVD** menu to select whether to reboot the server with this media connected or leave the servers in the existing power state.
- **Disconnect DVD Hardware—**Disconnects the current media connection and returns to the **DVD Connect Status** menu.



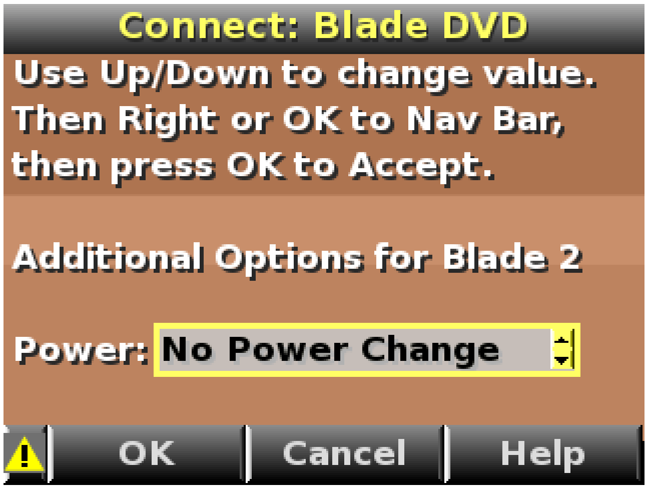
Blade DVD Connection

Modify the DVD connection for blade 2

Connect to Enclosure DVD
Connect to usb://d2/ubuntu-8.10-desk
Connect to usb://d2/RHEL4-U8-i386-AS
Disconnect DVD Hardware
Cancel

The following selections are valid:

- **No Power Change—**Connects the selected media to the server only.
- **Connect and Reboot—**Connects the selected media to the selected servers and reboots selected servers.



Connect: Blade DVD

Use Up/Down to change value. Then Right or OK to Nav Bar, then press OK to Accept.

Additional Options for Blade 2

Power: No Power Change

5. To accept all the settings and continue, navigate to the **Accept All** button at the bottom of the Enclosure Settings screen, and press **OK**.

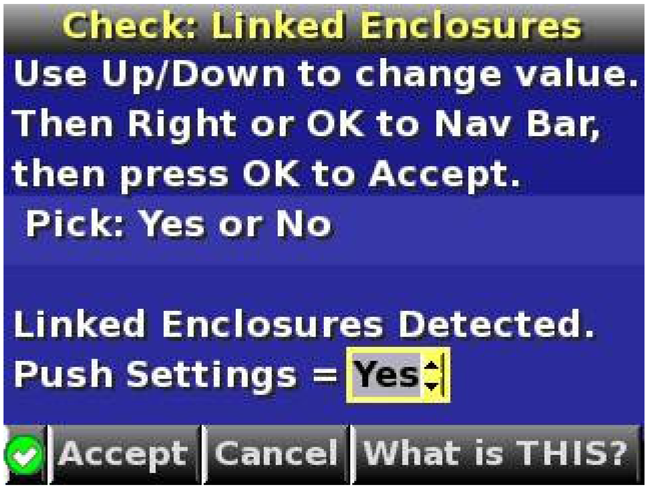
   If the Onboard Administrator module detects other enclosures, the message "Linked enclosures detected" appears.

6. Use the up and down arrow buttons to change **Push Settings =** to one of the following values:

   - **Yes—**Copy the configured power settings, rack name, and LCD Lockout PIN (if set) from the Enclosure Settings screen to the detected enclosures.
   - **No—**Continue configuring the current enclosure only. The Insight Display installation wizard must run on each detected enclosure. Select this option if each enclosure requires different power settings.

IMPORTANT:

If your facility uses Static IP addressing for the Onboard Administrator modules, you must manually enter those IP addresses into the Insight Display for each Insight Display separately. You can enter those Onboard Administrator module IP addresses before you send the settings to adjacent enclosures. You can return to the Enclosure Settings menu after the Installation Wizard completes to change the Onboard Administrator module IP addresses, if necessary.



Check: Linked Enclosures

Use Up/Down to change value. Then Right or OK to Nav Bar, then press OK to Accept.

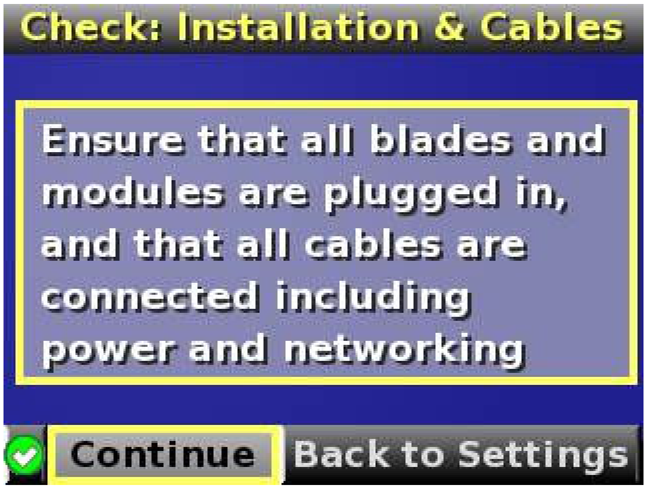
Pick: Yes or No

Linked Enclosures Detected.

Push Settings = Yes

7. Move the cursor to **Accept,** and press the **OK** button.

   The installation wizard displays the Check: Installation and Cables screen.



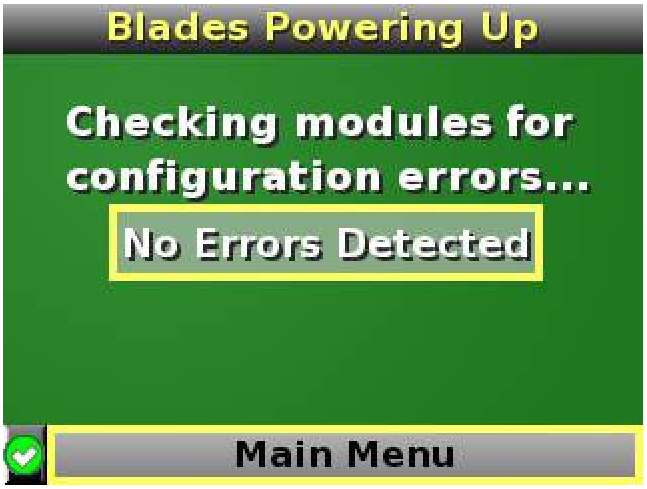
Check: Installation & Cables

Ensure that all blades and modules are plugged in, and that all cables are connected including power and networking

8. Verify all components are installed and connected.
9. To begin checking for configuration and installation errors, select **Continue,** and press **OK**. When **Continue** is selected, the enclosure UID automatically powers off. If **Push Settings = Yes:**

   - The enclosure settings are pushed to adjacent enclosures
   - The installation wizards run on each adjacent enclosure
   - The enclosure UID powers off on the adjacent enclosures

   If no errors are detected, the rear enclosure UID powers off, and the Insight Display screen illuminates green.
10. To return to the Main Menu, press **OK**. Enclosure and blade hardware setup and configuration is complete.



Blades Powering Up

Checking modules for configuration errors...

No Errors Detected

IMPORTANT:

If errors are detected, the Insight Display screen illuminates amber, and the Health Summary screen displays. For more information on troubleshooting configuration errors, see **Insight Display errors**.

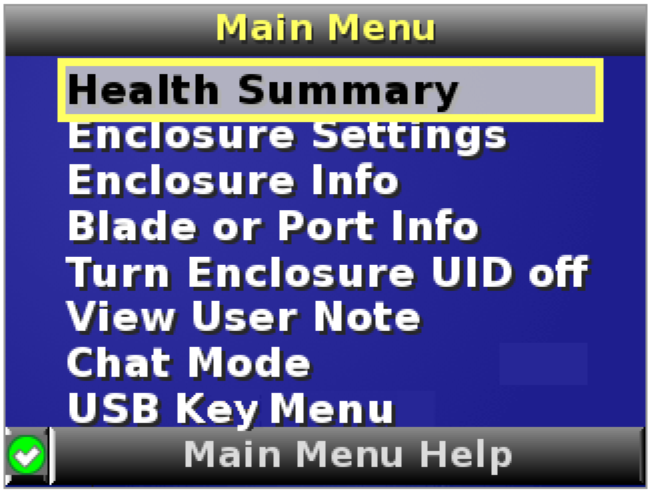
All configuration errors prevent the operation of the enclosure and should be corrected immediately.

11. Open a browser and connect to the active Onboard Administrator module using the Onboard Administrator IP address that was configured during the Insight Display installation wizard process.
12. Enter the user name and password from the tag supplied with the Onboard Administrator module to access the remote Onboard Administrator web interface and complete the Onboard Administrator first time installation wizard.

Navigating the Insight Display

Navigate through the menus and selections by using the arrow buttons on the Insight Display panel.

The first menu seen is the Main Menu:



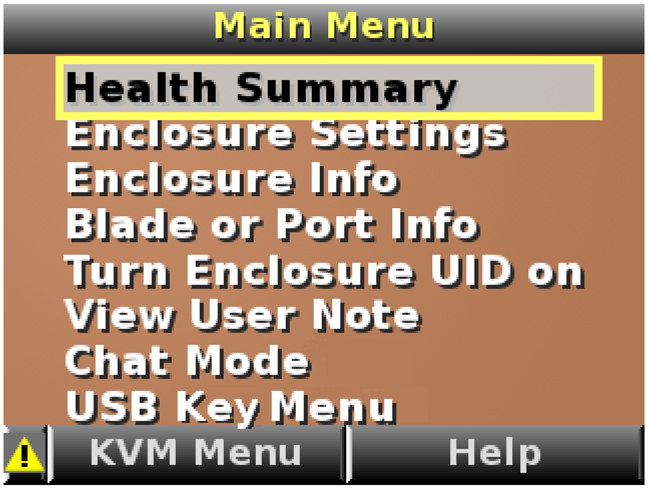
The Main Menu of the Insight Display has the following menu options:

- Health Summary
- Enclosure Settings
- Enclosure Info
- Blade or Port Info

- Turn Enclosure UID on/off
- View User Note
- Chat Mode
- USB Key Menu

If the active Onboard Administrator detects KVM capability, a KVM menu button appears on the navigation bar on the Main Menu. Selecting KVM Menu causes the Insight Display to go blank and activate the VGA connection of Onboard Administrator.

KVM capability is present in the following Main Menu image.



For detailed information regarding the Main Menu of the Insight Display, see the *HPE BladeSystem Insight Display User Guide*.

TIP:

Within any menu option, navigate the cursor to **What is This,** and press the **OK** button to view additional information about each setting, option, or alert.

The navigation bar contains options to:

- Navigate forward and backward through alert screens
- Return to the main menu
- Accept changes to current settings
- Cancel changes to current settings
- Access the Health Summary screen from any screen by selecting the Health Summary icon on the navigation bar

Health Summary screen

The Health Summary screen displays the current condition of the enclosure. The Health Summary screen can be accessed by:

- Selecting **Health Summary** from the main menu
- Selecting the **Health Summary icon** from any Insight Display screen

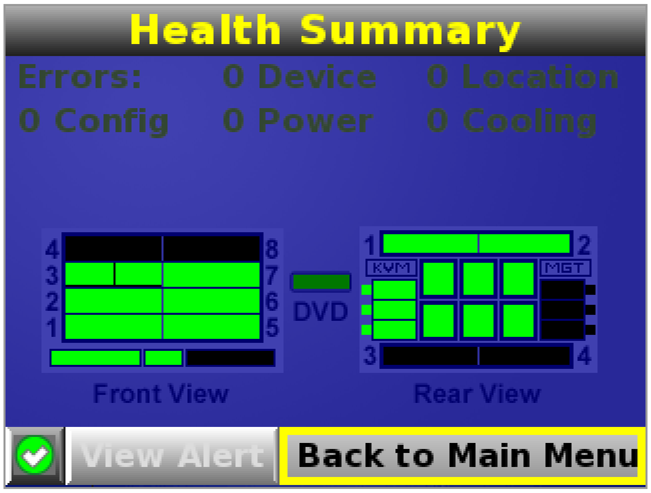
When an error or alert condition is detected, the Health Summary screen displays the total number of error conditions and the error locations.

Select **Next Alert** from the navigation bar, and press the **OK** button to view each individual error condition. The Insight Display displays each error condition in the order of severity. Critical alerts display first (if one exists), followed by caution alerts.

When the enclosure is operating normally, the Health Summary screen displays green. The bright green rectangles are components that are installed and on. A dark green rectangle represents a component that is installed but powered off with no errors. A black rectangle represents an empty bay.

Note: For the c-Class Enclosure DVD feature, a black DVD rectangle indicates no DVD drive is connected to the Onboard Administrator while a dark gray rectangle indicates the DVD drive is present but that no media is present. A dark green rectangle indicates media is present but not actively connected to any server or all connected servers have issued a disk eject command, so the disk can be removed from the drive. A bright green rectangle indicates the media is present in the drive and actively connected to at least one server in the enclosure, and the drive tray is locked.

If there is an error, the Health Summary screen background color changes from green to amber and the error is highlighted with yellow rectangles for caution and red rectangles for failures. Overall enclosure health icons in the bottom left corner of all Insight Display screens indicate the overall enclosure health.



Health Summary

Errors: 0 Device 0 Location

0 Config 0 Power 0 Cooling

Select **View Alert** and press the OK button to display the errors.

Select **Details** to view the details of the error.

Enclosure Settings screen

The Enclosure Settings screen displays the following setting information about the enclosure:

- Power Mode setting
- Power Limit setting
- Dynamic Power setting
- Active and Standby OA IP addresses
- Enclosure Name
- Rack Name
- DVD Drive
-
- Insight Display PIN

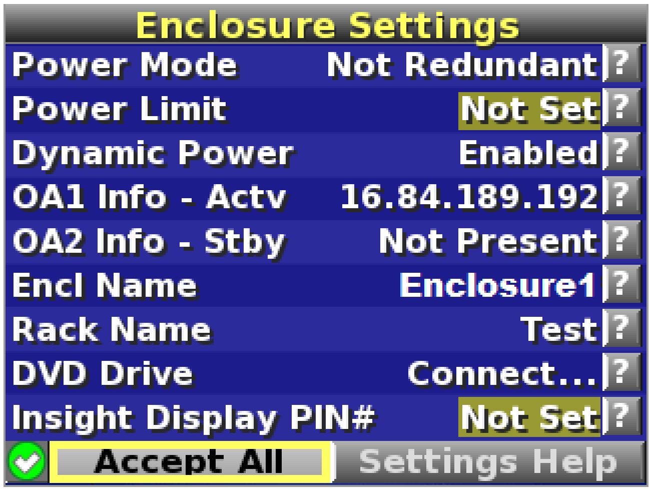
NOTE:

The DVD Drive setting can attach or detach a CD or DVD loaded in the optional c3000 enclosure DVD drive to any or all server blades in the enclosure. This feature can be used to install an operating system or software on the server blade(s). If the optional DVD drive is not present, an external HPE USB DVD drive can be used with this feature instead.

TIP:

Set a PIN to protect the enclosure settings from changes.

Navigate the cursor to a setting or to the ?, and press OK to change the setting or get help on that setting.



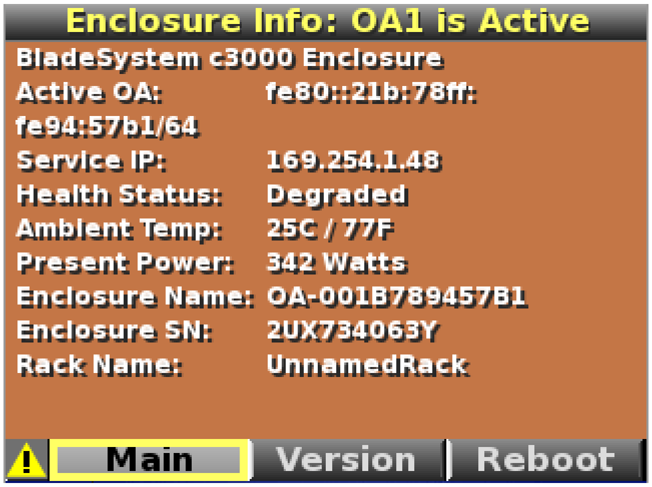
Enclosure Settings

Power Mode	Not Redundant
Power Limit	Not Set
Dynamic Power	Enabled
OA1 Info - Actv	16.84.189.192
OA2 Info - Stby	Not Present
Encl Name	Enclosure1
Rack Name	Test
DVD Drive	Connect...
Insight Display PIN#	Not Set

Enclosure Info screen

The Enclosure Info screen displays information about the enclosure, including:

- Active OA IP address
- Active OA Service IP address
- Current health status
- Current ambient temperature
- Current AC input power
- Name
- Serial number
- Rack name

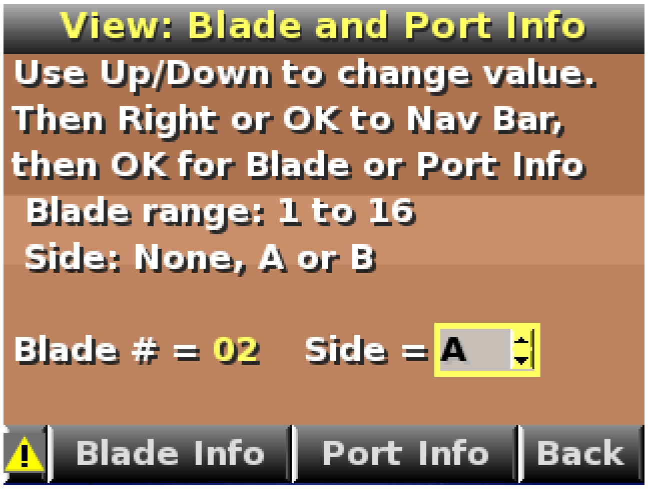


Enclosure Info: OA1 is Active

BladeSystem c3000 Enclosure
Active OA: fe80::21b:78ff:
fe94:57b1/64
Service IP: 169.254.1.48
Health Status: Degraded
Ambient Temp: 25C / 77F
Present Power: 342 Watts
Enclosure Name: OA-001B789457B1
Enclosure SN: 2UX734063Y
Rack Name: UnnamedRack

Blade and Port Info screen

The Blade or Port Info screen displays information about a specific server blade. On the first screen, select the server blade number, then press the OK button. Select **Blade Info** or **Port Info,** and press the OK button.



View: Blade and Port Info

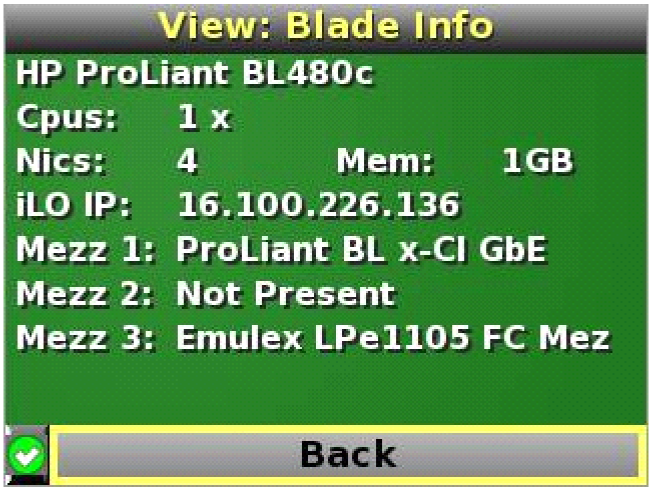
Use Up/Down to change value.
Then Right or OK to Nav Bar,
then OK for Blade or Port Info

Blade range: 1 to 16
Side: None, A or B

Blade # = 02 Side = A

If viewing a BL2x220c server, navigate right to the second selection box and use up or down to select server A or B. The right selection must be N/A to select all other server blade info screens.

To view information about the server blade, select **Blade Info** and press the OK button.

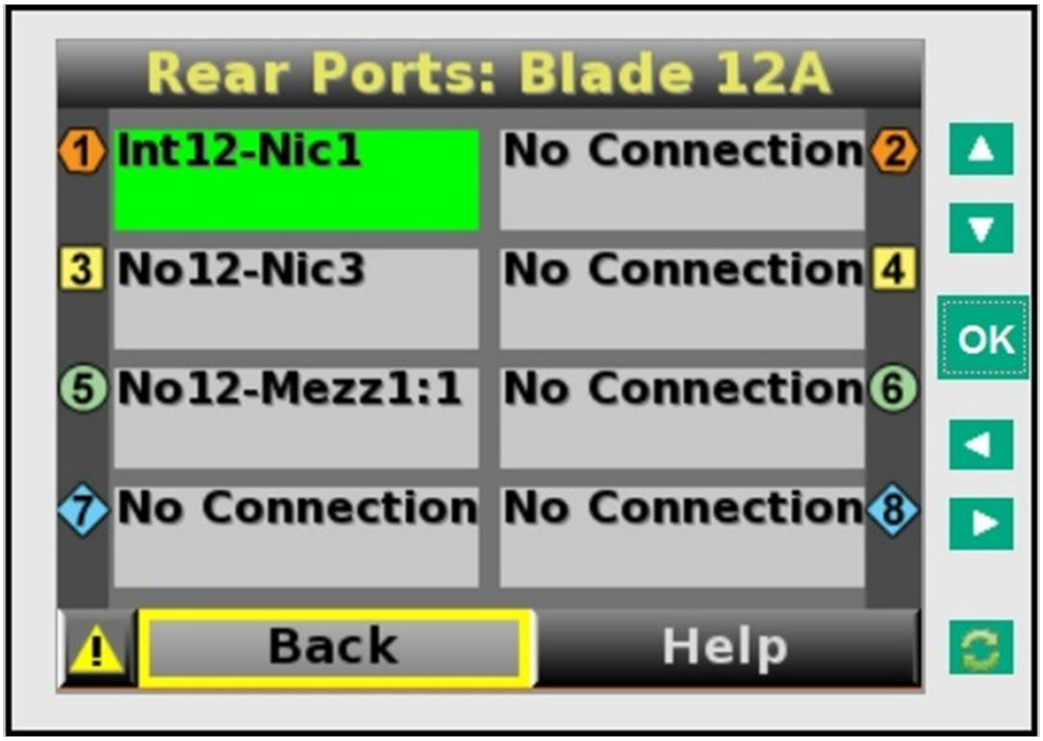


View: Blade Info

HP ProLiant BL480c
Cpus: 1 x
Nics: 4 Mem: 1GB
iLO IP: 16.100.226.136
Mezz 1: ProLiant BL x-CI GbE
Mezz 2: Not Present
Mezz 3: Emulex LPe1105 FC Mez

To view the ports used by a specific server blade, select **Port Info** and press the OK button.

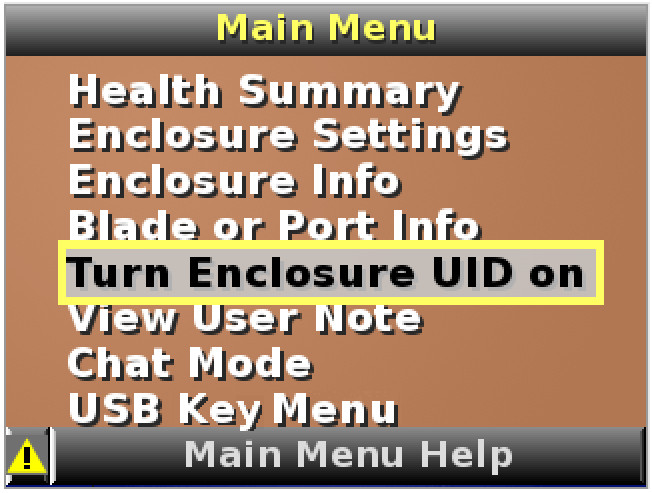
On the full-height server blade shown below, there are four embedded NICs. The other interconnect bays are empty. The four embedded NICs are connected to particular port numbers on the interconnect modules.



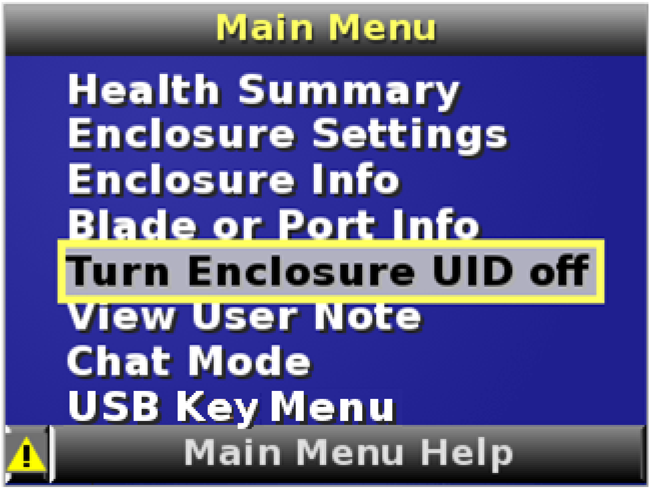
Turn Enclosure UID On/Off screen

The main menu option displays "Turn Enclosure UID Off" when the enclosure UID is active, and displays "Turn Enclosure UID on" when the enclosure UID is off.

Selecting **Turn Enclosure UID On** from the main menu turns on the rear enclosure UID LED and changes the color of the Insight Display screen to blue.

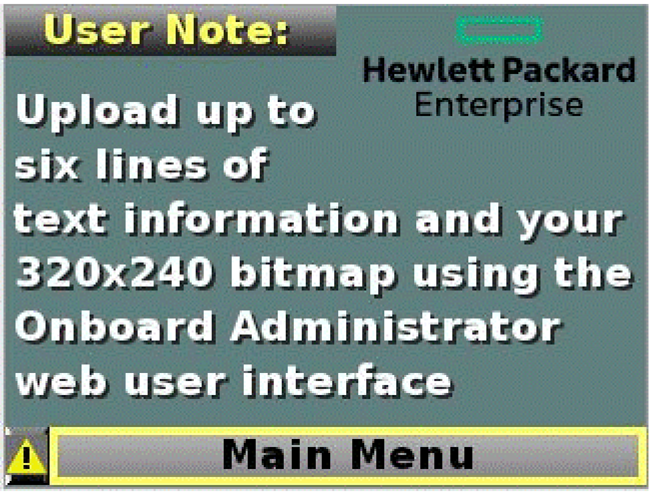


Selecting **Turn Enclosure UID Off** from the main menu turns off the rear enclosure UID LED and changes the color of the Insight Display screen to the current condition.



View User Note screen

The View User Note screen displays six lines of text, each containing a maximum of 25 characters. Use this screen to display helpful information such as contact phone numbers or other information. Change this screen using the remote Onboard Administrator user web interface. Both the background bitmap and the text can be changed.

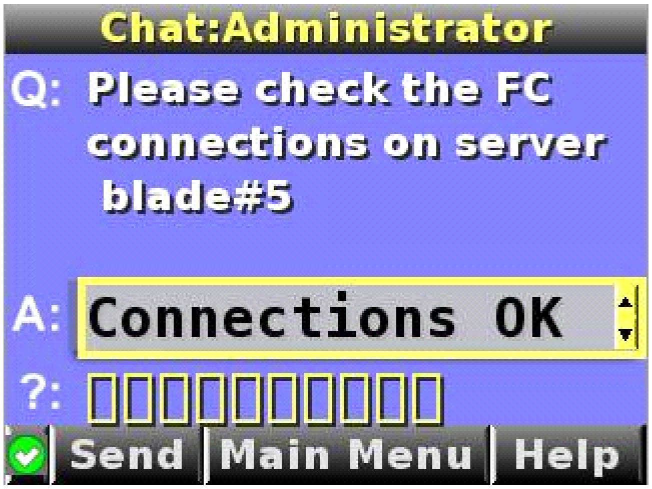


Upload up to
six lines of
text information and your
320x240 bitmap using the
Onboard Administrator
web user interface

Chat Mode screen

The Chat Mode screen is used by the remote administrator who uses the web interface to send a message to an enclosure Insight Display. The technician uses the Insight Display buttons to select from a set of prepared responses, or dials in a custom response message on the ? line. To send a response back to the Administrator, navigate the cursor to **Send,** then press the **OK** button.

The Chat Mode screen has top priority in the Insight Display and will remain on the screen until **Send** is selected. The technician can leave this chat screen temporarily and use the other Insight Display screens, then return to the Chat Mode screen from the Main Menu to send a response. After the response, the Chat Mode screen is cleared. Both the A and ? responses are then displayed to the remote Administrator on the web interface for LCD Chat.



Q: Please check the FC connections on server blade#5

A: Connections OK

?: □□□□□□□□□□

USB Menu screen

Onboard Administrator firmware version 2.30 and later offers added support for the following USB key options:

- Updating OA firmware (from a supported HPE SPP ISO image)
- Restoring OA configuration
- Saving OA Configuration

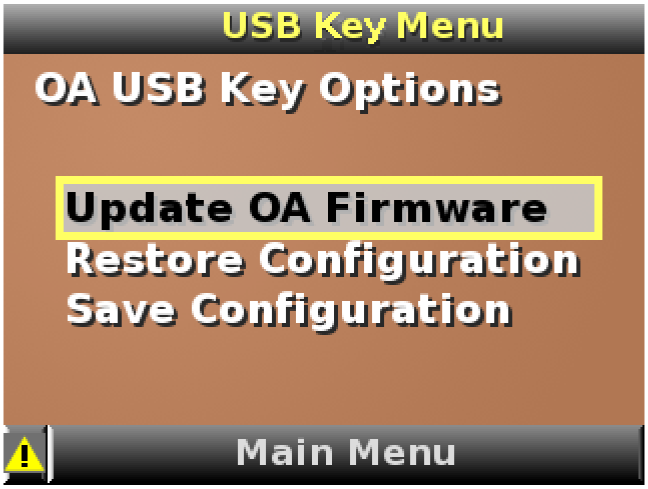
Onboard Administrator supports USB keys formatted with FAT32 or ext2 file systems. The maximum supported file size for USB keys formatted with FAT32 is 4GB. For SPP images greater than 4GB, use an ext2-formatted USB key. The steps for formatting your USB key with an ext2 file system are included at the end of this section.

You can insert a USB key in the port located on the active Onboard Administrator module on the front of the enclosure or a USB port on the optional KVM module.

Accessing the USB Key Menu

Procedure

1. Insert a USB key into Onboard Administrator or optional KVM module.
2. From the Main Menu, select **USB Key Menu**.

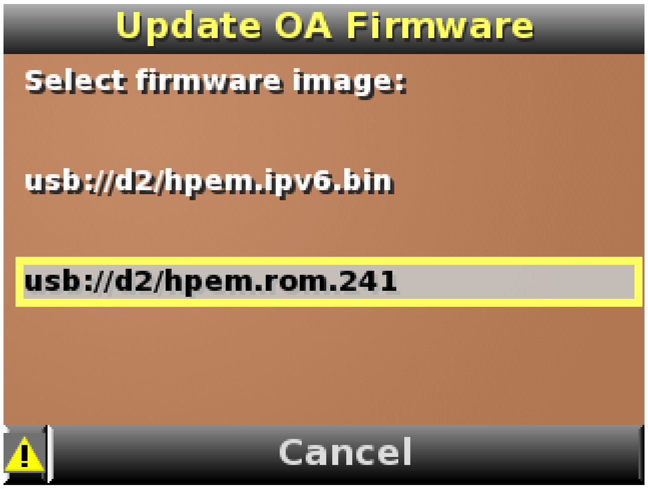


The following selections are available on the USB Key Menu:

- **Update OA Firmware**

  Select this option to upgrade the firmware. The USB key must contain an Onboard Administrator firmware image with a BIN file extension.

  For more information about upgrading Onboard Administrator modules in HPE BladeSystem c3000 and c7000 enclosures, see **Upgrading Onboard Administrator modules in a BladeSystem Enclosure**.



Update OA Firmware

Select firmware image:

usb://d2/hpem.ipv6.bin

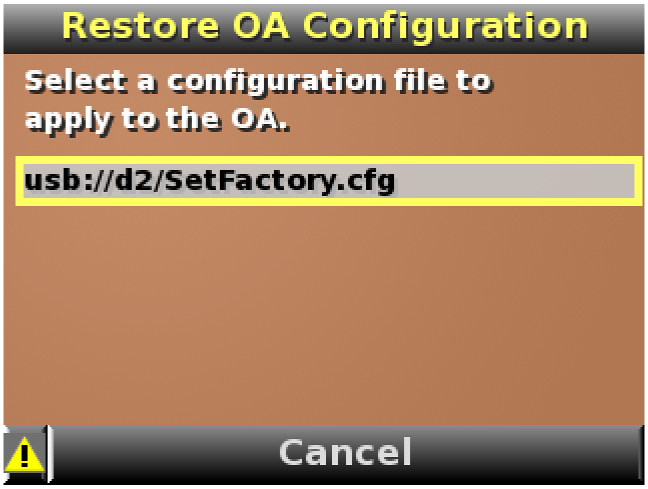
usb://d2/hpem.rom.241

- **Restore Configuration**

  Select this option to upload an enclosure configuration file with .CFG extension.

  The Restore OA Configuration menu lists all the files on the attached USB key with .CFG file extensions. Select the desired configuration file and press **OK**.

  Because the configuration file can modify settings like the Onboard Administrator IP address, be sure to only apply the same file to multiple enclosures if the settings are generic, such as SNMP or LDAP server addresses. Do not apply the same file to multiple enclosures if it contains Onboard Administrator IP address configuration commands or EBIPA IP address commands.



Restore OA Configuration

Select a configuration file to apply to the OA.

usb://d2/SetFactory.cfg

- **Save Configuration**

  Select this option to save the enclosure configuration to a file on the USB key.

Formatting the USB key with an ext2 file system from a Windows PC

Prerequisites

Before formatting the USB key, you must enable your Windows system to support ext2 file systems:

1. Download an `Ext2Fsd-x.xx.exe` file from the **SourceForge website**.
2. Install the downloaded executable file.

Once these initial steps are complete, your Windows system should be able to recognize ext2-formatted USB keys and allow writing to such USB keys.

Procedure

1. Download the Gparted Live CD ISO image from the **GNOME Partition Editor website**. The ISO image name is usually of the format `gparted-live-x.xx.x-x-i586.iso`.
2. Download a VM player of your choice and install it on your Windows system. For example, install the VMware player available on the **VMware website**.
3. Insert the USB key into your PC.
4. Using your VM player, create a Linux kernel VM configured with default configurations. (The Linux version of the kernel should comply with the Linux distribution provided by the Gparted Live CD.)
5. Set the Gparted Live CD ISO image as the CD/DVD option for your VM, and then start the VM.
6. To format your USB key to ext2, use the appropriate GUI options on the Gparted VM.
7. Remove the USB key from the VM.
8. Shut down the VM from the VM player.
9. To confirm that the USB key is now formatted to ext2, check the properties of the USB key from your PC.

Copying the SPP ISO image onto the USB key

Procedure

1. Install the ext2 file-system drivers for Windows. Drivers are located at the **SourceForge website**.

   Your Windows systems should now detect the ext2-formatted USB drive.
2. Load the SPP ISO image onto the USB key.

KVM Menu screen

If the Enclosure KVM feature is supported, the Insight Display Main Menu displays the **KVM Menu** button. Select this button to deactivate the Insight Display and activate the VGA connector on the KVM module. Only one of the two interfaces can be active at a time. For more information, see **Enclosure KVM**.

Insight Display errors

The enclosure installation is successful when all errors are corrected. The errors in the following sections are specific to installation and initial configuration of the enclosure. To clear errors that occur after initial powerup and configuration, see the Onboard Administrator User Guide for information.

The following types of errors can occur when installing and configuring the enclosure:

- **Power errors**
- **Cooling errors**
- **Location errors**
- **Configuration errors**
- **Device failure errors**

When the enclosure UID LED is off, the Insight Display is illuminated amber when any error condition exists. The navigation bar displays the following selections when an error condition exists:

- Health summary icon—Displays the Health Summary screen.
- Fix THIS—Suggests corrective action to clear the current error.

- Next Alert—Displays the next alert, or if none exist, displays the Health Summary screen.
- Previous Alert—Displays the previous alert.

Power errors

Power errors can occur because of insufficient power to bring up an enclosure. Power errors can occur on server blades, storage blades, or interconnect modules.

To correct a power error:

1. Use the arrow buttons to navigate to **Fix This,** and press **OK.**
2. Review and complete the corrective action suggested by the Insight Display. In most cases, you must either add power supplies to the enclosure or remove the indicated components.

Cooling errors

Cooling errors occur when too few fans are installed in the enclosure or when the existing fans are not installed in an effective configuration. Cooling errors can occur on server blades, storage blades, or interconnect modules.

To correct a cooling error:

1. Use the arrow buttons to navigate to **Fix This,** and press **OK.**
2. Review and complete the corrective action suggested by the Insight Display. In most cases, you must either add fans to the enclosure, correct the fan configuration, or remove the indicated components.

Location errors

Location (installation) errors occur when the component is not installed in the appropriate bay. Location errors can occur on server blades, storage blades, power supplies, and fans.

To correct a location error:

1. Use the arrow buttons to navigate to **Fix This,** and press **OK.**
2. Review and complete the corrective action suggested by the Insight Display. Remove the indicated component, and install it into the correct bay. The Insight Display will indicate the correct bay number.

Configuration errors

Configuration errors can occur if the interconnect modules are installed in the wrong bays or if mezzanine cards are installed in the wrong connectors in the server blade. Configuration errors can occur on server blades and interconnect modules.

To correct a configuration error:

1. Use the arrow buttons to navigate to **Fix This,** and press **OK.**
2. Review and complete the corrective action suggested by the Insight Display. Depending on the error received, do one of the following:
    - Remove the indicated interconnect module and install it into the correct bay (the Insight Display indicates the correct bay).
    - Remove the server blade to correct the mezzanine card installation (the Insight Display will indicate the correct bay). For information on installing the mezzanine card, see the server-specific user guide on the Documentation CD.

Device failure errors

Device failure errors occur when a component has failed. Device failure errors can occur on all components, including:

- Server blades
- Storage blades
- Power supplies
- Interconnect modules
- Onboard Administrator modules
- Fans
- AC power inputs

To correct a device failure error:

1. Use the arrow buttons to navigate to **Fix This,** and press **OK**.
2. Review and complete the corrective action suggested by the Insight Display. In most cases, you must remove the failed component to clear the error.
3. Replace the failed component with a spare, if applicable.

NOTE:

If the device failure error is an AC power input failure error, you must have the failed AC input repaired to clear the error.

Enclosure KVM

The Enclosure KVM feature enables the Onboard Administrator to switch between server video consoles, using only an attached VGA monitor, USB keyboard, and USB mouse without requiring a PC. In addition to launching and running server video consoles, the Enclosure KVM Menu provides health status of each server and enables you to power servers on and off and attach an enclosure DVD to those servers.

The Insight Display is deactivated (appears blank) while Enclosure KVM is active. The Enclosure KVM Menu includes a button to access the Insight Display screens on the VGA monitor using the keyboard cursor keys.

The Enclosure KVM Menu also includes a button to select the Onboard Administrator CLI console. After logging in to the Onboard Administrator CLI console using Enclosure KVM, you can access all the CLI functions.

On the c3000 Enclosure, the KVM feature requires that the optional KVM Module be installed in the rear of the enclosure. This KVM Module provides a VGA connector and two additional USB 2.0 connectors. For the c7000 Enclosure, this feature requires the Onboard Administrator module with VGA connector.

Methods for using the Enclosure KVM feature

Use the Enclosure KVM by choosing one of the following methods:

- Connect the VGA connector directly to a VGA monitor, and then connect a keyboard and a mouse to the USB connectors.
- Connect the VGA connector to an HPE KVM Switch using a CAT5 KVM USB adapter, and then connect the USB cable from the adapter to the Onboard Administrator USB connector.

NOTE:

If character repeat problems occur when typing in a GUI text console on a Linux system, the following configuration settings might require modification:

- Set the keyboard repeat/delay setting to 1000 msec (kbdrate –d 1000 in the server init script).
- Configure the GUI autorepeat rate to 1 second.

Accessing the KVM menu

Access the KVM Menu by choosing one of the following options:

- From a USB keyboard connected to the KVM module, press **Prt Scrn** or **SysReq**.
- From a VGA monitor with a keyboard and mouse, press **Prt Scrn**.
- If the KVM module is connected to a Hewlett Packard Enterprise rack KVM switch using a VGA or USB adapter, press **Prt Scrn** to activate the rack KVM selection menu, and press **Prt Scrn** again to display the Enclosure KVM Menu.

Select the Hewlett Packard Enterprise rack KVM port connected to the enclosure, and then press **Enter** to select the Enclosure KVM Menu. If the screen is blank, touch any key on the keyboard to activate the KVM Menu and deactivate the enclosure Insight Display .

The Insight Display appears blank when the Enclosure KVM Menu is active.

Returning to the KVM menu from another interface

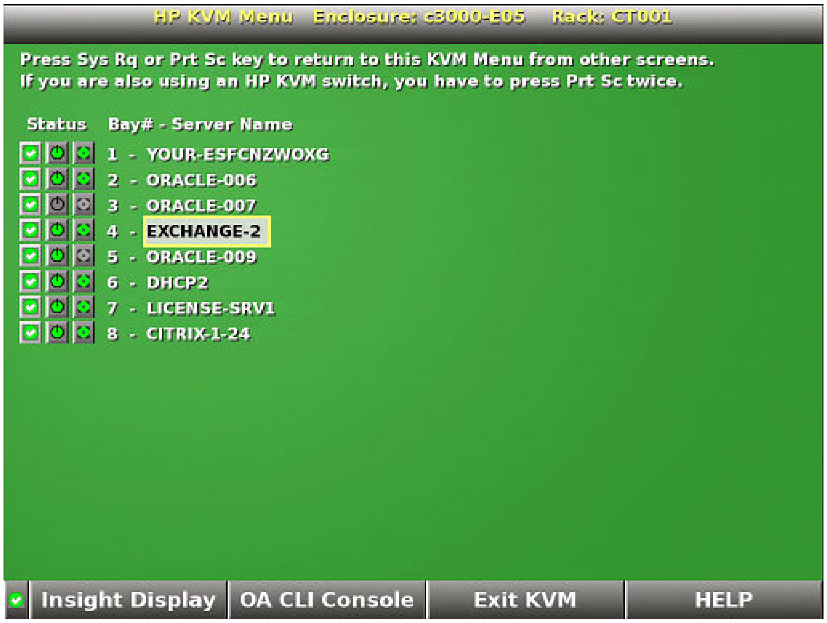
To return to the KVM Menu from a server console, Insight Display, or the OA CLI display, press the **Prt Scrn** key on the USB keyboard.

Returning to Insight Display from the KVM menu

To restore the Insight Display and blank the KVM Menu (A slight delay may occur.), press any Insight Display button, or select **Exit KVM** on the KVM Menu.

Navigating the KVM menu

The following figure shows the KVM Menu:



HP KVM Menu   Enclosure: c3000-E05   Rack: CT001

Press Sys Rq or Prt Sc key to return to this KVM Menu from other screens.
If you are also using an HP KVM switch, you have to press Prt Sc twice.

Status   Bay# - Server Name

1 - YOUR-ESFCNZWOXG
2 - ORACLE-006
3 - ORACLE-007
4 - EXCHANGE-2
5 - ORACLE-009
6 - DHCP2
7 - LICENSE-SRV1
8 - CITRIX-1-24

To navigate the KVM Menu, use the keyboard arrow keys. To select a menu action, press the keyboard **Enter** key.

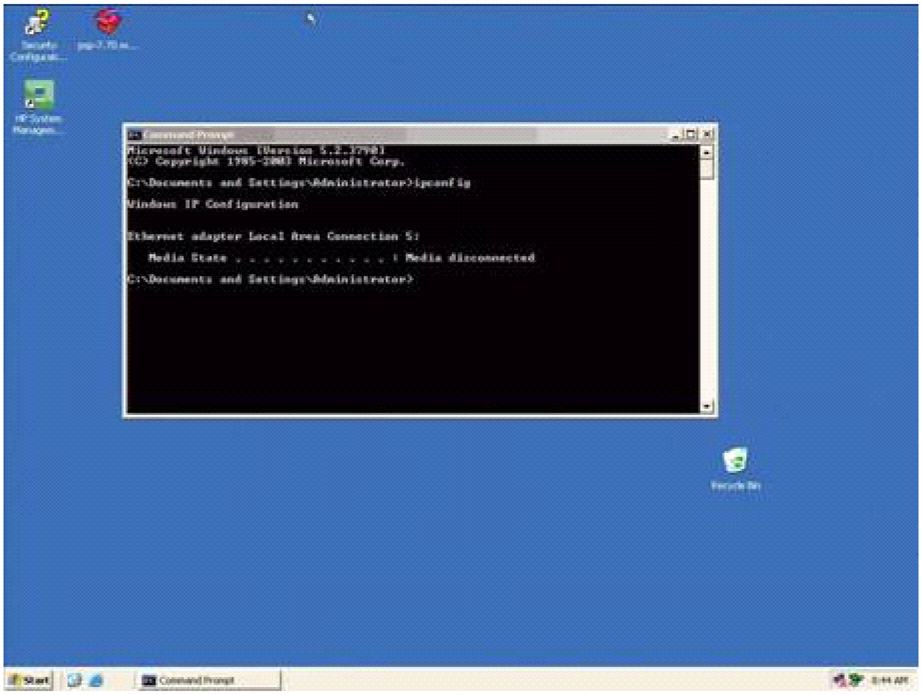
The available actions include:

- Power icon—Changes the power state for the server.
- DVD icon—Changes the Enclosure DVD state for the server.
- Server Name—Connects to the server full-screen KVM console, including keyboard and mouse support. To return to the KVM Menu, press the **Prt Scrn** or **SysRq** key.
- Insight Display—Uses the KVM monitor and the keyboard arrow and **Enter** keys to operate the Insight Display.
- OA CLI Console—Uses the KVM monitor and keyboard to access the OA CLI commands.
- Exit KVM—Disables the KVM monitor and enables the enclosure Insight Display.
- Help—Displays the HPE KVM Help screen with information about the status icons and KVM operation.

If the LCD PIN is set, all the server power and server DVD controls are LCD PIN-protected. Server Console and Onboard Administrator CLI are protected by user logins.

The KVM Menu contains the following options:

- Server Console—Select a server console by selecting the server name. The selected server console is full screen graphics or text based on the current environment on that server. All KVM keyboard keystrokes except PrtSc are sent to the server, along with the KVM mouse. To exit the server console and return to the KVM Menu, press **Prt Scrn**.

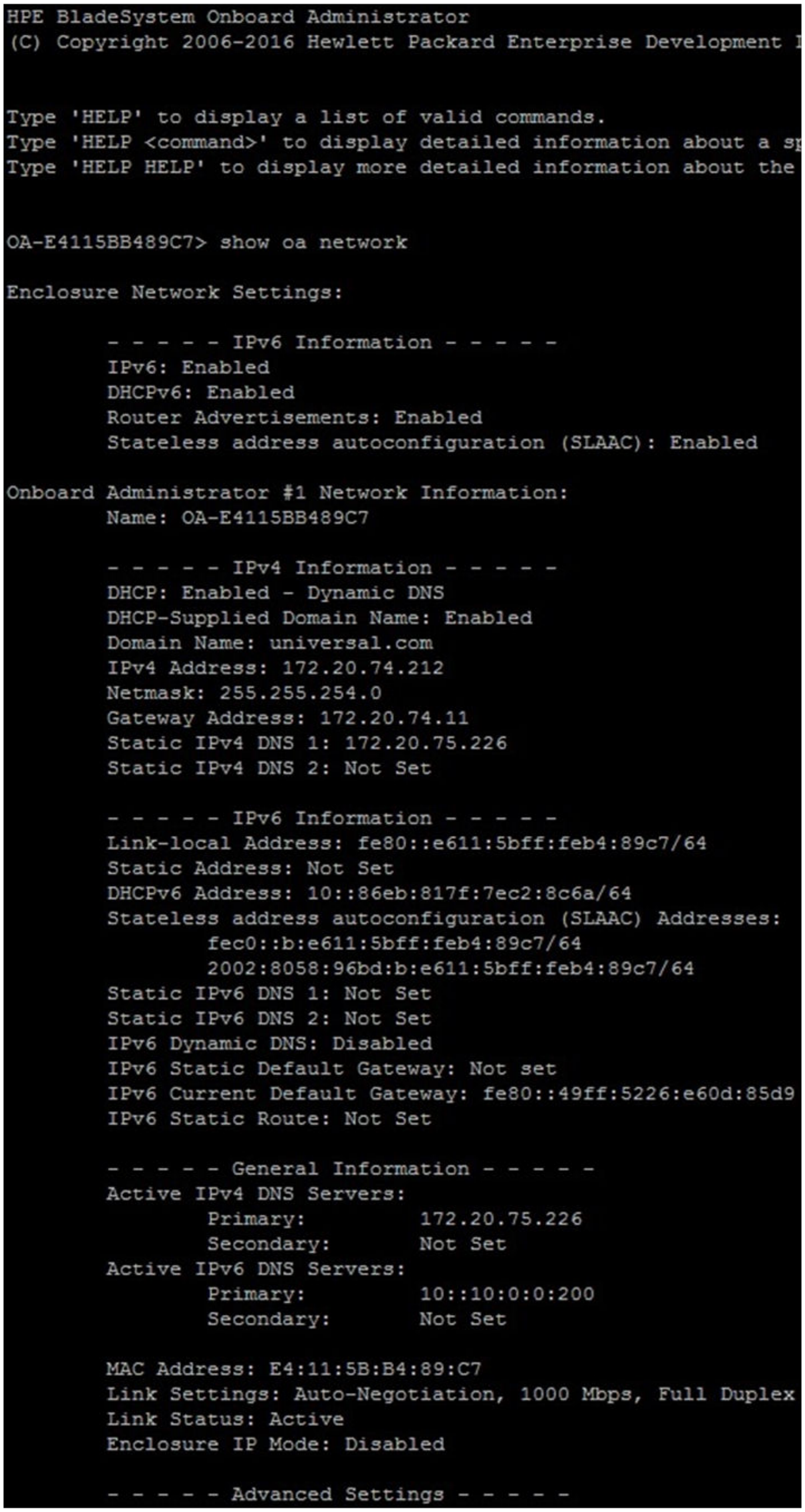


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 5:

   Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>
```

NOTE:

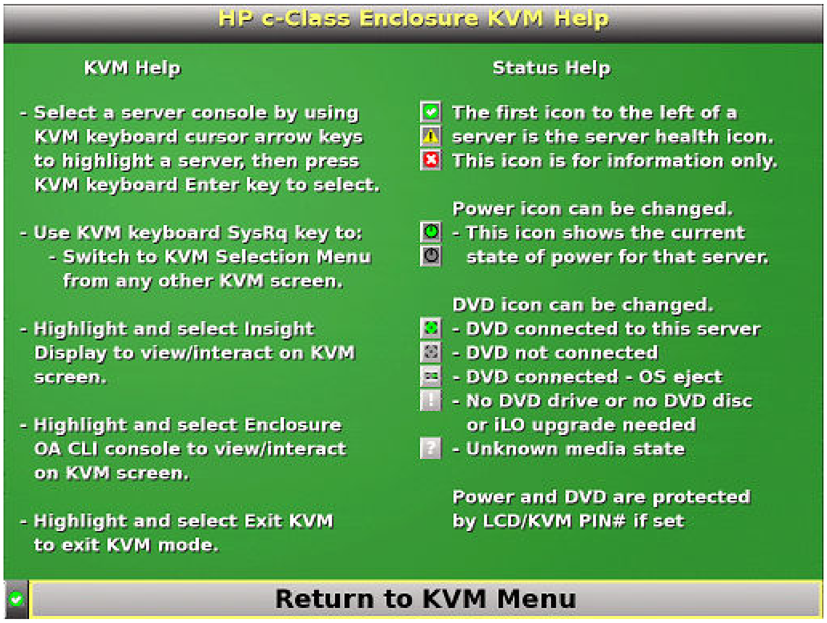
For resolutions 1024x768 through 1600x1200, the screen resolution matches the server console screen resolution. Server console resolutions below 1024x768 result with a display on a portion of the Onboard Administrator KVM screen in 1024x768 mode. For server console resolutions above 1600x1200, a warning message displays, and you are brought back to the Enclosure KVM Menu screen.

- Server Power—Select this power icon for a server to change the server power state.
- Server DVD—Select this DVD icon for a server to change the enclosure DVD connection for this server.
- Server Health—Select this health icon to display the current health state for that server.
- Insight Display—Select the Insight Display button to access Insight Display screens from the KVM Menu.
- OA CLI—Select **OA CLI** to launch the Onboard Administrator CLI. Log in to the Onboard Administrator using the KVM keyboard. This launches a full screen text console to the active Onboard Administrator CLI. To exit the Onboard Administrator CLI console and return to the KVM Menu, press **Prt Scrn**.



```
HPE BladeSystem Onboard Administrator
(C) Copyright 2006-2016 Hewlett Packard Enterprise Development I


Type 'HELP' to display a list of valid commands.
Type 'HELP <command>' to display detailed information about a sp
Type 'HELP HELP' to display more detailed information about the


OA-E4115BB489C7> show oa network

Enclosure Network Settings:

        - - - - - IPv6 Information - - - - -
        IPv6: Enabled
        DHCPv6: Enabled
        Router Advertisements: Enabled
        Stateless address autoconfiguration (SLAAC): Enabled

Onboard Administrator #1 Network Information:
        Name: OA-E4115BB489C7

        - - - - - IPv4 Information - - - - -
        DHCP: Enabled - Dynamic DNS
        DHCP-Supplied Domain Name: Enabled
        Domain Name: universal.com
        IPv4 Address: 172.20.74.212
        Netmask: 255.255.254.0
        Gateway Address: 172.20.74.11
        Static IPv4 DNS 1: 172.20.75.226
        Static IPv4 DNS 2: Not Set

        - - - - - IPv6 Information - - - - -
        Link-local Address: fe80::e611:5bff:feb4:89c7/64
        Static Address: Not Set
        DHCPv6 Address: 10::86eb:817f:7ec2:8c6a/64
        Stateless address autoconfiguration (SLAAC) Addresses:
                fec0::b:e611:5bff:feb4:89c7/64
                2002:8058:96bd:b:e611:5bff:feb4:89c7/64
        Static IPv6 DNS 1: Not Set
        Static IPv6 DNS 2: Not Set
        IPv6 Dynamic DNS: Disabled
        IPv6 Static Default Gateway: Not set
        IPv6 Current Default Gateway: fe80::49ff:5226:e60d:85d9
        IPv6 Static Route: Not Set

        - - - - - General Information - - - - -
        Active IPv4 DNS Servers:
                Primary:         172.20.75.226
                Secondary:       Not Set
        Active IPv6 DNS Servers:
                Primary:         10::10:0:0:200
                Secondary:       Not Set

        MAC Address: E4:11:5B:B4:89:C7
        Link Settings: Auto-Negotiation, 1000 Mbps, Full Duplex
        Link Status: Active
        Enclosure IP Mode: Disabled

        - - - - - Advanced Settings - - - - -
```

- Help—Select **Help** to view the KVM help information.



HP c-Class Enclosure KVM Help

KVM Help

- Select a server console by using KVM keyboard cursor arrow keys to highlight a server, then press KVM keyboard Enter key to select.
- Use KVM keyboard SysRq key to:
  - Switch to KVM Selection Menu from any other KVM screen.
- Highlight and select Insight Display to view/interact on KVM screen.
- Highlight and select Enclosure OA CLI console to view/interact on KVM screen.
- Highlight and select Exit KVM to exit KVM mode.

Status Help

The first icon to the left of a server is the server health icon. This icon is for information only.

Power icon can be changed.
- This icon shows the current state of power for that server.

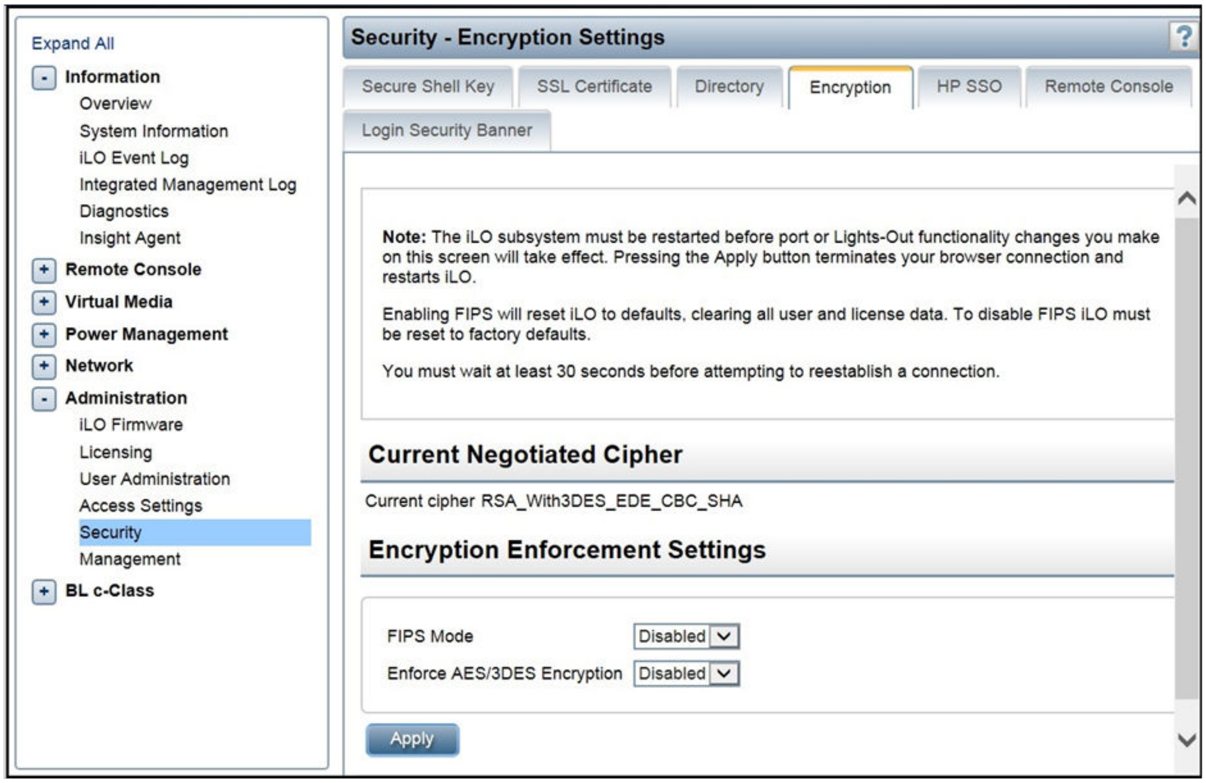
DVD icon can be changed.
- DVD connected to this server
- DVD not connected
- DVD connected - OS eject
- No DVD drive or no DVD disc or iLO upgrade needed
- Unknown media state

Power and DVD are protected by LCD/KVM PIN# if set

NOTE: When the Onboard Administrator is in FIPS Mode, iLO security access setting, Enforce AES/3DES Encryption, must be enabled.

To change the iLO setting, navigate to **Administration > Security > Encryption**.

KVM connection to iLO2 is not supported while in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug.



Security - Encryption Settings

Note: The iLO subsystem must be restarted before port or Lights-Out functionality changes you make on this screen will take effect. Pressing the Apply button terminates your browser connection and restarts iLO.

Enabling FIPS will reset iLO to defaults, clearing all user and license data. To disable FIPS iLO must be reset to factory defaults.

You must wait at least 30 seconds before attempting to reestablish a connection.

Current Negotiated Cipher

Current cipher RSA_With3DES_EDE_CBC_SHA

Encryption Enforcement Settings

FIPS Mode: Disabled

Enforce AES/3DES Encryption: Disabled

First Time Setup Wizard

Prerequisites to running the First Time Setup Wizard

Before running the First Time Setup Wizard, complete the following tasks:

Procedure

1. Install the Onboard Administrator modules.
2. Connect the Onboard Administrator modules to the network.
3. Complete the Insight Display installation wizard. At a minimum, configure the active Onboard Administrator IP address.
4. Run the Insight Display installation.

Signing in to Onboard Administrator

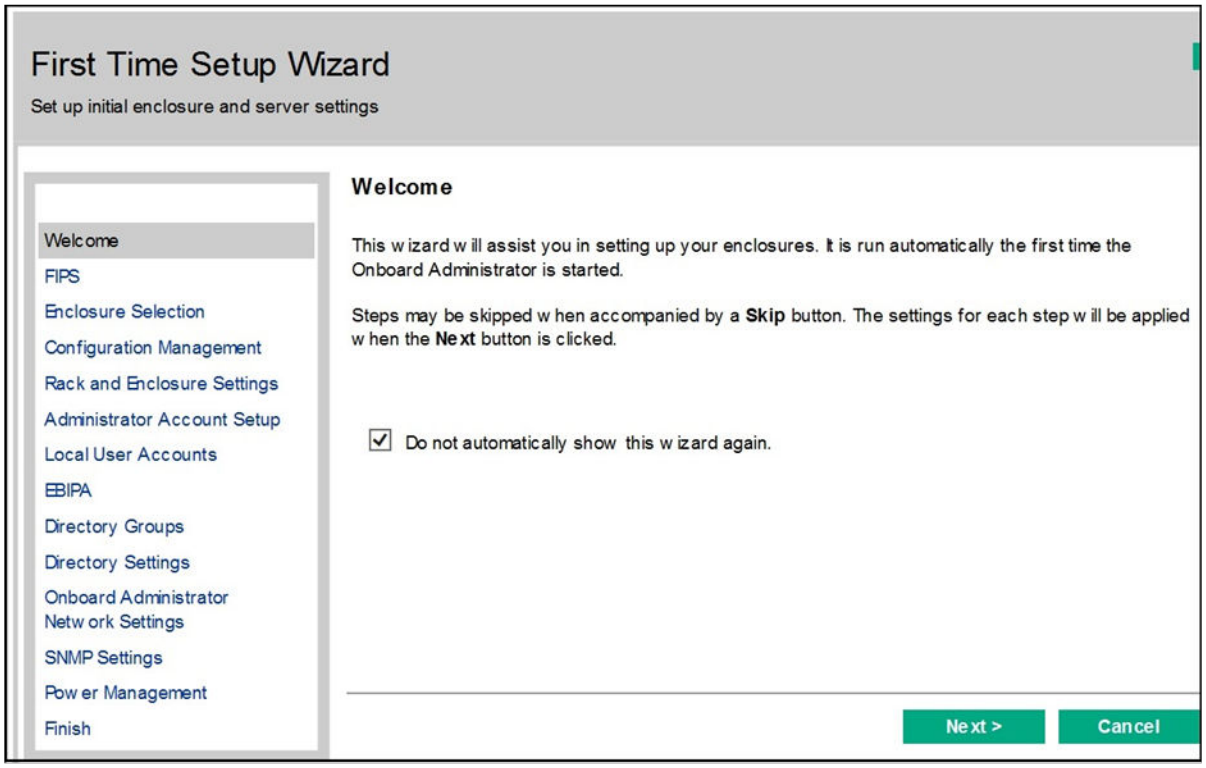
Procedure

1. Open a browser and connect to the active Onboard Administrator using the IP address that was configured during the Insight Display installation wizard process.
2. Enter the user name and initial administration password for your Onboard Administrator account found on the tag attached to the Onboard Administrator.

The first time you sign in, the Onboard Administrator automatically runs the First Time Setup Wizard.

To navigate through the setup wizard, click **Next** to save your changes and go to the next step. Click **Skip** if you want to leave the step without saving changes.

You can return to previous wizard steps by selecting them in the left tree view. You can also run the wizard again at any time by selecting it from the Wizards menu.



First Time Setup Wizard

Set up initial enclosure and server settings

Welcome

This wizard will assist you in setting up your enclosures. It is run automatically the first time the Onboard Administrator is started.

Steps may be skipped when accompanied by a **Skip** button. The settings for each step will be applied when the **Next** button is clicked.

☑ Do not automatically show this wizard again.

Causes for possible issues when signing in to Onboard Administrator

The following is a list of reasons why issues might occur when signing in:

- You are not entering the correct to sign in. Passwords are case-sensitive.
- The account information you are entering has not been set up for Onboard Administrator.
- The user name you are entering has been deleted, disabled, or locked out.
- The password for the account must be changed.
- You are attempting to sign in from an IP address that is not valid for the specified account.

If you have checked these issues and continue to have problems signing in, contact your administrator.

User Preferences

To change the display language, select a display language from the dropdown list, and then click **Apply.** The selected language overrides the browser's current language preference setting and persists with subsequent GUI sessions with the same Onboard Administrator. However, the setting does not apply for GUI sessions with other Onboard Administrators. (The setting relies on a cookie that is valid only for the current Onboard Administrator IP address. If the IP address changes, the setting must be applied again from the new address.)

If you want the language to display for connections to other Onboard Administrator GUIs using this browser:

1. Add the language to the top of the browser's preferred language list.
2. On the Onboard Administrator User Preferences screen, select "Use browser settings" from the dropdown list.
3. Refresh the display language by clicking **Apply**. The corresponding language pack must be installed on the other Onboard Administrators; for more information about installing a language pack, see the **Active Onboard Administrator Language Pack tab**.

   If "Use browser settings" is already set, refresh the display language without changing the setting by clicking **Refresh**.

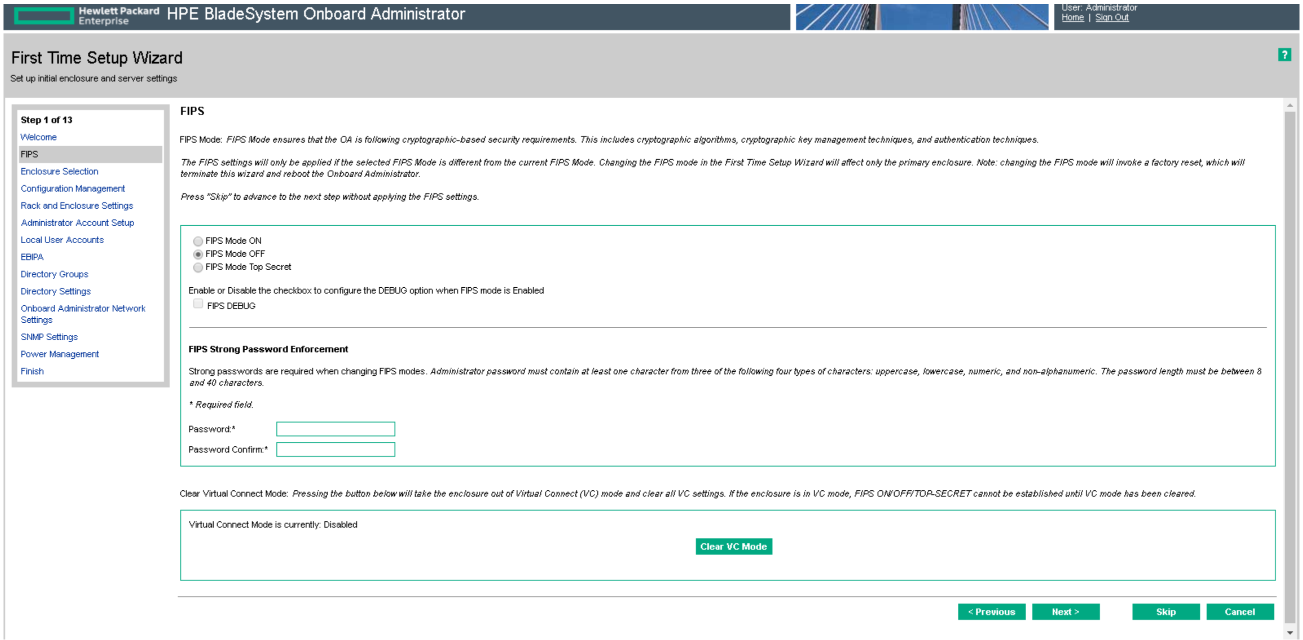
The User Preferences dropdown list includes only those languages that have been installed or are embedded on the Onboard Administrator. If you set the browser language preference to a language that is not listed, the Onboard Administrator GUI will not use the browser language setting; the GUI uses the default language (English) instead.

NOTE:

If the display language does not load properly, clear the browser cache and refresh the application by refreshing or reloading the browser.

If you are using an installed language pack with the Onboard Administrator GUI, and your browser does not display all characters correctly, make sure the operating system has the corresponding language support installed.

FIPS



Hewlett Packard Enterprise
HPE BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
?

First Time Setup Wizard

Set up initial enclosure and server settings

FIPS

FIPS Mode: *FIPS Mode ensures that the OA is following cryptographic-based security requirements. This includes cryptographic algorithms, cryptographic key management techniques, and authentication techniques.*

The FIPS settings will only be applied if the selected FIPS Mode is different from the current FIPS Mode. Changing the FIPS mode in the First Time Setup Wizard will affect only the primary enclosure. Note: changing the FIPS mode will invoke a factory reset, which will terminate this wizard and reboot the Onboard Administrator.

Press "Skip" to advance to the next step without applying the FIPS settings.

○ FIPS Mode ON
● FIPS Mode OFF
○ FIPS Mode Top Secret

Enable or Disable the checkbox to configure the DEBUG option when FIPS mode is Enabled

□ FIPS DEBUG

FIPS Strong Password Enforcement

Strong passwords are required when changing FIPS modes. *Administrator password must contain at least one character from three of the following four types of characters: uppercase, lowercase, numeric, and non-alphanumeric. The password length must be between 8 and 40 characters.*

** Required field.*

Password:*

Password Confirm:*

Clear Virtual Connect Mode: *Pressing the button below will take the enclosure out of Virtual Connect (VC) mode and clear all VC settings. If the enclosure is in VC mode, FIPS ON/OFF/TOP-SECRET cannot be established until VC mode has been cleared.*

Virtual Connect Mode is currently: Disabled

To save the settings, click **Next**. In case of linked enclosures, only the primary enclosure is affected. To advance to the next step without applying the FIPS settings, click **Skip**.

NOTE:

Entering and exiting FIPS Mode performs a factory restore operation and locks the Insight Display (LCD). If the Onboard Administrator was previously configured with a static IP address, it defaults to a DHCP address until reconfigured with a static IP address. Recovery requires access to the Onboard Administrator serial console to perform the `SHOW OA NETWORK` command to discover the new Onboard Administrator IP address.

The term "FIPS Mode" used in this document and within the product is to describe the feature, and not its validation status. The FIPS validation process is lengthy, so not all versions are FIPS validated. For information about the current FIPS status of this or any other firmware version, see the following documents:

- **Cryptographic Module Validation Program FIPS 140-1 and FIPS 140-2 Modules In Process List**
- **FIPS 140-1 and FIPS 140-2 Vendor List**
- **Commercial National Security Algorithm Suite**

Clearing VC mode

Clearing the VC mode removes all VC settings from the enclosure. Power off all VC-configured servers before clearing the VC mode. If servers are not powered down, they might maintain the VC settings until they are rebooted. You must clear the VC mode before changing to the FIPS Mode OFF/ON/DEBUG/Top-Secret/Top-Secret Debug.

Procedure

1. Click **Clear VC Mode**. A confirmation screen appears, stating `All servers should be powered off and not configured by Virtual Connect prior to clearing VC mode. Are you sure that you wish to clear VC mode?`
2. Click **OK**.

Advanced security settings

You can enable or disable selected security protocols and ciphers from the **Enclosure Settings** > **Network Access** > **FIPS tab**.

FIPS mode

NOTE:

FIPS Mode changes to ON/DEBUG/Top-Secret/Top-Secret Debug or OFF do not take effect unless VC Mode is disabled.

When the Onboard Administrator is operating in FIPS Mode ON, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. In FIPS Top-Secret Mode - certificates must have a minimum RSA key length of 3072 bits or ECDSA 384 bits, and the signature hash algorithm must be SHA-384.

In FIPS OFF mode, when OA versions 4.70 and later are downgraded, the selection of protocols and ciphers will revert to the default list.

- **FIPS Mode OFF** - Enables the use of non-FIPS-140-2-approved algorithms.
- **FIPS Mode ON** - Enforces the use of the Onboard Administrator in a FIPS 140-2-approved mode. This setting supports the use of approved cryptographic protocols and ciphers.
- **FIPS Mode TOP-SECRET** - Enforces the use of the Onboard Administrator in CNSA approved mode. This setting supports the use of approved cryptographic protocols and ciphers.

  FIPS mode DEBUG will no longer be a separate FIPS mode. Instead, DEBUG option can be enabled or disabled by an OA administrator when switching between FIPS Mode ON and Top-Secret.

The Onboard Administrator restarts after all changes are made.

IMPORTANT:

All existing settings are lost when you run this operation. Any change to the FIPS Mode setting performs a Restore to Factory Default operation.

NOTE:

When in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug, ensure that a strong password is set.

FIPS Mode status icons

With FIPS Mode ON or Top-Secret enabled, the current status of FIPS Mode is indicated by an icon displayed on the Onboard Administrator header bar on GUI screens. It is also displayed on the Onboard Administrator Sign-in page in the Connection column of the enclosure table. The status icons are described in the following table:

FIPS Mode icon	Description
FIPS	FIPS Mode is enabled (ON).
FIPS ⚠	FIPS Mode ON has one or more warnings. To determine the nature of the warning, hover the mouse pointer over the icon.
FIPS	FIPS Mode DEBUG is enabled.

Table Continued

FIPS Mode icon	Description
FIPS ⚠	FIPS Mode DEBUG has one or more warnings. To determine the nature of the warning, hover the mouse pointer over the icon.
FIPS	FIPS Mode is enabled (Top-Secret).
FIPS	FIPS Mode Top-Secret Debug is enabled.

FIPS strong password enforcement

When changing between available FIPS modes, strong passwords are enabled, minimum password length is set to eight characters, and a new Administrator account password is requested. Additionally, if changing to either FIPS Mode ON or FIPS Mode Top-Secret, the Enclosure IP Mode, Telnet, SNMPv1 and SNMPv2 protocols are disabled .In case of FIPS mode Top-Secret SNMPv3 is also disabled.

Enclosure Selection screen

The Enclosure Selection screen displays all discovered enclosures and selects the active enclosure (the enclosure you are signed in to) by default. The check box next to each enclosure enables you to select or clear that enclosure. To toggle the check box for all enclosures, select the **All Enclosures** check box.

To update the rack topology information, click **Refresh Topology**. When you select **Refresh Topology**, the Enclosure Selection screen switches to the Linked Mode and all linked enclosures appear.

Linked enclosures have one of the following states:

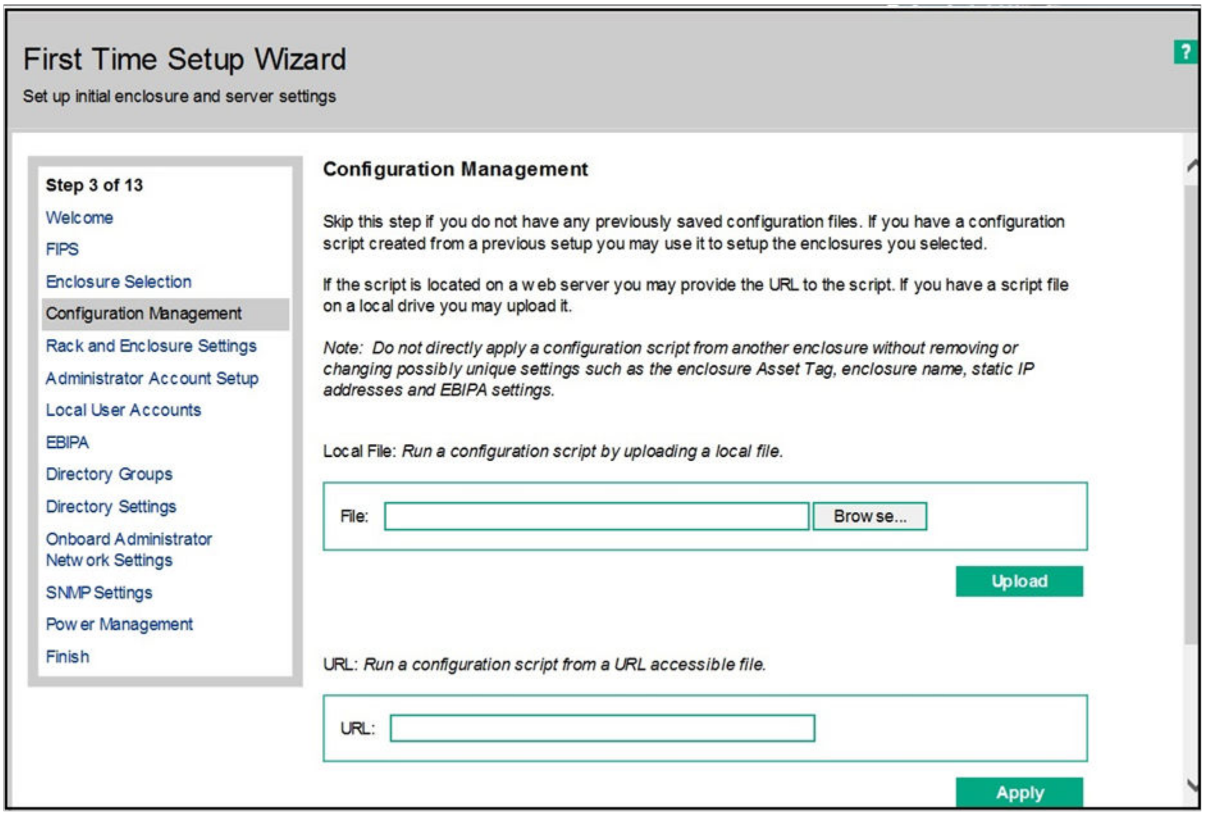
- Linked—Not Signed In. Select the enclosure and enter the Administrator password in the password text box. To authenticate the enclosure, click **Next**.
- Linked—Not Signed In with a card reader icon. This state indicates the linked enclosure is Two-Factor or CAC Authentication enabled but is not authenticated. This state occurs under three conditions:
    - ◦ If the configuration is not supported. The primary enclosure must be enabled for Two-Factor Authentication and both the primary and linked enclosures must have the same credentials for the linked enclosure to authenticate using Two-Factor Authentication. If the primary enclosure does not have Two-Factor Authentication enabled, then you cannot select the linked enclosure with Two-Factor Authentication enabled.
    - ◦ If the configuration is not supported . The primary enclosure must be enabled for CAC Authentication and both the primary and linked enclosure must have same credentials for the linked enclosure to authenticate using CAC Authentication. If the primary enclosure does not have CAC Authentication enabled, then you cannot select the linked enclosure with CAC Authentication enabled.
    - ◦ If you click the sign out link on a Two-factor or CAC Authentication enabled enclosure that is already authenticated , this state appears. If you select this enclosure, then authentication is attempted when you click **Next**
- Linked—Signed In with or without a card reader icon. This state indicates the linked enclosure is authenticated. If the enclosure information has not been loaded already, then it is loaded when you click **Next**.

If more than one enclosure is listed on the Enclosure Selection screen, select the enclosure you want to set up, and then click **Next**.

For possible values and descriptions of each field, see **Enclosure Information screen**.

Configuration Management screen

The Configuration Management screen enables you to set up the selected enclosures using a configuration file saved from a previous setup. You can run scripts for multiple Onboard Administrators before leaving the current screen.



First Time Setup Wizard

Set up initial enclosure and server settings

Step 3 of 13

Configuration Management

Skip this step if you do not have any previously saved configuration files. If you have a configuration script created from a previous setup you may use it to setup the enclosures you selected.

If the script is located on a web server you may provide the URL to the script. If you have a script file on a local drive you may upload it.

Note: Do not directly apply a configuration script from another enclosure without removing or changing possibly unique settings such as the enclosure Asset Tag, enclosure name, static IP addresses and EBIPA settings.

Local File: *Run a configuration script by uploading a local file.*

File:

URL: *Run a configuration script from a URL accessible file.*

URL:

To set up selected enclosures using a configuration file:

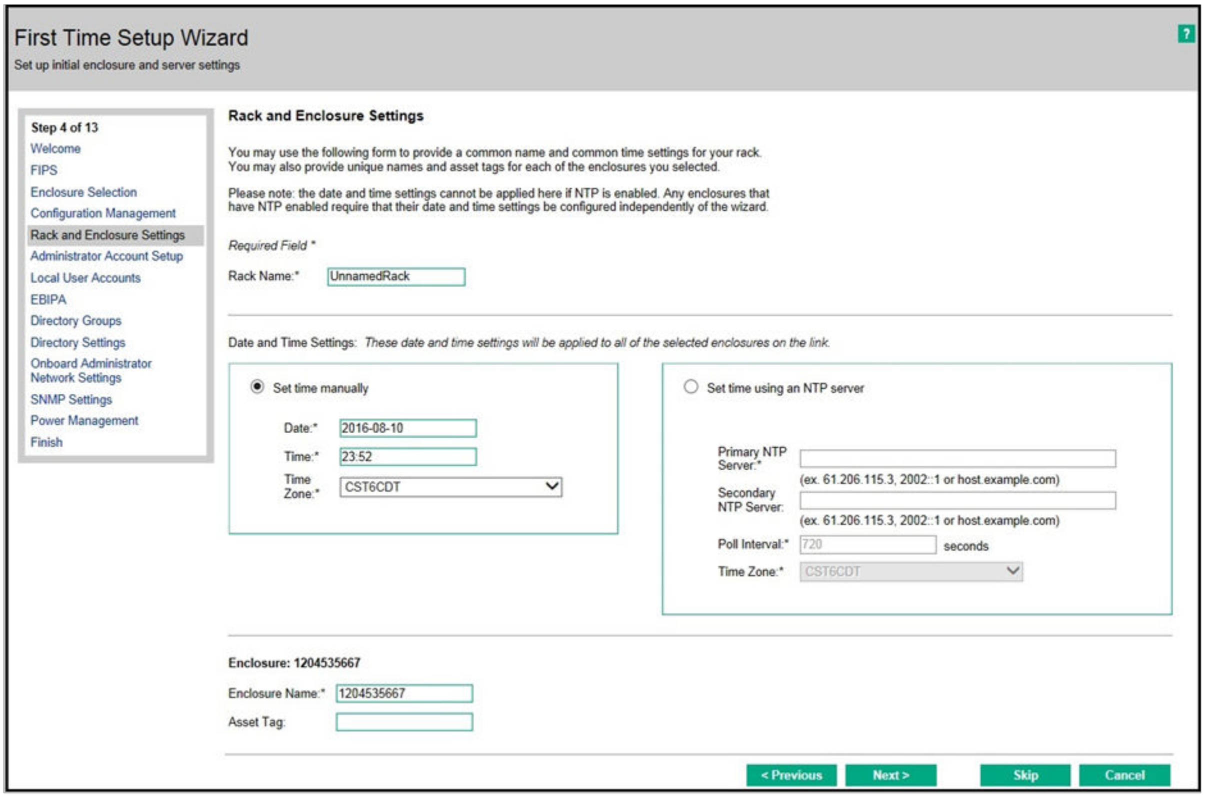
Select the enclosure to which you want to upload the configuration file. You can only upload the configuration file to one enclosure, even if you selected **All Enclosures** on the **Enclosure Selection** screen. You can select a local file, URL, or USB file:

- **Local file**—You can browse for the configuration file or you can enter the path of the configuration file into the textbox. The maximum number of characters in the file path is 256. Enter the configuration file path, click **Upload.**
- **URL—**If the configuration file is located on a web server, enter an HTTP path to the file. The maximum number of characters in the file path is 256. After entering the URL, click **Apply.**
- **USB file—**You can select a configuration file on a USB key plugged into the enclosure. Select the appropriate configuration file from the dropdown list. After selecting the configuration file, click **Apply.** This option only appears if a USB key is plugged into the enclosure.

After selecting the file location, a dialog box displays the results.

Rack and Enclosure Settings screen

Use this form to assign time settings and a common name to your rack and to assign unique names and asset tags to your enclosures.



First Time Setup Wizard

Set up initial enclosure and server settings

Step 4 of 13

Rack and Enclosure Settings

You may use the following form to provide a common name and common time settings for your rack. You may also provide unique names and asset tags for each of the enclosures you selected.

Please note: the date and time settings cannot be applied here if NTP is enabled. Any enclosures that have NTP enabled require that their date and time settings be configured independently of the wizard.

*Required Field **

Rack Name:* UnnamedRack

Date and Time Settings: *These date and time settings will be applied to all of the selected enclosures on the link.*

● Set time manually

Date:* 2016-08-10

Time:* 23:52

Time Zone:* CST6CDT

○ Set time using an NTP server

Primary NTP Server:*

(ex. 61.206.115.3, 2002::1 or host.example.com)

Secondary NTP Server:

(ex. 61.206.115.3, 2002::1 or host.example.com)

Poll Interval:* 720 seconds

Time Zone:* CST6CDT

Enclosure: 1204535667

Enclosure Name:* 1204535667

Asset Tag:

Field	Possible value	Description
Rack Name	1 to 32 characters including all alphanumeric characters, the dash (-), and the underscore (_)	The name of the rack in which the enclosure is installed
Date and Time Settings	• Set time manually • Set time using an NTP server	The method used to assign the date and time to all the selected enclosures on the link
Date	yyyy-mm-dd, where: • mm is an integer from 1 to 12 • dd is an integer from 1 to 31	The current date assigned to the enclosure
Time	hh:mm (24-hour time) • hh is an integer from 0 to 23 • mm is an integer from 0 to 59	The current time assigned to the enclosure
Time Zone	Time zone settings • **Africa time zone settings** • **Americas time zone settings** • **Asia time zone settings** • **Universal time zone settings** • **Oceanic time zone settings** • **Europe time zone settings** • **Polar time zone settings**	The time zone assigned to the enclosure

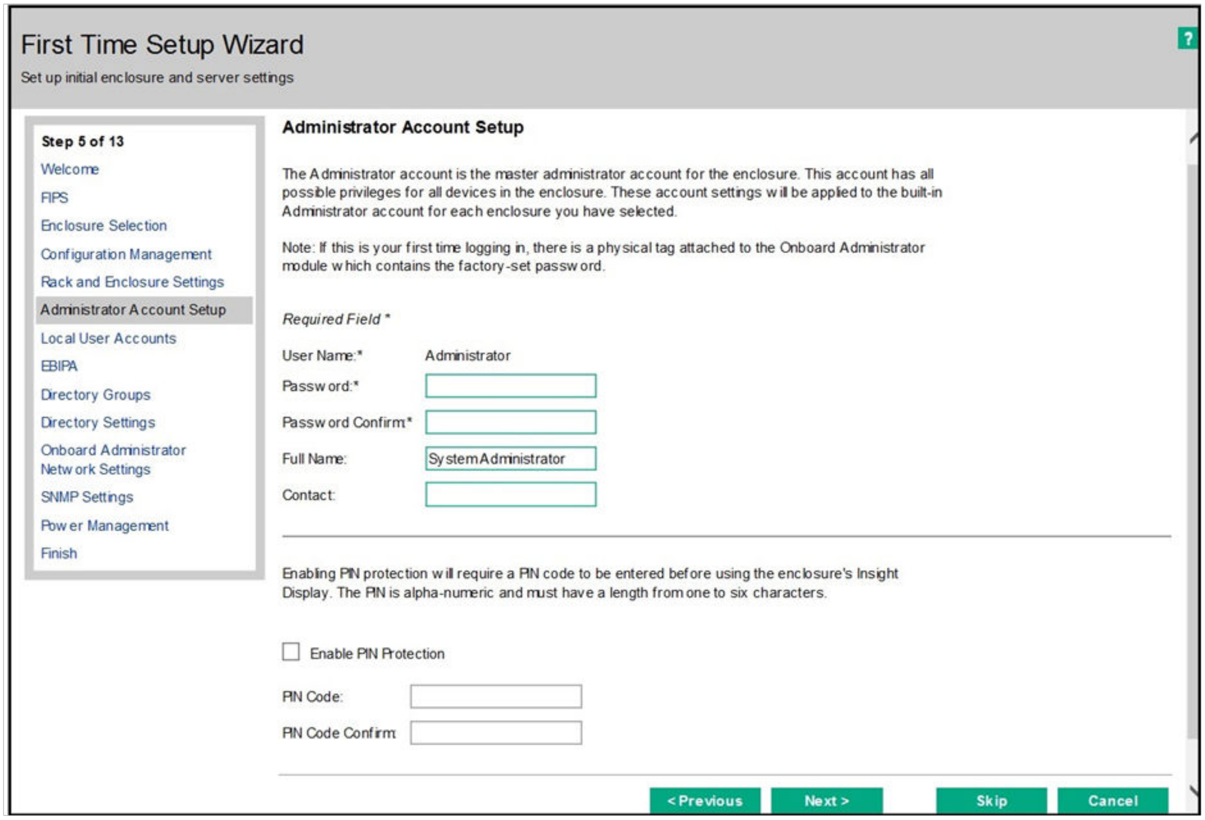
Table Continued

Field	Possible value	Description
Primary NTP Server	• IPv4 address—###.###.###.### where ### ranges from 0 to 255 • IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. • DNS name—1 to 64 characters including all alphanumeric characters and the dash (-).	IP address or DNS name of primary NTP server that provides date and time information
Secondary NTP Server	• IPv4 address—###.###.###.### where ### ranges from 0 to 255 • IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. • DNS name—1 to 64 characters including all alphanumeric characters and the dash (-).	IP address or DNS name of secondary NTP server that provides date and time information
Poll Interval	An integer from 60 to 86400	The interval at which the NTP server is polled in seconds
Enclosure Name	1 to 32 characters including all alphanumeric characters, the dash (-), and the underscore (_)	The name of the selected enclosure
Asset Tag	0 to 32 characters including all alphanumeric characters, the dash (-), and the underscore (_)	The asset tag is used for inventory control The default asset tag is blank

For more information on connecting enclosures, see the BladeSystem c7000 User Guide.

Administrator Account Setup screen

The Administrator Account Setup screen initially displays the name of the active enclosure and the current settings. If multiple enclosures were selected on the Enclosure Selection screen, a button is activated that enables you to view separate inputs for each selected Onboard Administrator.



First Time Setup Wizard

Set up initial enclosure and server settings

Administrator Account Setup

The Administrator account is the master administrator account for the enclosure. This account has all possible privileges for all devices in the enclosure. These account settings will be applied to the built-in Administrator account for each enclosure you have selected.

Note: If this is your first time logging in, there is a physical tag attached to the Onboard Administrator module which contains the factory-set password.

*Required Field **

User Name:* Administrator

Password:*

Password Confirm:*

Full Name: SystemAdministrator

Contact:

Enabling PIN protection will require a PIN code to be entered before using the enclosure's Insight Display. The PIN is alpha-numeric and must have a length from one to six characters.

□ Enable PIN Protection

PIN Code:

PIN Code Confirm:

Field	**Possible value**	**Description**
Full Name	0 to 20 characters including all alphanumeric characters, the dash (-), the underscore (_), and the space	The full name of the user
Contact	0 to 20 characters including all alphanumeric characters, the dash (-), the underscore (_), and the space	Contact information for the user account. The contact information can be the name of an individual, a telephone number, or other useful information.
Administrator Password	3 to 40 characters including all printable characters	The password for the user account
Administrator Password Confirm	3 to 40 characters including all printable characters	Must match the Administrator Password value
Enable Insight Display PIN protection	Select or clear check box	Select this check box to require a PIN code to be entered to access the enclosure Insight Display.
PIN Code	1 to 6 characters from the character sets 0 to 9, a to z, and A to Z	The PIN code for the enclosure Insight Display
PIN Code Confirm	1 to 6 characters from the character sets 0 to 9, a to z, and A to Z	Must match the Insight Display PIN value

NOTE:

When Onboard Administrator is operating in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug, the PIN protection cannot be disabled.

Local User Accounts screen

The Local User Accounts screen displays the user accounts assigned to the Active Onboard Administrator and provides choices for adding, editing, and deleting accounts.

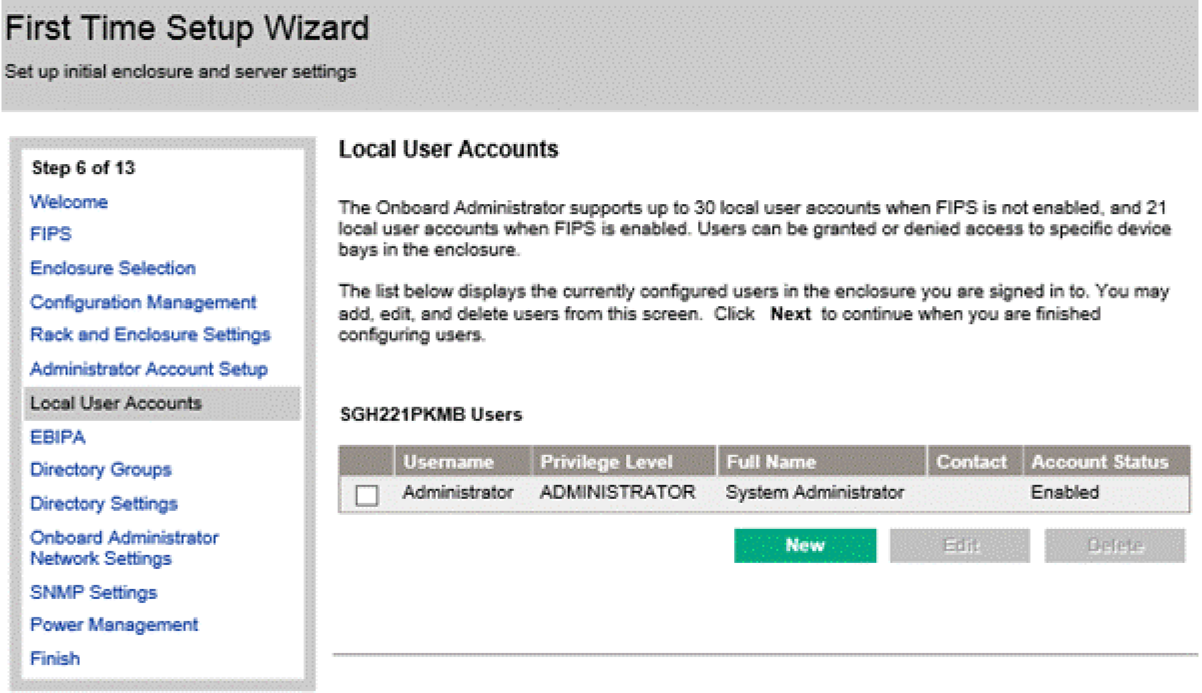
- **New**—To add a new user to the selected enclosure, click **New**. The Add Local User screen appears.

  NOTE:

  A maximum of 30 user accounts can be configured in FIPS Mode OFF, while a maximum of 21 user accounts can be configured in FIPS Mode ON or Top-Secret. The maximum user account limit includes reserved accounts such as the Administrator and Virtual Connect accounts.

  When Onboard Administrator is operating in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug, the PIN protection cannot be disabled.

- **Edit**—Select a user (only one can be selected) by selecting the check box next to the name of the user. To change the settings on the Edit Local User screen, click **Edit**.
- **Delete**—Select a user or users to be deleted by selecting the check box next to the name of each user. To remove the accounts, click **Delete**. If an attempt is made to delete the last remaining Administrator account, you will receive an alert warning that one Administrator account must remain and the delete action will be canceled.



First Time Setup Wizard

Set up initial enclosure and server settings

Local User Accounts

The Onboard Administrator supports up to 30 local user accounts when FIPS is not enabled, and 21 local user accounts when FIPS is enabled. Users can be granted or denied access to specific device bays in the enclosure.

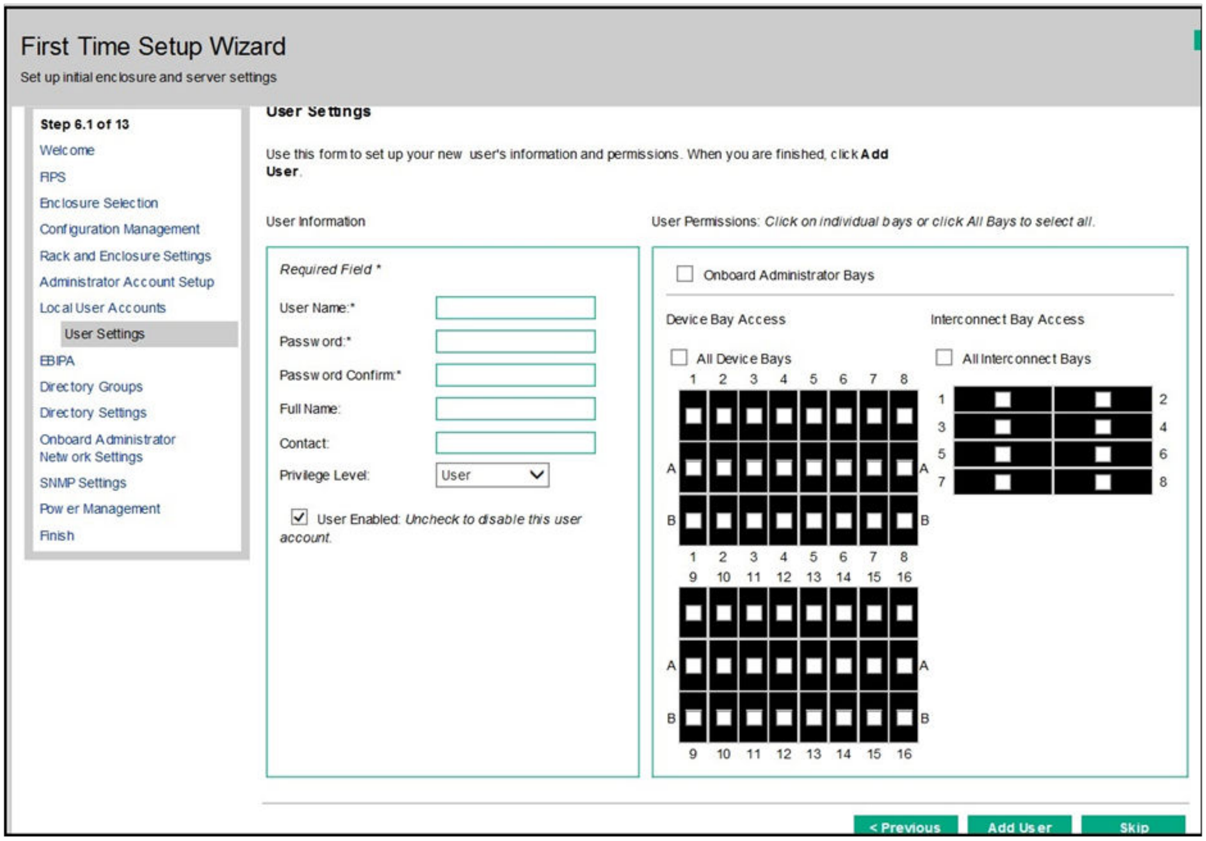
The list below displays the currently configured users in the enclosure you are signed in to. You may add, edit, and delete users from this screen. Click **Next** to continue when you are finished configuring users.

SGH221PKMB Users

	Username	Privilege Level	Full Name	Contact	Account Status
□	Administrator	ADMINISTRATOR	System Administrator		Enabled

User Settings screen

The User Settings screen displays configurable user information. Enter user information in the User Information and User Permissions sections. To save the information, click **Add User**. To return to the Local User Accounts screen, click **Cancel**.



User Settings

Use this form to set up your new user's information and permissions. When you are finished, click **Add User**.

User Information

*Required Field **

User Name:*

Password:*

Password Confirm:*

Full Name:

Contact:

Privilege Level: User

☑ User Enabled: *Uncheck to disable this user account.*

User Permissions: *Click on individual bays or click All Bays to select all.*

☐ Onboard Administrator Bays

Device Bay Access

☐ All Device Bays

Interconnect Bay Access

☐ All Interconnect Bays

For each user added, select the appropriate boxes to grant access to servers and interconnect bays.

For possible values and descriptions of each field, see **Add Local User**.

Enclosure Bay IP Addressing

The First Time Setup Wizard Enclosure Bay IP Addressing screens allow you to configure IPv4 and IPv6 fixed addresses for Onboard Administrator enclosure bays. The Onboard Administrator EBIPA feature helps you provision a fixed IP address based on bay number, which preserves the IP address for a particular bay even if a device is replaced. The management interface for components plugged into the bays must be set for DHCP. EBIPA can only be used if the devices are set to boot from DHCP. If a device is configured for static IP, then it must be manually reconfigured to DHCP to change the EBIPA IP address.

NOTE:

The Onboard Administrator documentation refers to EBIPA IP addresses as "fixed IP addresses" or "fixed DHCP addresses," meaning that each of these addresses is an IP address permanently associated with a specific bay number independent of the actual device currently attached to the bay.

The server blade iLO bays and interconnect module management bays can obtain IP addresses on the management network in several ways: dynamic IP addressing using an external DHCP server, static IP addressing, SLAAC via router advertisements (IPv6 only), or EBIPA. If your network has a DHCP service or if you want to manually assign static IP addresses one by one to the server blades and interconnect modules, click **Skip** to bypass configuring Enclosure Bay IP Addressing.

EBIPA only assigns fixed DHCP IP addresses to the management interface for server iLOs and interconnect modules on the management network internal to the enclosure. EBIPA does not assign IP addresses for any other devices on the management network external to the enclosure and cannot be used as a DHCP server on the production network.

The server blade iLO defaults to DHCP addressing, which is obtained through the network connector of the Active Onboard Administrator. Interconnect modules that have an internal management network connection to the Onboard Administrator might also default to DHCP addressing.

NOTE:

EBIPA enforces unique IP addresses for all bays, even if bays are on a different VLAN.

EBIPA configuration guidelines

This provides general configuration information. For configuration information specific to IPv4 or IPv6, see the corresponding sections that follow.

If your facility prefers fixed IP address assignment, you can specify unique fixed addresses individually for each of the server blade iLO bays and interconnect module management bays, or you can use EBIPA to assign a range of fixed IP addresses to individual server blade and interconnect module bays. If you specify fixed addresses individually, the subnet mask (IPv4), gateway, DNS servers, NTP servers (IPv4 interconnect), and domain name can be the same or different for each bay. If you use EBIPA to assign a range of fixed addresses, you must specify the first IP address in a range and the subnet mask. When you click the **Autofill** down arrow button for that bay, the bays listed below that bay are automatically assigned consecutive IP addresses. The subnet mask, gateway, DNS servers, NTP servers, and domain name are also copied to each of the consecutive bays in the list.

For example, if you specify IPv4 address 16.100.226.21 for EBIPA bay 1, then using the Autofill feature, bays 1 through 16 are assigned consecutive IP addresses in the range 16.100.226.21 to 16.100.226.36. If you specify 16.200.139.51 for interconnect bay 3 and use the feature, interconnect bays 3 through 8 are assigned consecutive IP addresses in the range 16.200.139.51 to 16.200.139.56.

NOTE:

The **Autofill** button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on.

When using Autofill, specify an IPv4 subnet mask or IPv6 subnet prefix that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a subnet mask or prefix that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.

If you use fixed IP addresses for management processors, then the Onboard Administrator `hponcfg` command can be used to send the iLO network settings RIBCL script to an iLO if that iLO already has an IP address. EBIPA can be used to bootstrap IP addresses to iLOs, so that Onboard Administrator `hponcfg` command can be used to send configuration scripts to those iLOs. Changes to iLO network settings results in that iLO resetting the network interface and breaking the current connections for a few seconds.

If you have double dense server blades, do not configure EBIPA settings for the base bays (Bay 1, 2, and so forth). Configure the side A bays (1A, 2A, and so on) and side B bays (1B, 2B, and so on). Using the Autofill feature assigns consecutive IP addresses to the bays listed below the bay where you specify the first IP address in the range (for example, if you specify the IP address for bay 1A and use the Autofill feature, bays 2A, 3A, and so on are assigned consecutive addresses).

To configure the interconnect bays, use the Interconnect List (located below the Device List, on the same Wizard screen).

To apply settings, click **Next**.

Servers in the device bays automatically acquire the device bay EBIPA addresses within a few minutes, but the interconnect switch modules must be manually restarted by clicking the **Virtual Power** button on each Onboard Administrator Interconnect Module information page.

Setting up your enclosure using EBIPA without an active network connection

Procedure

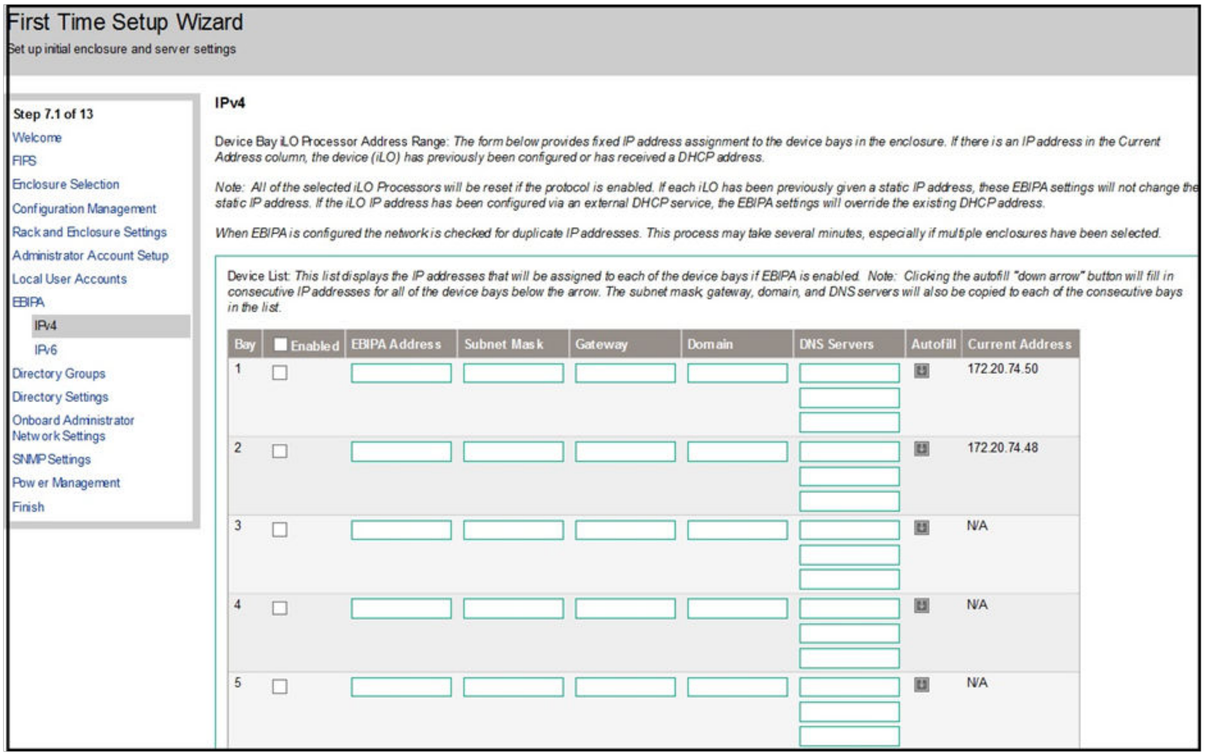
1. Configure a static IP for each Onboard Administrator using Insight Display, and note the active OA Service IP address on the Insight Display Enclosure Info screen. Attach the client PC to the enclosure Service Port (Enclosure Link Up connector) between the OA bays with a standard Ethernet patch cable. The client PC NIC must be configured for DHCP because it acquires an IP address in the range 169.254.x.y approximately 1 minute later.
2. Launch a web browser (or alternatively a Telnet or SSH session), and select the Onboard Administrator Service IP address as displayed in the enclosure Insight Display on the Enclosure Info screen.
3. Using the administrative password attached to the active Onboard Administrator, log in to the Onboard Administrator as Administrator.
4. During the First Time Setup Wizard, enable Device Bay EBIPA with a starting fixed IP address and enable Interconnect Bay EBIPA with a different starting IP address.

   After running the First Time Setup Wizard, you can modify the EBIPA settings at any time by selecting **Enclosure Bay IP Addressing** in the Enclosure Settings list.

   Clicking the **Autofill** button creates as many sequential, fixed IP addresses as needed. The subnet mask, gateway, DNS servers, NTP servers, and domain name are also copied to each of the consecutive bays in the list. Alternatively, you can assign individual fixed IP addresses by manually entering the desired IP address in the EBIPA Address field for the specific bay. The subnet mask, gateway, DNS servers, NTP servers, and domain can be same or different for each bay.

   After you apply settings, servers in the device bays automatically acquire the device bay EBIPA addresses within a few minutes, but the interconnect switch modules must be manually restarted by clicking the **Virtual Power** button on each Onboard Administrator Interconnect Module information page.
5. To verify that the server blade iLO addresses have been set according to the EBIPA starting IP address and range, use the Onboard Administrator Device list.

First Time Setup Wizard EBIPA IPv4 screen



IPv4

Device Bay iLO Processor Address Range: *The form below provides fixed IP address assignment to the device bays in the enclosure. If there is an IP address in the Current Address column, the device (iLO) has previously been configured or has received a DHCP address.*

Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IP address, these EBIPA settings will not change the static IP address. If the iLO IP address has been configured via an external DHCP service, the EBIPA settings will override the existing DHCP address.

When EBIPA is configured the network is checked for duplicate IP addresses. This process may take several minutes, especially if multiple enclosures have been selected.

Device List: *This list displays the IP addresses that will be assigned to each of the device bays if EBIPA is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IP addresses for all of the device bays below the arrow. The subnet mask, gateway, domain, and DNS servers will also be copied to each of the consecutive bays in the list.*

Bay	□ Enabled	EBIPA Address	Subnet Mask	Gateway	Domain	DNS Servers	Autofill	Current Address
1	□						⬇	172.20.74.50
2	□						⬇	172.20.74.48
3	□						⬇	N/A
4	□						⬇	N/A
5	□						⬇	N/A

ⓘ **IMPORTANT:**

Do not use the 169.254.x.x range when configuring EBIPA-assigned addresses, as this network address range is reserved for use by the Onboard Administrator.

Device List

Column	Description
Bay	The bay in the enclosure of the device.
Enabled	Enables EBIPA settings for the device bay. EBIPA settings for all device bays can be enabled by selecting the check box next to Enabled in the heading row or individual device bays can be selected by clicking the check box for that particular device bay.
EBIPA Address	The fixed IP address you want to assign to the device bay. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Subnet Mask	Subnet mask for the device bays. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Gateway	The fixed gateway IP address that you want to assign for the device bays. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Domain	Domain name for the device bays. Possible values are a character string with a maximum of 64 characters, including all alphanumeric characters, the dash (-), and the period (.).
DNS Servers	IP addresses for primary, secondary, and tertiary DNS servers. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Autofill	Assigns consecutive IP addresses for the selected device bays below in the device list. To assign the IP addresses, click the **Autofill** down arrow. The Autofill button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on. When using Autofill, specify an IPv4 subnet mask that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a subnet mask that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.
Current Address	The current IP address of the device bay.

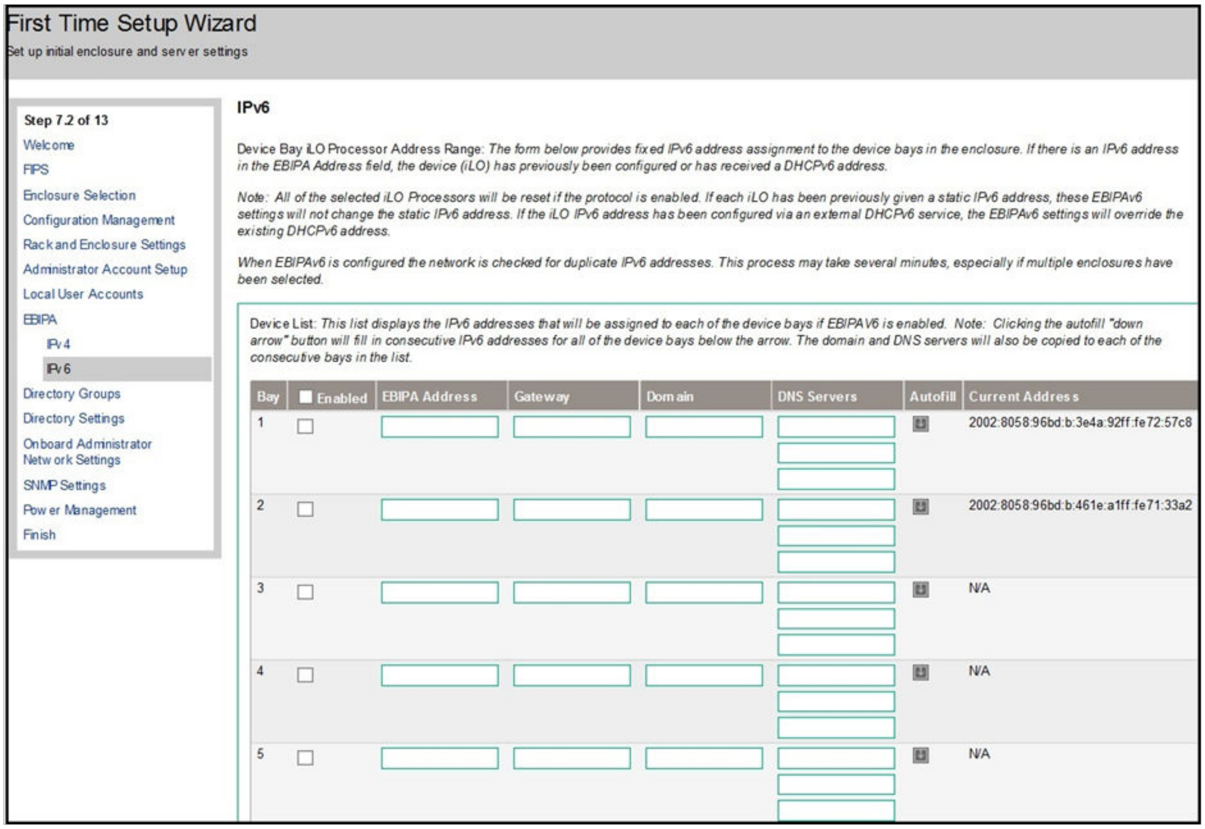
Interconnect List

Column	Description
Bay	The bay in the enclosure of the interconnect device.
Enabled	Enables EBIPA for IPv4 settings for the interconnect bay. EBIPA for IPv4 settings for all interconnect bays can be enabled by selecting the check box next to Enabled in the heading row or individual interconnect bays can be enabled by selecting the check box for that particular interconnect bay.
EBIPA Address	The fixed DHCP IP address you want to assign to the device bay.
Subnet Mask	Subnet mask for the device bays. Possible values are ###.###.###.### where ### ranges from 0 to 255.

Table Continued

Column	Description
Gateway	Gateway address for the device bays. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Domain	Domain name for the device bays. Possible values are a character string with a maximum of 64 characters, including all alphanumeric characters, the dash (-), and the period (.).
DNS Servers	IPv4 addresses for primary, secondary, and tertiary DNS servers. Possible values are ###.###.###.### where ### ranges from 0 to 255.
NTP Server	The IPv4 address of the server used for synchronizing time and date using the NTP protocol. ###.###.###.###, where ### ranges from 0 to 255.
Autofill	Assigns consecutive IPv4 addresses for the selected interconnect bays below in the interconnect list. To assign the IP addresses, click the **Autofill** down arrow. The Autofill button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on. When using Autofill, specify an IPv4 subnet mask that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a subnet mask that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.
Current Address	The current IPv4 address of the interconnect bay.

First Time Setup Wizard EBIPA IPv6 screen



First Time Setup Wizard

Set up initial enclosure and server settings

IPv6

Device Bay iLO Processor Address Range: *The form below provides fixed IPv6 address assignment to the device bays in the enclosure. If there is an IPv6 address in the EBIPA Address field, the device (iLO) has previously been configured or has received a DHCPv6 address.*

Note: *All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IPv6 address, these EBIPAv6 settings will not change the static IPv6 address. If the iLO IPv6 address has been configured via an external DHCPv6 service, the EBIPAv6 settings will override the existing DHCPv6 address.*

When EBIPAv6 is configured the network is checked for duplicate IPv6 addresses. This process may take several minutes, especially if multiple enclosures have been selected.

Device List: *This list displays the IPv6 addresses that will be assigned to each of the device bays if EBIPAV6 is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the device bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.*

Bay	■ Enabled	EBIPA Address	Gateway	Domain	DNS Servers	Autofill	Current Address
1	□						2002:8058:96bd:b:3e4a:92ff:fe72:57c8
2	□						2002:8058:96bd:b:461e:a1ff:fe71:33a2
3	□						N/A
4	□						N/A
5	□						N/A

IMPORTANT:

Do not use the fe80::/10 prefix when configuring EBIPA-assigned addresses, as this network prefix is reserved for link local SLAAC addresses.

NOTE:

For EBIPA IPv6 fixed addresses to be successfully configured, the **Enable IPv6** setting must be enabled. To enable this setting, use the First Time Setup Wizard Network IPv6 Settings screen or the Enclosure Settings IPv6 Settings tab.

The **Enable SLAAC** and **Enable DHCPv6** settings have no effect on EBIPA IPv6 functionality.

Device List

Column	Description
Bay	The bay in the enclosure of the device.
Enabled	Enables EBIPA settings for the device bay. EBIPA settings for all device bays can be enabled by selecting the check box next to Enabled in the heading row or individual device bays can be selected by clicking the check box for that particular device bay.
EBIPA Address	The fixed IPv6 address you want to assign to the device bay. Possible values are ####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. The prefix /### ranges from 1 to 128; the prefix length is mandatory.
Gateway	The fixed IPv6 gateway address you want to assign for the device bays. Possible values are ####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. Do not specify a prefix. The gateway is assumed reachable from within the network. If this gateway is specified as a Link-Local address, the gateway will always be configured on the enclosure device using this address. If the gateway is specified with any other type of IPv6 address, the Onboard Administrator sends neighbor solicitation requests to identify the Link-Local address of the gateway device for use in configuring the enclosure device. If the gateway does not exist or does not respond to neighbor solicitation requests, no gateway is configured.
Domain	Domain name for the device bays. Possible values are a character string with a maximum of 64 characters, including all alphanumeric characters, the dash (-), and the period (.).
DNS Servers	IPv6 addresses for primary, secondary, and tertiary DNS servers. Possible values are ####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.

Table Continued

Column	Description
Autofill	Assigns consecutive IPv6 addresses for the selected device bays below in the device list. To assign the IP addresses, click the **Autofill** down arrow. The Autofill button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on. When using Autofill, specify an IPv6 subnet prefix that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a prefix that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.
Current Address	The current IPv6 address of the device bay.

Interconnect list

Column	Description
Bay	The bay in the enclosure of the interconnect device.
Enabled	Enables EBIPA for IPv6 settings for the interconnect bay. EBIPA for IPv6 settings for all interconnect bays can be enabled by selecting the check box next to Enabled in the heading row or individual interconnect bays can be enabled by selecting the check box for that particular interconnect bay.
EBIPA Address	The fixed DHCP IPv6 IP address you want to assign to the interconnect bay. Possible values are ####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. The prefix /### ranges from 1 to 128; the prefix length is mandatory.
Gateway	The fixed gateway IPv6 address you want to assign for the interconnect bays. Possible values are ####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. Do not specify a prefix. The gateway is assumed reachable from within the network. If this gateway is specified as a Link-Local address, the gateway will always be configured on the enclosure device using this address. If the gateway is specified with any other type of IPv6 address, the Onboard Administrator sends neighbor solicitation requests to identify the Link-Local address of the gateway device for use in configuring the enclosure device. If the gateway does not exist or does not respond to neighbor solicitation requests, no gateway is configured.
Domain	Domain name for the device bays. Possible values are a character string with a maximum of 64 characters, including all alphanumeric characters, the dash (-), and the period (.).
DNS Servers	IPv6 addresses for primary, secondary, and tertiary DNS servers. Possible values are ####:####:####:####:####:####:####:####, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.

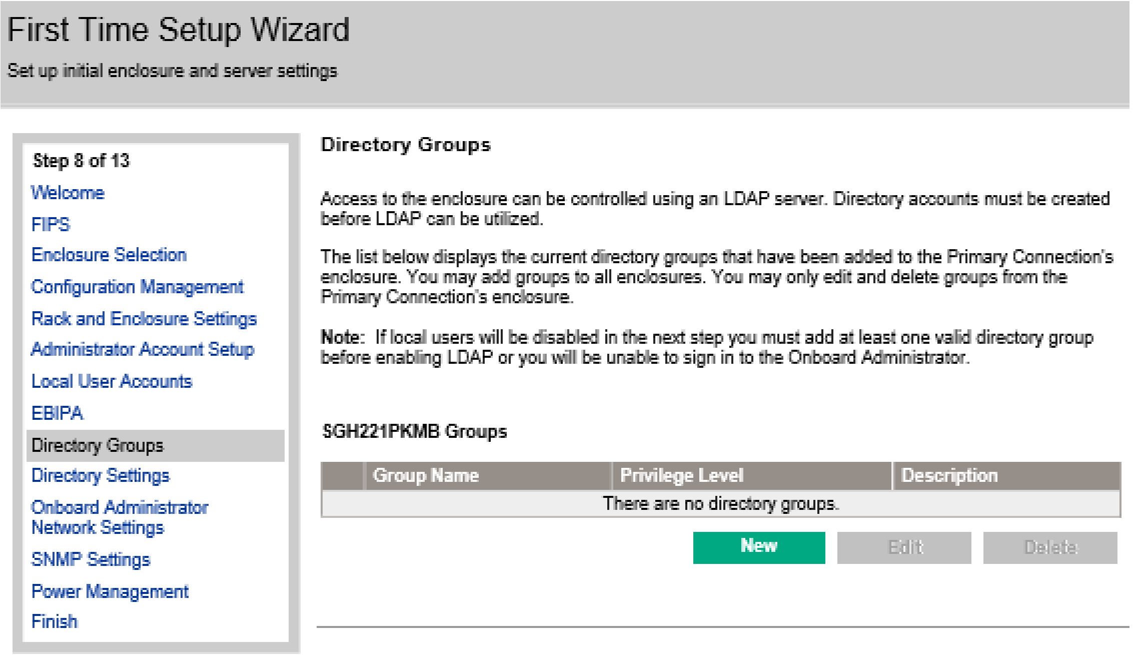
Table Continued

Column	Description
Autofill	Assigns consecutive IPv6 addresses for the selected interconnect bays below in the interconnect list. To assign the IP addresses, click the **Autofill** down arrow. The Autofill button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on. When using Autofill, specify an IPv6 subnet prefix that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a prefix that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.
Current Address	The current IPv6 address of the interconnect bay.

Directory Groups Configuration screen

LDAP is an open protocol for accessing information directories. While LDAP is based on the X.500 standard, LDAP is less complex. LDAP supports TCP/IP, which enables applications to work independently of the server hosting the directory.

The following figure shows the First Time Setup Wizard Directory Groups screen, which allows you to add, edit, and delete directory groups.



First Time Setup Wizard

Set up initial enclosure and server settings

Directory Groups

Access to the enclosure can be controlled using an LDAP server. Directory accounts must be created before LDAP can be utilized.

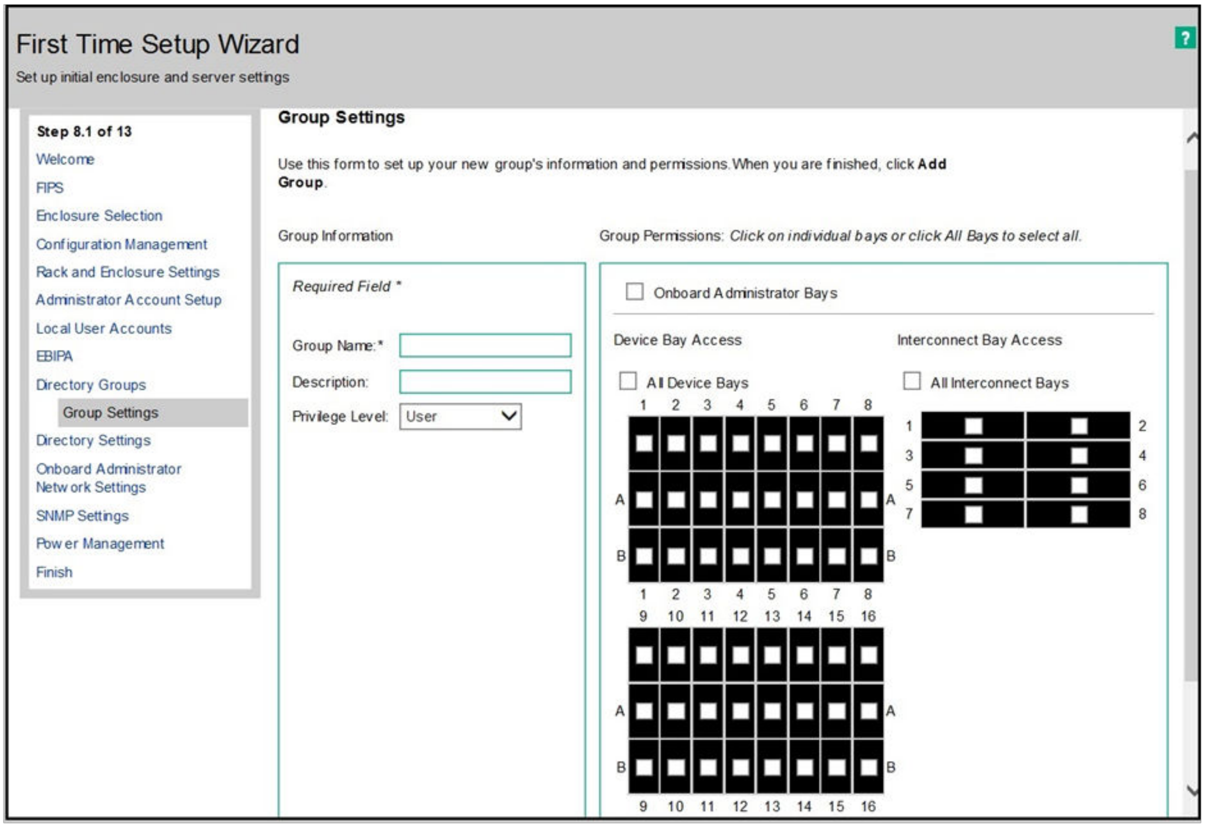
The list below displays the current directory groups that have been added to the Primary Connection's enclosure. You may add groups to all enclosures. You may only edit and delete groups from the Primary Connection's enclosure.

Note: If local users will be disabled in the next step you must add at least one valid directory group before enabling LDAP or you will be unable to sign in to the Onboard Administrator.

SGH221PKMB Groups

	Group Name	Privilege Level	Description
There are no directory groups.			

To add a directory group, click **New**. The following figure shows the First Time Setup Wizard Group Settings screen that allows you to configure a new directory group and set directory access for the selected enclosures.



First Time Setup Wizard

Set up initial enclosure and server settings

Step 8.1 of 13

- Welcome
- FIPS
- Enclosure Selection
- Configuration Management
- Rack and Enclosure Settings
- Administrator Account Setup
- Local User Accounts
- EBIPA
- Directory Groups
  - Group Settings
- Directory Settings
- Onboard Administrator Network Settings
- SNMP Settings
- Power Management
- Finish

Group Settings

Use this form to set up your new group's information and permissions. When you are finished, click **Add Group**.

Group Information

*Required Field **

Group Name:*

Description:

Privilege Level: User

Group Permissions: *Click on individual bays or click All Bays to select all.*

☐ Onboard Administrator Bays

Device Bay Access

☐ All Device Bays

Interconnect Bay Access

☐ All Interconnect Bays

Access to the enclosure can be granted using LDAP. To use the LDAP server, you must create directory accounts.

The Directory Groups screen displays current directory groups that have been added to the Primary Connection enclosure. You may add user groups to all enclosures. You may edit and delete user groups from the Primary Connection enclosure only. To use LDAP services, you must add at least one directory group.

Column	Description
Check box	Used to select Directory Group for editing or deleting
Group Name	1 to 255 characters and contains the same characters as search contexts. The group name is used to determine LDAP users' group membership. The group name must match one of the following five properties of a directory group: the name, distinguished name, common name, Display Name, or SAM Account Name. For nested groups, matching is based on `objectSid` (an attribute that specifies the security ID of the group). The distinguished name is recommended to uniquely specify the LDAP group. If the Onboard Administrator is configured to search the GC port and a distinguished name is not used, then an incorrect match in multiple domains may occur which could result in unintended authorization.
Privilege Level	Used to determine which administrative functions the user is allowed to perform. A user's privilege level can be administrator, operator, or user.
Description	0 to 58 characters, containing alphanumeric characters, the dash (-), the underscore (_), and the space. The description of the LDAP group, a more readable version of the group name, or other useful information.

- **New**—To add a new Directory Group to the selected enclosure, click **New.** You can add a maximum of 30 Directory Groups. The Add LDAP Group screen appears.
- **Edit**—Select a Directory Group to be edited by selecting the check box next to the name of the group. To change the settings on the Edit LDAP Group screen, click **Edit.**
- **Delete**—Select the Directory Group to be deleted by selecting the check box next to the name of the group. To remove the group, click **Delete.**

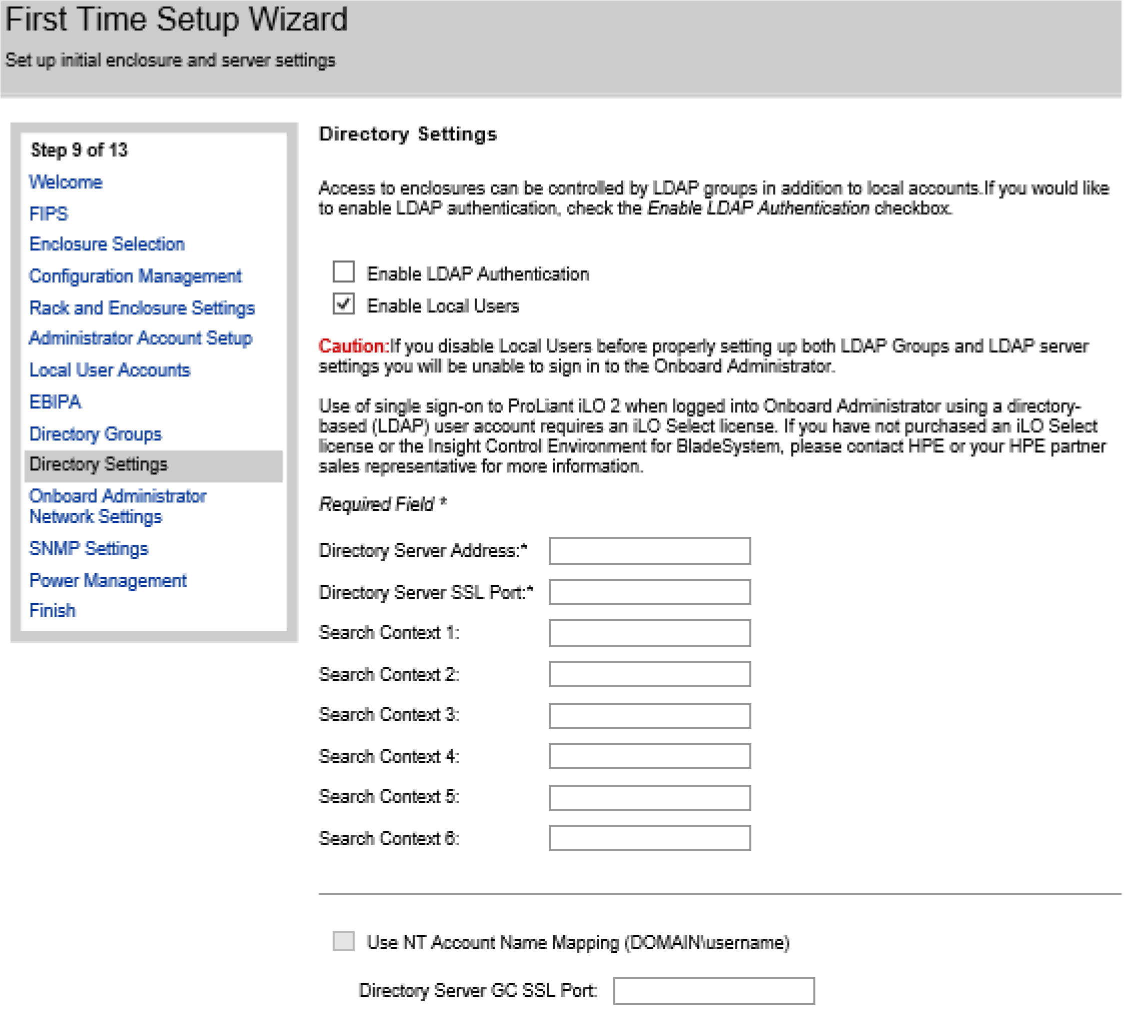
Nested LDAP group support

When using Microsoft Active Directory, you can place one or more groups in another group. Groups that are contained within another group are called nested groups. The group that contains nested groups is called a nesting group. The advantage of nested groups is that users of a nested group can log in to the Onboard Administrator if their nesting group is configured appropriately. For example, assume `group2` is nested in `group1`. Users in `group2` are allowed to log in to the Onboard Administrator if the parent LDAP group (`group1`) is added to the Onboard Administrator and can be found using one of the search contexts. The search context is not restricted to the exact location: if the search context path is high in the LDAP directory tree, subtree searching is used. The Onboard Administrator supports the security group type only. Distribution group type is not supported.

To apply settings, click **Next**.

Directory Settings screen

Use the following Directory Settings screen to set directory access for the currently selected enclosures.



First Time Setup Wizard

Set up initial enclosure and server settings

Directory Settings

Access to enclosures can be controlled by LDAP groups in addition to local accounts.If you would like to enable LDAP authentication, check the *Enable LDAP Authentication* checkbox.

□ Enable LDAP Authentication

☑ Enable Local Users

Caution:If you disable Local Users before properly setting up both LDAP Groups and LDAP server settings you will be unable to sign in to the Onboard Administrator.

Use of single sign-on to ProLiant iLO 2 when logged into Onboard Administrator using a directory-based (LDAP) user account requires an iLO Select license. If you have not purchased an iLO Select license or the Insight Control Environment for BladeSystem, please contact HPE or your HPE partner sales representative for more information.

*Required Field **

Directory Server Address:*	
Directory Server SSL Port:*	
Search Context 1:	
Search Context 2:	
Search Context 3:	
Search Context 4:	
Search Context 5:	
Search Context 6:	

□ Use NT Account Name Mapping (DOMAIN\username)

Directory Server GC SSL Port:

NOTE:

The Onboard Administrator LDAP feature supports Microsoft® Active Directory using the `memberOf` attribute. Novell eDirectory is also supported with the `groupMembership` attribute. OpenLDAP is not supported.

On this screen you can configure the following settings:

- **Enable LDAP Authentication**—Select this check box to enable a directory server to authenticate a user sign in.
- **Enable Local Users**—Select this check box to enable a user to sign in using a local user account instead of a directory account.
- **Search Context**—Specify one to six search contexts. A search context is a search filter or shortcut to a common directory, defining the directory user search to start at the specified path. By specifying a search context, users do not have to specify their full DNs at login. A DN might be long, and users might not be familiar with their DN or might have accounts in different directory contexts. The Onboard Administrator attempts to contact the directory service by DN, and then applies the search contexts in order, beginning with `Search Context 1` and continuing through any subsequent search contexts until successful.

  - **Example 1**:

    Assume that you are `user1`. If you enter the search context `ou=OU1,dc=hp,dc=com`, you can log in as `user1` instead of `cn=user1,ou=OU1,dc=hp,dc=com`.

  - **Example 2**:

    Assume the following search contexts are defined:

    - Search Context 1: `ou=OU1,dc=hp,dc=com`
    - Search Context 2: `ou=OU2,ou=OU1,dc=hp,dc=com`

    If two users have the same common name `user1` in both search contexts, and their passwords are the same, when either user attempts to log in, the Onboard Administrator contacts `cn=user1,ou=OU1,dc=hp,dc=com`.

    If their passwords are different, and a user provides the password for the user in `OU2`, the Onboard Administrator uses DN `cn=user1,ou=OU1,dc=hp,dc=com`, but that will be rejected because the password does not match. The next login will be attempted using `cn=user1,ou=OU2,ou=OU1,dc=hp,dc=com`, which will succeed.

  Search context is also applicable to LDAP directory groups, which are useful when LDAP nested groups are configured. When specifying the search context for an LDAP directory group, the exact context is not required. For example, if a group's location is ou=OU2,ou=OU1,dc=hp,dc=com, the higher-level search context ou=OU1,dc=hp,dc=com can be used to locate that group. This feature helps circumvent the length limit of search contexts. For more information about nested groups, see **Directory Groups Configuration screen**.

Field	Possible value	Description
Directory Server Address	IPv4 Address: ###.###.###.### where ### ranges from 0 to 255 or DNS name of the directory server or the name of the domain. IPv6 Address: ####:####:####:####:####:####:####:####, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.	The IP address or the DNS name or the name of the domain of the directory service. This field is required.
Directory Server SSL Port	1 to 65535	The port used for LDAP communications. Port 636 is the standard SSL LDAP port. This field is required.
Search Context 1	All characters except " (quotes), not to exceed 127 characters	First searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 2	All characters except " (quotes), not to exceed 127 characters	Second searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 3	All characters except " (quotes), not to exceed 127 characters	Third searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 4	All characters except " (quotes), not to exceed 127 characters	Fourth searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 5	All characters except " (quotes), not to exceed 127 characters	Fifth searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 6	All characters except " (quotes), not to exceed 127 characters	Sixth searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.

- **Use NT Account Name Mapping (DOMAIN\username)**—Select this check box to enable NT name mapping. This field enables users to log in by using the NT `domain\username` format. The Onboard Administrator may be optionally configured to search the Directory Server Global Catalog and locate the authenticated user information and associated authorized groups. The standard Directory Server GC SSL Port is 3269. This field is optional, and if left blank, the global catalog is not used.

IMPORTANT:

If NT Account Name Mapping is used with the global catalog, and the search context is not restrictive enough, or the domain name is not specified, the Onboard Administrator may associate the authenticated user with a user account that has the same name in a different domain. The authenticated user would then receive the authorization of the user in the other domain. To avoid ambiguity when logging on LDAP user, select search contexts or provide the domain name.

NOTE:

If NT Account Name Mapping is used with the global catalog, and cannot be resolved to a single user, then the user is not authorized to access the Onboard Administrator. This may occur with search contexts that are not restrictive enough and if multiple accounts with the same name exist in different domains. To avoid ambiguity, select search contexts.

Password rules enforced on LDAP servers might be different than password rules enforced for local user accounts. Make sure both sets of rules adhere to security policies.

To apply settings, click **Next**.

Onboard Administrator Network Settings

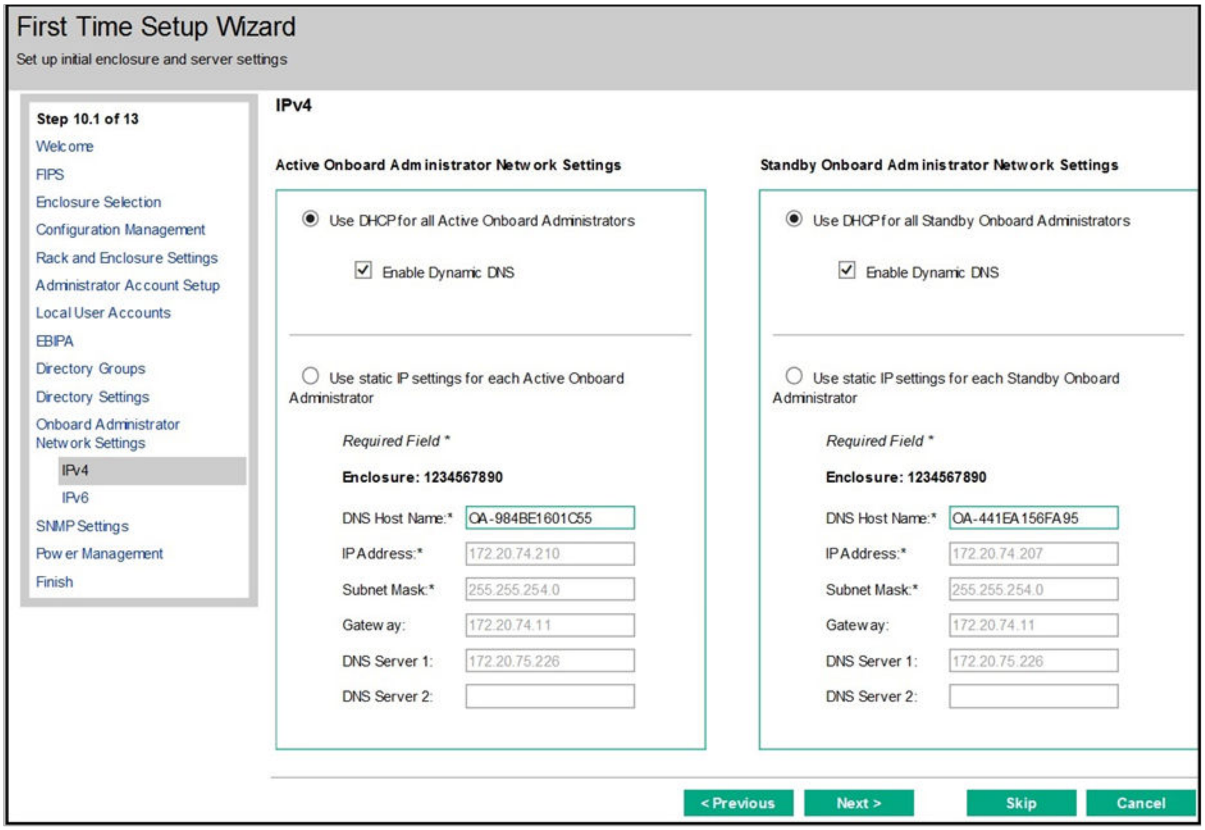
To modify network settings for all the Onboard Administrator modules in the selected enclosures, use the Onboard Administrator Network Settings IPv4 or IPv6 screens. Each screen allows you to configure network settings for the Active Onboard Administrator and the Standby Onboard Administrator. Settings for Standby Onboard Administrator modules only appear if the modules are present.

Changing network settings on the Onboard Administrator that you are signed in to might disconnect you from the Onboard Administrator, in which case after applying the settings, you will have to sign in to the Onboard Administrator again.

To continue, click **Next**.

If you do not want to change network settings, click **Skip**.

First Time Setup Wizard IPv4 Network Settings



First Time Setup Wizard

Set up initial enclosure and server settings

IPv4

Active Onboard Administrator Network Settings

● Use DHCP for all Active Onboard Administrators

☑ Enable Dynamic DNS

○ Use static IP settings for each Active Onboard Administrator

*Required Field **

Enclosure: 1234567890

DNS Host Name:* OA-984BE1601C55
IP Address:* 172.20.74.210
Subnet Mask:* 255.255.254.0
Gateway: 172.20.74.11
DNS Server 1: 172.20.75.226
DNS Server 2:

Standby Onboard Administrator Network Settings

● Use DHCP for all Standby Onboard Administrators

☑ Enable Dynamic DNS

○ Use static IP settings for each Standby Onboard Administrator

*Required Field **

Enclosure: 1234567890

DNS Host Name:* OA-441EA156FA95
IP Address:* 172.20.74.207
Subnet Mask:* 255.255.254.0
Gateway: 172.20.74.11
DNS Server 1: 172.20.75.226
DNS Server 2:

Figure 1: First Time Setup Wizard IPv4 Network Settings screen

The Onboard Administrator allows the IPv4 network configuration to be based either on dynamically assigned IP addresses obtained from a DHCP server or on static IP addresses that you specify manually. You choose the basis for network configuration by selecting the appropriate radio button. If you choose DHCP, you can enable Dynamic DNS.

- **Use DHCP for all Active (or Standby) Onboard Administrator** —Obtains the IP address for the Onboard Administrator from a DHCP server. The Standby check box is only shown if there is a Standby Onboard Administrator in the enclosure.
- **Enable Dynamic DNS**—Enables you to use the same host name for the Onboard Administrator over time, although the dynamically assigned IP address might change. The host name is registered with a DNS server. DDNS updates the DNS server with new or changed records for IP addresses.

  Disabling Dynamic DNS on the Onboard Administrator stops the Onboard Administrator's updates to the DNS server. However, note that some DHCP servers may have a provision to update DNS servers directly. To completely disable Dynamic DNS updates, disable Dynamic DNS both at the Onboard Administrator as well as at the DHCP server.
- **Use static IP settings for each Active (or Standby) Onboard Administrator** —Manually set up static IP settings for the Onboard Administrator. The Standby check box is only shown if there is a Standby Onboard Administrator in the enclosure.

CAUTION:

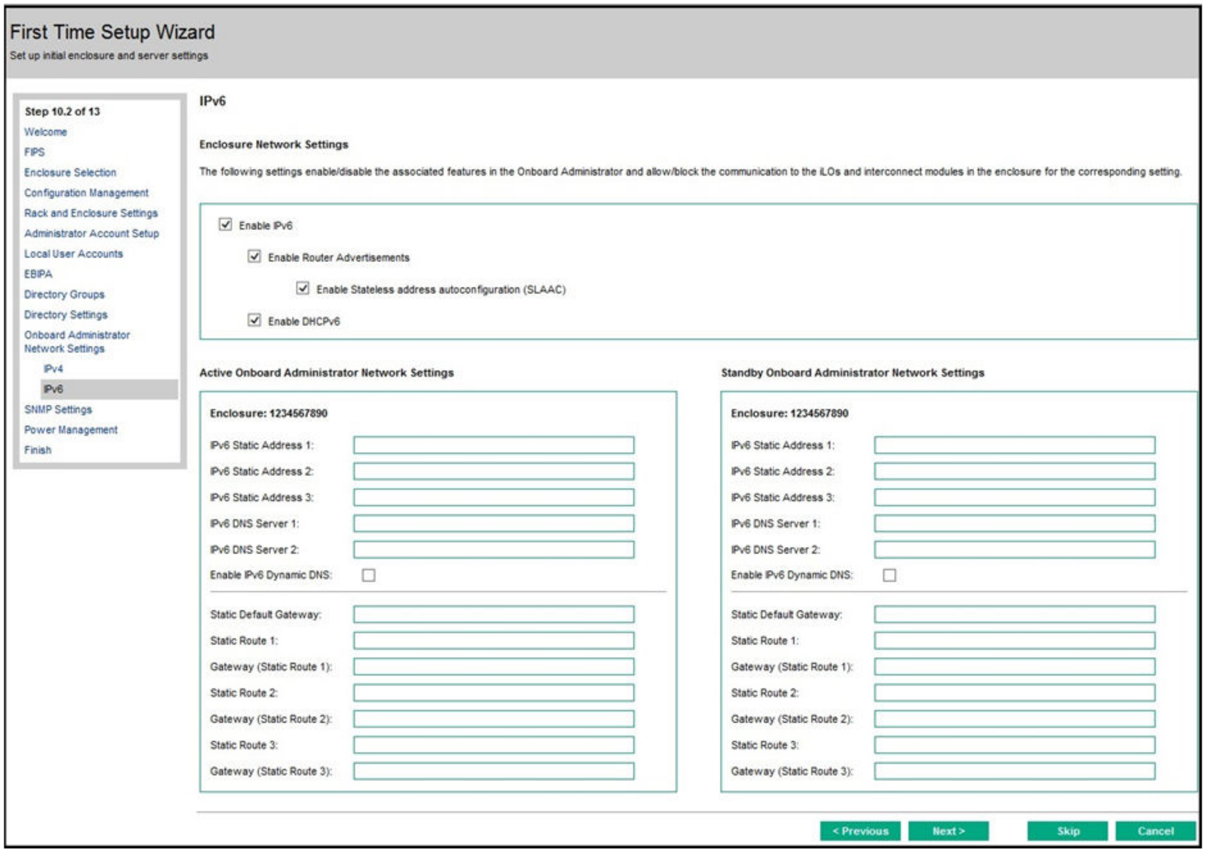
When enabling DHCP for IPv4, any static IPv4 settings are lost.

Field	Possible value	Description
DNS Host Name	1 to 32 characters including all alphanumeric characters, the dash (-), and the underscore (_).	The Onboard Administrator DNS host name. This setting applies to both IPv4 and IPv6 environments. The DNS host name can be assigned when using either DHCP or static IP settings. Changing the Onboard Administrator DNS Name could cause a host name mismatch on the SSL certificate. You may have to update the certificate information on the affected Onboard Administrator, using the **Active Onboard Administrator Certificate Administration screen** or the **Standby Onboard Administrator Certificate Administration screen** , as appropriate.
IP Address	###.###.###.### where ### ranges from 0 to 255	Static IP address for the Onboard Administrator (required if static IP settings is selected).
Subnet Mask	###.###.###.### where ### ranges from 0 to 255	Subnet mask for the Onboard Administrator (required if static IP settings is selected).
Gateway	###.###.###.### where ### ranges from 0 to 255	Gateway address for the Onboard Administrator (required if static IP settings is selected).
DNS Server 1	###.###.###.### where ### ranges from 0 to 255	The IP address for the primary IPv4 DNS server. [1]
DNS Server 2	###.###.###.### where ### ranges from 0 to 255	The IP address for the secondary IPv4 DNS server. [1]

[1] ** The order in which the Onboard Administrator uses DNS servers is described in* **IPv4 Settings tab**.

To save new IPv4 settings, click **Next**.

First Time Setup Wizard IPv6 Network Settings



IPv6

Enclosure Network Settings

The following settings enable/disable the associated features in the Onboard Administrator and allow/block the communication to the iLOs and interconnect modules in the enclosure for the corresponding setting.

☑ Enable IPv6

☑ Enable Router Advertisements

☑ Enable Stateless address autoconfiguration (SLAAC)

☑ Enable DHCPv6

Active Onboard Administrator Network Settings

Enclosure: 1234567890

IPv6 Static Address 1:

IPv6 Static Address 2:

IPv6 Static Address 3:

IPv6 DNS Server 1:

IPv6 DNS Server 2:

Enable IPv6 Dynamic DNS: □

Static Default Gateway:

Static Route 1:

Gateway (Static Route 1):

Static Route 2:

Gateway (Static Route 2):

Static Route 3:

Gateway (Static Route 3):

Standby Onboard Administrator Network Settings

Enclosure: 1234567890

IPv6 Static Address 1:

IPv6 Static Address 2:

IPv6 Static Address 3:

IPv6 DNS Server 1:

IPv6 DNS Server 2:

Enable IPv6 Dynamic DNS: □

Static Default Gateway:

Static Route 1:

Gateway (Static Route 1):

Static Route 2:

Gateway (Static Route 2):

Static Route 3:

Gateway (Static Route 3):

Figure 2: First Time Setup Wizard IPv6 Network Settings screen

IPv6 supports multiple addresses. You can enable any combination of the network settings. With IPv6, SLAAC and/or DHCPv6 enabled, the Onboard Administrator can obtain IP addresses from all the selected sources. It can have both automatically assigned and user-specified static IP addresses. The **Enable SLAAC**, **Enable DHCPv6**, and **Enable Router Advertisements** settings take effect only if IPv6 is enabled.

- **Enable IPv6**—Enables IPv6 protocol for all Onboard Administrator, interconnect, and server iLO modules in the enclosure.
- **Enable Router Advertisements**—Allows IPv6 router advertisements from the external management network onto the internal enclosure management network. If you disable this setting, the Onboard Administrator blocks IPv6 router advertisements sent from the external management network, preventing them from entering the internal enclosure management network.
- **Enable SLAAC**—Enables IPv6 Stateless address autoconfiguration messages to all Onboard Administrator, interconnect, and server iLO modules in the enclosure. This feature affects only global IPv6 addresses.
- **Enable DHCPv6**—Enables the active (and standby, if configured) Onboard Administrator to request a DHCPv6 IP address. Allows DHCPv6 traffic on the enclosure management network.

△ **CAUTION:**

If you disable IPv6 in an IPv6-only environment, you will lose your connection to the Onboard Administrator GUI and any SSH sessions. To reestablish your connection, you must perform the initial enclosure configuration via IPv4 networking, the Insight Display, or the Onboard Administrator serial console interface. When disabling IPv6, SLAAC, or DHCPv6, all connections that depend on the disabled protocol are closed. For example, if you are connected to the Onboard Administrator using its DHCPv6-assigned address, disabling the enclosure DHCPv6 setting results in your session being closed.

NOTE:

For SLAAC addresses to be successfully configured, the **Enable SLAAC** and **Enable Router Advertisements** settings must be enabled on the enclosure. In addition, an IPv6 router must be configured on the enclosure management network to provide the SLAAC addresses via router advertisements. Any iLOs may need to be configured separately to obtain SLAAC addresses. The **Enable SLAAC**, **Enable Router Advertisements**, and **Enable IPv6** settings must be enabled to allow the necessary traffic on the enclosure management network.

For DHCPv6 addresses to be successfully configured, the **Enable IPv6** enclosure setting must be enabled and a DHCPv6 server configured on the management network. Any iLOs and interconnects must be configured separately to request a DHCPv6 address. If they are configured to request DHCPv6 addresses, the **Enable IPv6** and **Enable DHCPv6** settings must be enabled to allow the necessary traffic on the enclosure management network.

After a factory reset, the enclosure IPv6 network settings for IPv6, SLAAC, DHCPv6, and Router Advertisements are enabled by default.

When the Enable DHCPv6, Enable Router Advertisements, or Enable SLAAC enclosure IPv6 settings are disabled on the Onboard Administrator, the respective DHCPv6 or SLAAC addresses of the iLOs in the enclosure are retained until these addresses expire automatically based on their respective configurations. A manual reset of the iLO releases these addresses immediately.

Field	Possible value	Description
IPv6 Static Address 1	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128. [1 2]	Onboard Administrator external NIC IPv6 address 1.
IPv6 Static Address 2	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1,2]	Onboard Administrator external NIC IPv6 address 2.
IPv6 Static Address 3	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1,2]	Onboard Administrator external NIC IPv6 address 3.
IPv6 DNS Server 1	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128. The prefix is optional.[1]	The IPv6 address for the first Static IPv6 DNS server. [3]

Table Continued

Field	Possible value	Description
IPv6 DNS Server 2	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128. The prefix is optional.[1]	The IPv6 address for the second Static IPv6 DNS server.[3]
Enable IPv6 Dynamic DNS	Enabled (check box selected) or disabled (check box cleared).	Enables you to use a host name for the Onboard Administrator that persists even when the dynamically assigned IP address might change. The host name is registered with a DNS server. Dynamic DNS updates the DNS server with new or changed records for IP addresses. [4] Disabling Dynamic DNS on the Onboard Administrator stops the Onboard Administrator's updates to the DNS server. However, note that some DHCP servers may have a provision to update DNS servers directly. To completely disable Dynamic DNS updates, disable Dynamic DNS both at the Onboard Administrator as well as at the DHCP server.
Static Default Gateway	####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. Do not specify a prefix. The gateway must be reachable from within the Onboard Administrator network.[1]	The static IPv6 address for the default gateway. This setting is required in an IPv6 network environment configured to be fully static. The Onboard Administrator can accept IPv6 gateway configuration directly via this setting and, if router advertisements are configured, via router advertisements from IPv6 routers on the management network. If router advertisements provide IPv6 gateway configuration, the gateway configuration provided by router advertisements overrides the static IPv6 gateway setting. The IPv6 gateway currently in use by the Onboard Administrator is displayed in the Current Default Gateway field on the **Active Onboard Administrator TCP/IP Settings** screen and the Standby Onboard Administrator TCP/IP Settings screen.

Table Continued

Field	Possible value	Description
Static Route 1	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1]	Adds an IPv6 static route to the Onboard Administrator's routing table (manual configuration). [5] The static route defines an explicit path that the Onboard Administrator uses to reach an external network through a gateway. In a static network configuration, the static route removes the need to configure the router to send route information via router advertisements. If router advertisements are active in the network, and the default gateway is already configured, the router informs all nodes about the available static routes, thereby making manual configuration of the static routes unnecessary. If you specify the Static Route 1, you must also specify the associated Gateway (Static Route 1).
Gateway (Static Route 1)	####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. Do not specify a prefix. The gateway must be reachable from both the Onboard Administrator network and the external network.[1]	The IPv6 address of the gateway using the path defined by Static Route 1. You must also specify Static Route 1.
Static Route 2	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1]	Adds a second IPv6 static route to the Onboard Administrator's routing table (manual configuration). If you specify the Static Route 2, you must also specify the associated Gateway (Static Route 2).
Gateway (Static Route 2)	####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. Do not specify a prefix. The gateway must be reachable from both the Onboard Administrator network and the external network.[1]	The IPv6 address of the gateway using the path defined by Static Route 2. You must also specify Static Route 2.

Table Continued

Field	Possible value	Description
Static Route 3	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1]	Adds a third IPv6 static route to the Onboard Administrator's routing table (manual configuration). If you specify the Static Route 3, you must also specify the associated Gateway (Static Route 3).
Gateway (Static Route 3)	####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. Do not specify a prefix. The gateway must be reachable from both the Onboard Administrator network and the external network.[1]	The IPv6 address of the gateway, using the path defined by Static Route 3. You must also specify Static Route 3.

[1] A compressed version of the same IPv6 address is also supported.

[2] The Onboard Administrator does not accept a link local address as an IPv6 Static address.

[3] The order in which the Onboard Administrator uses DNS servers is described in **IPv6 Settings tab**.

[4] IPv6 Dynamic DNS requires that a valid DNS server (either IPv4 or IPv6) be configured on the Onboard Administrator.

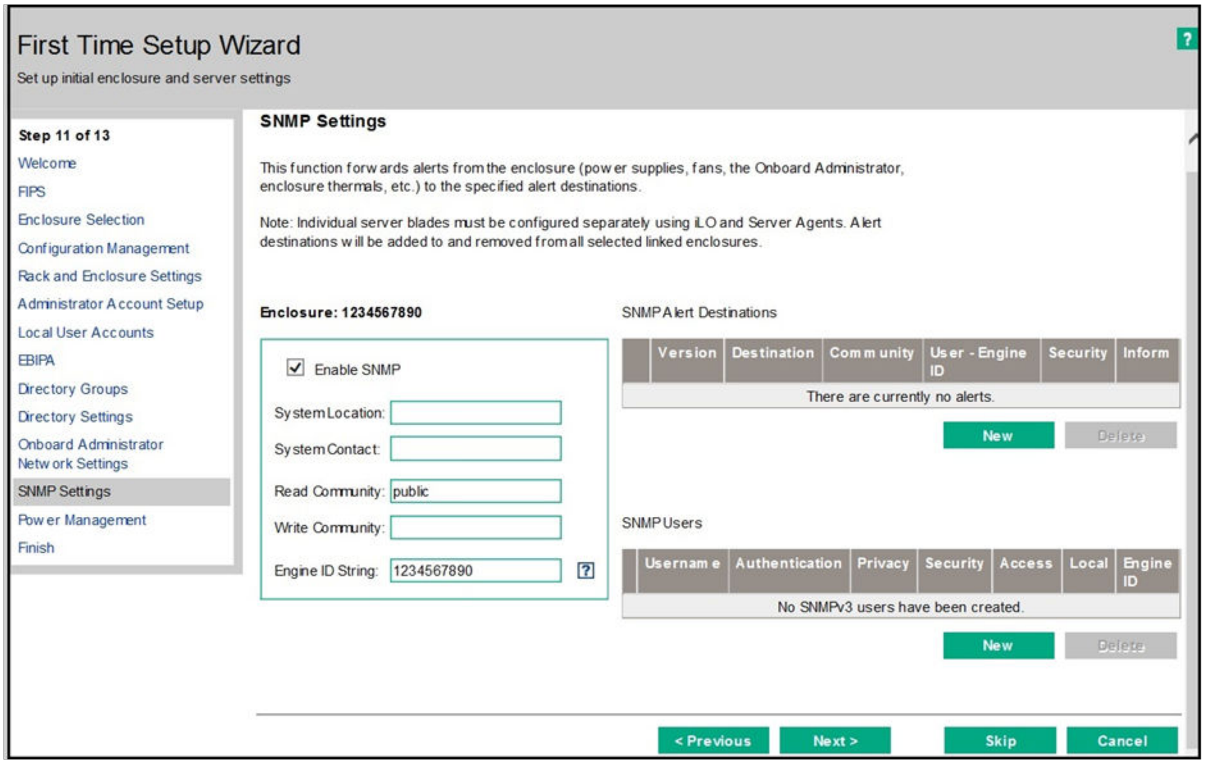
[5]

CAUTION:
Adding or removing a static route can result in loss of connectivity for clients accessing the Onboard Administrator.

To save new IPv6 settings, click **Next**.

Enclosure SNMP Settings screen

Use the Enclosure SNMP Settings screen to configure or modify the SNMP settings for the active Onboard Administrator.



First Time Setup Wizard

Set up initial enclosure and server settings

Step 11 of 13

- Welcome
- FIPS
- Enclosure Selection
- Configuration Management
- Rack and Enclosure Settings
- Administrator Account Setup
- Local User Accounts
- EBIPA
- Directory Groups
- Directory Settings
- Onboard Administrator Network Settings
- SNMP Settings
- Power Management
- Finish

SNMP Settings

This function forwards alerts from the enclosure (power supplies, fans, the Onboard Administrator, enclosure thermals, etc.) to the specified alert destinations.

Note: Individual server blades must be configured separately using iLO and Server Agents. Alert destinations will be added to and removed from all selected linked enclosures.

Enclosure: 1234567890

☑ Enable SNMP

System Location:

System Contact:

Read Community: public

Write Community:

Engine ID String: 1234567890

SNMP Alert Destinations

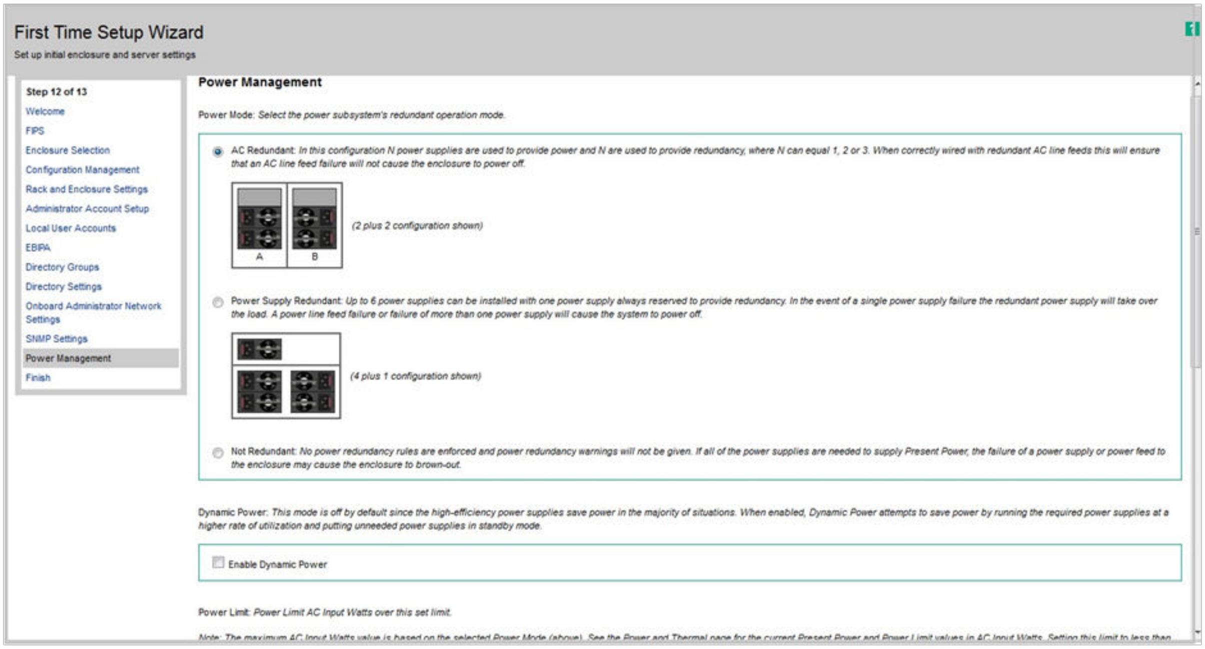
	Version	Destination	Community	User - Engine ID	Security	Inform
There are currently no alerts.						

SNMP Users

	Username	Authentication	Privacy	Security	Access	Local	Engine ID
No SNMPv3 users have been created.							

For possible values and descriptions of each field, see **SNMP Settings**.

Power Management screen



First Time Setup Wizard

Set up initial enclosure and server settings

Step 12 of 13

- Welcome
- FIPS
- Enclosure Selection
- Configuration Management
- Rack and Enclosure Settings
- Administrator Account Setup
- Local User Accounts
- EBIPA
- Directory Groups
- Directory Settings
- Onboard Administrator Network Settings
- SNMP Settings
- Power Management
- Finish

Power Management

Power Mode: *Select the power subsystem's redundant operation mode.*

● AC Redundant: *In this configuration N power supplies are used to provide power and N are used to provide redundancy, where N can equal 1, 2 or 3. When correctly wired with redundant AC line feeds this will ensure that an AC line feed failure will not cause the enclosure to power off.*

(2 plus 2 configuration shown)

○ Power Supply Redundant: *Up to 6 power supplies can be installed with one power supply always reserved to provide redundancy. In the event of a single power supply failure the redundant power supply will take over the load. A power line feed failure or failure of more than one power supply will cause the system to power off.*

(4 plus 1 configuration shown)

○ Not Redundant: *No power redundancy rules are enforced and power redundancy warnings will not be given. If all of the power supplies are needed to supply Present Power, the failure of a power supply or power feed to the enclosure may cause the enclosure to brown-out.*

Dynamic Power: *This mode is off by default since the high-efficiency power supplies save power in the majority of situations. When enabled, Dynamic Power attempts to save power by running the required power supplies at a higher rate of utilization and putting unneeded power supplies in standby mode.*

□ Enable Dynamic Power

Power Limit: *Power Limit AC Input Watts over this set limit.*

Note: The maximum AC Input Watts value is based on the selected Power Mode (above). See the Power and Thermal page for the current Present Power and Power Limit values in AC Input Watts. Setting this limit to less than

IMPORTANT:

If redundancy mode is set to DC Redundant, AC Redundant, or Power Supply Redundant, and power redundancy is lost, then you must either add additional power supplies or change the redundancy mode setting in the Onboard Administrator to restore Power Subsystem status. See the Insight Display for corrective steps.

To change the power redundancy mode, you must disable EDPC. After changing the power redundancy mode, reset EDPC based on the new ranges.

Power management options

The BladeSystem c3000 and c7000 Enclosure power management systems enable you to configure the enclosure to meet your needs. You can choose from the different power management options on the Onboard Administrator Power Management screen. These power management options are explained in the following table.

Power management option	Insight Display name	Description
Power mode (power redundancy mode)		
Redundant or AC Redundant	Redundant or AC Redundant	The OA detects the type of power supplies present, automatically adapts the power mode behavior accordingly, and displays the corresponding mode name: • If DC power supplies are present: Redundant mode • If AC power supplies are present: AC Redundant mode Also known as N+N redundancy or grid redundancy. N power supplies are used to provide power and N are used to provide redundancy (where N can equal 1, 2, or 3). Up to three power supplies can fail without causing the enclosure to fail. When correctly wired with redundant AC or DC line feeds, this configuration also ensures that an AC or DC line feed failure does not cause the enclosure to power off. In the unlikely event that more than one power supply is unable to provide power because of multiple power supply failures or a power grid failure, the system might power down. The system powers down when the surviving power supplies do not have enough power to meet the system's power requirements.

Table Continued

Power management option	Insight Display name	Description
Power Supply Redundant	Power Supply	For all power supplies. This mode supports two to six power supplies. Also known as N+1 redundancy. With this power mode, N power supplies are used to provide power and 1 is used to provide redundancy (where N can equal 1, 2, 3, 4, or 5). If using a c7000 Enclosure 3-phase power input module, Hewlett Packard Enterprise recommends 3 or 6 active power supplies (2+1 or 5+1) for proper phase balancing. This power mode is designed to protect the system from one power supply failing. In the unlikely event that more than one power supply is unable to provide power because of multiple power supply failures or a power grid failure, the system might power down. The system powers down when the surviving power supplies do not have enough power to meet the system's power requirements.
Not Redundant	None	For all power supplies. This mode supports 1 to 6 power supplies. With this power mode, N power supplies are used to provide power and none are used to provide redundancy (where N can equal 1, 2, 3, 4, 5, or 6). If using a c7000 Enclosure 3-phase power input module, Hewlett Packard Enterprise recommends 3 or 6 active power supplies for proper phase balancing. There is no power redundancy, and no power redundancy warnings are given. If a power supply is unable to provide power because of a power supply failure or a grid failure, the system might power down. It will power down if the surviving power supplies do not have enough power to meet the system's power requirements. This power mode is not recommended for deployed systems in production environments.
Dynamic Power mode (enabled or disabled)		
Dynamic Power	Dynamic Power	If enabled, Dynamic Power automatically places unused power supplies in standby mode to increase enclosure power supply efficiency, thereby minimizing enclosure power consumption during lower power demand. Increased power demands automatically return standby power supplies to full performance. More information about Dynamic Power follows this table.
Power Limit mode		

Table Continued

Power management option	Insight Display name	Description
Enclosure Dynamic Power Cap	None	Allows specifying a limit for the enclosure power consumption. The power draw is limited by dynamically managing server blade power caps to stay under the overall enclosure power cap. For more information, see the Power Limit table that follows.
Static Power Limit	Power Limit	An optional setting to limit power. Whenever you attempt to power on a device, the total power demands of the new device and of the devices already on are compared against this Static Power Limit. If the total power demands exceed the limit, the new device is prevented from powering on. For more information about the Static Power Limit and how it compares to the Enclosure Dynamic Power Cap, see the Power Limit table that follows.

NOTE:

Independent of the redundancy mode enabled, all operational power supplies present in the enclosure are typically active and share in delivering the enclosure power needs. If Dynamic Power mode is enabled, some power supplies might automatically be placed on standby to increase overall enclosure power efficiency. For more information, see the discussion of Dynamic Power mode that follows.

The Onboard Administrator allows you to change the power (redundancy) mode setting after the enclosure and devices are powered up. If the power mode is changed, the Onboard Administrator updates the redundancy status as needed, reporting degraded/failed redundancy if applicable. For example, the original power mode was Power Supply Redundant (N+1) when all blades powered on and then was changed to AC Redundant (N+N) reducing the Power Capacity as seen by the Onboard Administrator. As long as enough power is available, all blades will remain operational. However, under some circumstances a blade will not be powered on, such as when it is replacing another server blade. Additional information is provided in the table and sections that follow.

Dynamic Power—The default setting is Disabled. The following selections are valid:

- Enabled—Some power supplies can be automatically placed on standby to increase overall enclosure power subsystem efficiency.
- Disabled—All power supplies share the load. The power subsystem efficiency varies based on load.

NOTE:

Dynamic Power is supported with all c3000 power supplies. It is supported with all c7000 power supplies except those operating with low-line input voltage (nominal 100-120V AC).

For OA v4.01 and later, the factory default value associated with the Dynamic Power setting was changed from enabled to disabled. The operating efficiency of the currently available HPE Gold (92% efficient) and HPE Platinum (94% efficient) enclosure power supplies makes this firmware-based power management strategy unnecessary. The Dynamic Power setting is recommended only for enclosure power supplies with an efficiency value less than 92%. When upgrading to OA v4.01 or later, the current Dynamic Power setting is retained after the upgrade. For more information, see the **Customer Advisory c03957955**.

Power Limit

Do not set a Static Power Limit or Enclosure Dynamic Power Cap on an empty enclosure.

Mode	Insight Display name	Description
Enclosure Dynamic Power Cap	None	An optional feature that enables you to cap the servers in an enclosure as a group. As the servers run, the demand for power varies for each server. A power cap for each server is automatically adjusted to provide the server with enough power to meet workload demands while still conforming to the Enclosure Dynamic Power Cap. A redundant OA board is required for setting the Dynamic Power Cap feature. The feature is enabled with three configuration parameters: • Dynamic Power Cap—Total enclosure average power will not exceed Dynamic Power Cap. • Derated Circuit Capacity—Average power on a single circuit will not exceed Derated Circuit Capacity. • Rated Circuit Capacity—Peak power on a single circuit will not exceed Rated Circuit Capacity. When configuring these parameters, the Derated Circuit Capacity must be at least as large as the Dynamic Power Cap and no larger than the Rated Circuit Capacity. The Dynamic Power Cap is used to limit the enclosure power consumption based on a cooling constraint that might be lower than the Derated Circuit Capacity. The Derated Circuit Capacity is used to limit the enclosure average power consumption on a circuit. The Rated Circuit Capacity is used to limit the enclosure peak power consumption on a circuit. If you need to restrict an enclosure electrical load and thermal output, an Enclosure Dynamic Power Cap is better than a Static Power Limit. Enclosure Dynamic Power Cap enables more blades to power on than a Static Power Limit.
Static Power Limit	Power Limit	An optional setting to limit power. Whenever you attempt to power on a device, the total power demands of the new device and of the devices already on are compared against this Static Power Limit. If the total power demands exceed the limit, the new device is prevented from powering on. A Static Power Limit is better when: • You do not want caps dynamically adjusted on your blades. • You prefer to not power on a server blade if it cannot be allocated full power (even if it typically consumes less). • More than 1/4 of the blades in the enclosure do not meet hardware or firmware requirements for the Enclosure Dynamic Power Cap.
None	None	The enclosure power usage is not managed or capped.

Understanding power capping varieties

Hewlett Packard Enterprise delivers three varieties of power management that enable users to limit the server power consumption. All three power capping varieties work to limit your consumption to a specified Watt or Btu/hr goal. The three technologies are Power Capping, Dynamic Power Capping, and Enclosure Dynamic Power Capping.

Power Capping

In May 2007, Hewlett Packard Enterprise launched Power Capping technology with iLO 2 version 1.30. This firmware-based technology limits the average power consumption of the server to a user-defined Watt or Btu/hr goal. Because this technology runs in firmware, it cannot limit power consumption rapidly enough to ensure protection of PDU-level circuit breakers. Power Capping does limit power consumption rapidly enough to protect cooling infrastructure, so it is an effective solution for data centers experiencing cooling capacity constraints. Power Capping is supported on any ProLiant server or blade that has an iLO management processor and power measurement capabilities. Using Power Capping requires iLO 2 version 1.30 (or later) firmware and an updated system ROM/BIOS.

Dynamic Power Capping

Dynamic Power Capping is a hardware-based technology that limits power consumption fast enough to protect circuit breakers and cooling infrastructure. Hewlett Packard Enterprise launched Dynamic Power Capping in December of 2008 with iLO 2 version 1.70. Supported servers contain an internal hardware circuit that monitors server power consumption on a sub-second basis. If server power consumption approaches the power cap limit set in iLO, the internal hardware circuit limits power consumption rapidly enough to protect PDU-level circuits from over-subscription and prevent power-related server outages.

Dynamic Power Capping requires specific hardware on the system board. Dynamic Power Capping also requires iLO 2 version 1.70 (or later) firmware and a system ROM/BIOS dated 10/1/2008 (or later). iLO automatically updates firmware in the Dynamic Power Capping hardware power circuit.

Dynamic Power Capping is supported on the following BladeSystem server blades:

- BL260c G5 (Notes: 2)
- BL2x220 G5 (Notes: 2)
- BL460c G1 (Notes: 1 and 2)
- BL460c G5 (Notes: 2)
- BL465c G5 (Notes: 2)
- BL495c G5 (Notes: 2)
- BL685c G5 (Notes: 2)
- All G6 server blades
- All G7 server blades
- All G8 server blades

Additional information

- These systems require Quad-Core capable system boards to support Dynamic Power Capping.
- When implementing power capping for BladeSystem, Hewlett Packard Enterprise recommends using Enclosure Dynamic Power Capping set through the Onboard Administrator. To use Enclosure Dynamic Power Capping, you must upgrade iLO 2 firmware to version 1.70 or later and are encouraged to update system ROM to version 10/1/2008 or later. For some older BL460c Servers, the iLO firmware might not be able to automatically update the Dynamic Power Capping hardware circuit. In these instances, Onboard Administrator compensates for the absence of the internal hardware circuit and continues to guarantee circuit protection.

Enclosure Dynamic Power Capping

Enclosure Dynamic Power Capping combines the power capping technology of the BladeSystem server with a power balancing control algorithm in the Onboard Administrator to maximize the aggregate performance of the enclosure. Enclosure Dynamic Power Capping protects your circuit breakers and maximizes your performance.

Using Enclosure Dynamic Power Capping, you set a power cap for the entire enclosure. The Onboard Administrator allocates individual limits to each participating server blade. The server blades manage consumption to that limit. The Onboard Administrator continuously monitors power consumption requirements for each server blade and continuously rebalances the individual limits to ensure that busy server blades receive more power than idle server blades. This power allocation improves aggregate enclosure performance.

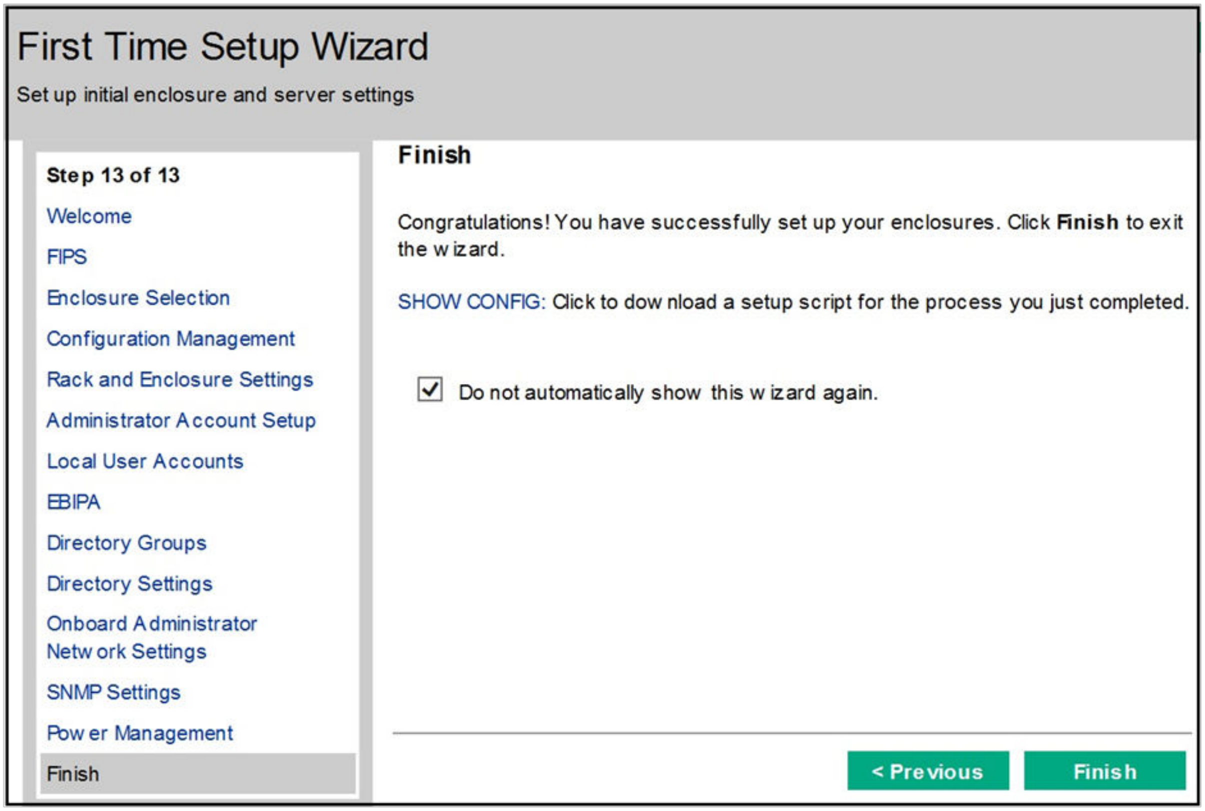
BladeSystem server power caps are set in the Onboard Administrator. Enclosure Dynamic Power Capping protects both cooling and electrical infrastructures. Enclosure Dynamic Power Capping works with either firmware-based power capping technology on the server or with the fast, hardware-based technology. The Enclosure Dynamic Power Capping solution performs better if the server blades that support the fast, hardware-based capping technology are upgraded.

Enclosure Dynamic Power Capping requires Onboard Administrator 2.30 (or later), iLO 2 version 1.70 (or later), and System ROM/BIOS dated 10/1/2008 (or later).

NOTE:

Power caps set for less than 50% of the difference between maximum power and idle power might become unreachable due to changes in the server. Power caps set for less than 20% are not recommended, and might cause the server to reboot or the server operating system to stop responding.

Finish



First Time Setup Wizard

Set up initial enclosure and server settings

Finish

Congratulations! You have successfully set up your enclosures. Click **Finish** to exit the wizard.

SHOW CONFIG: Click to download a setup script for the process you just completed.

☑ Do not automatically show this wizard again.

To view a current configuration for the enclosure:

1. Click the **SHOW CONFIG** link. The configuration opens in a new browser window.
2. To save the configuration as a text file, choose one of the following options:

- If you use Microsoft Internet Explorer, select **Save As**.
- If you use Mozilla Firefox, select **Save Page As**.
- If you use Google Chrome, select **Save Link As**.

For security, the retrieved current configuration does not contain any user passwords. You can manually edit the script to add the user passwords after the user name on the ADD USER lines. Also, the retrieved current configuration does not contain any of the LCD settings (Lock Buttons, Enable PIN Protection, and PIN Code). These settings cannot be added from the configuration script.

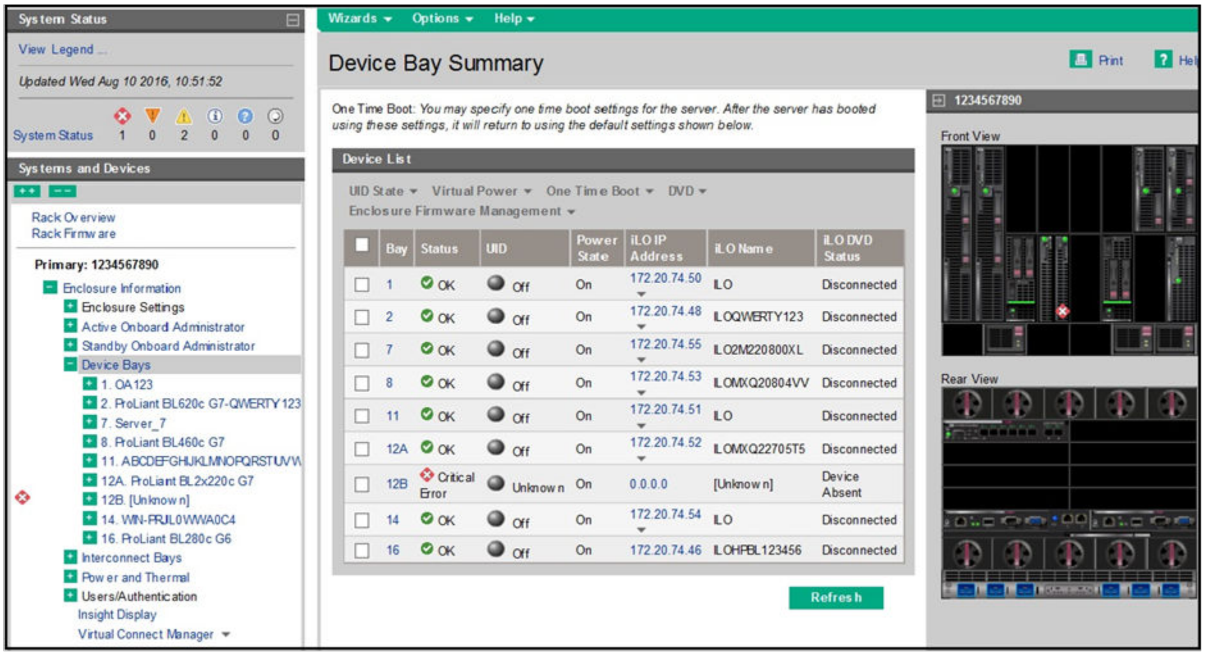
To force the First Time Setup Wizard to run again the next time a user signs into the Onboard Administrator, clear the **Do not automatically start this wizard again** check box.

To save and exit the First Time Setup Wizard, click **Finish**. The First Time Setup Wizard screen closes and you are returned to the default main screen of HPE BladeSystem Onboard Administrator.

Navigating Onboard Administrator

Navigation overview

The main HPE BladeSystem Onboard Administrator navigation system consists of a tree view on the left side of the screen, which facilitates navigation through the various GUI screens. It remains visible when navigating through the tree. The center of the screen displays status information and parameters that you can modify. The right side of the screen displays a physical picture of the enclosure. You can navigate through enclosure devices and functions using either the tree view or the graphical view.



Updated Wed Aug 10 2016, 10:51:52

System Status	1	0	2	0	0	0

Device Bay Summary

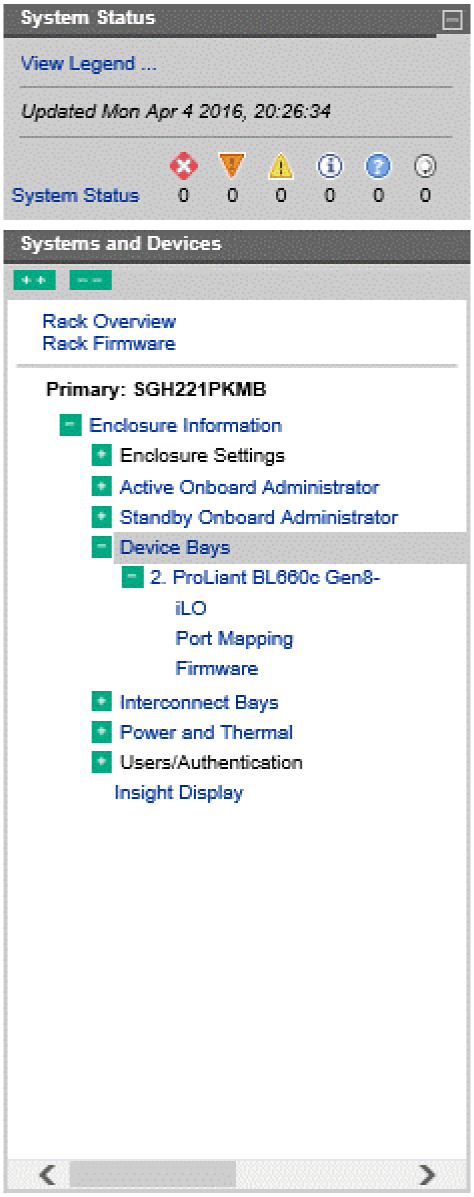
One Time Boot: *You may specify one time boot settings for the server. After the server has booted using these settings, it will return to using the default settings shown below.*

☐	Bay	Status	UID	Power State	iLO IP Address	iLO Name	iLO DVD Status
☐	1	✓ OK	● Off	On	172.20.74.50	ILO	Disconnected
☐	2	✓ OK	● Off	On	172.20.74.48	ILOQWERTY123	Disconnected
☐	7	✓ OK	● Off	On	172.20.74.55	ILO2M220800XL	Disconnected
☐	8	✓ OK	● Off	On	172.20.74.53	ILOMXQ20804VV	Disconnected
☐	11	✓ OK	● Off	On	172.20.74.51	ILO	Disconnected
☐	12A	✓ OK	● Off	On	172.20.74.52	ILOMXQ22705T5	Disconnected
☐	12B	Critical Error	● Unknown	On	0.0.0.0	[Unknown]	Device Absent
☐	14	✓ OK	● Off	On	172.20.74.54	ILO	Disconnected
☐	16	✓ OK	● Off	On	172.20.74.46	ILOHPBL123456	Disconnected

Tree view

The tree view aids in navigating through enclosure devices and functions for multiple enclosures in a Hierarchical manner. The way in which the tree view is rendered depends on several factors including user permissions, device availability, and device status. If a user is configured to be an operator or user, some options might not be visible in the tree view.

The tree views for the c3000 and c7000 enclosures are analogous.



System Status

View Legend ...

Updated Mon Apr 4 2016, 20:26:34

	✖	▼	⚠	ⓘ	?	○
System Status	0	0	0	0	0	0

Systems and Devices

Rack Overview
Rack Firmware

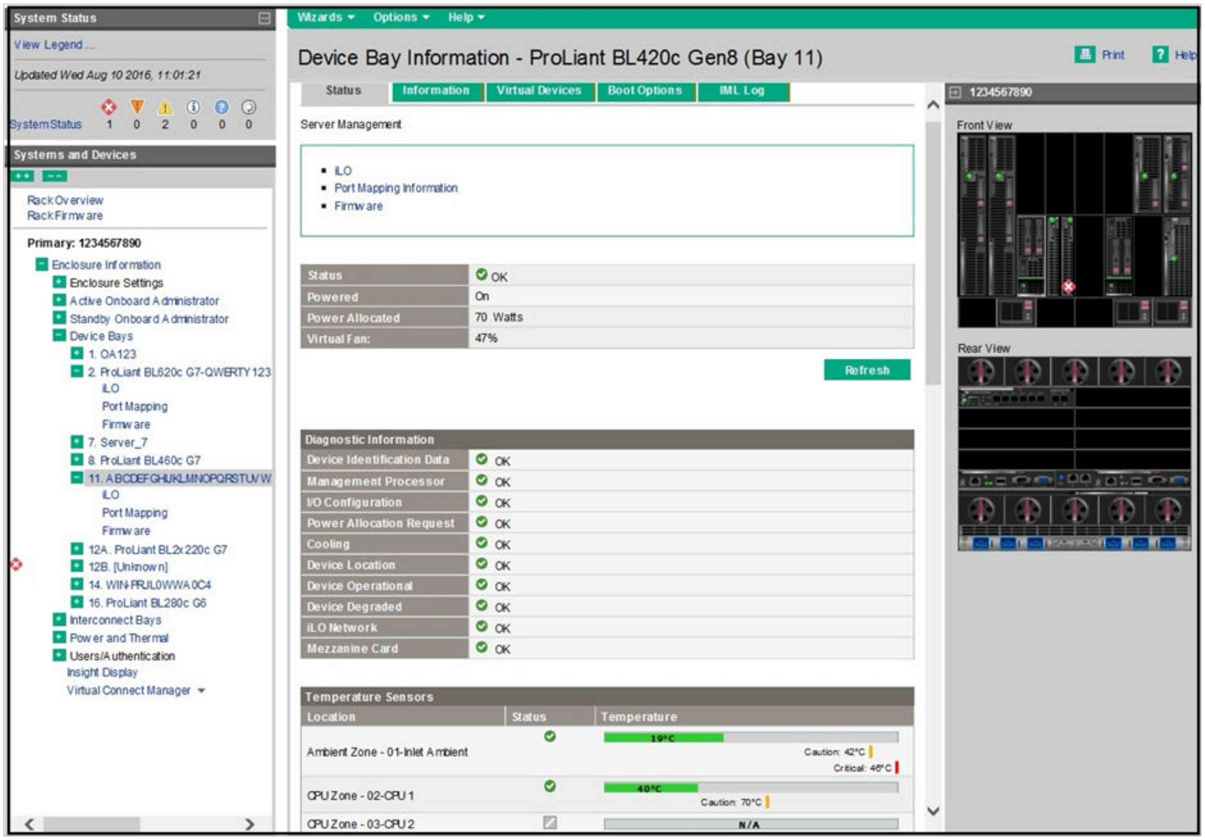
Primary: SGH221PKMB

- ⊟ Enclosure Information
  - ⊞ Enclosure Settings
  - ⊞ Active Onboard Administrator
  - ⊞ Standby Onboard Administrator
  - ⊟ Device Bays
    - ⊟ 2. ProLiant BL660c Gen8-
      - iLO
      - Port Mapping
      - Firmware
  - ⊞ Interconnect Bays
  - ⊞ Power and Thermal
  - ⊞ Users/Authentication
  - Insight Display

The tree view enables navigation, using categories based on the major systems within the enclosure. When a category is expanded by clicking the ⊞ sign to the left of the category, an icon next to the category name can indicate a degraded status of the affected system. In the case of multiple components reporting status, the status icon indicates a cumulative worst-case status of all the devices in the same category.

Individual device pages

Clicking the link for an individual device selects the device, opens the device detail page, and selects the device in the graphical view in the right frame of the GUI. Individual device pages contain detailed information about the selected device and any other functions related to that device.



Device Bay Information - ProLiant BL420c Gen8 (Bay 11)

Server Management

- iLO
- Port Mapping Information
- Firmware

Status	✓ OK
Powered	On
Power Allocated	70 Watts
Virtual Fan:	47%

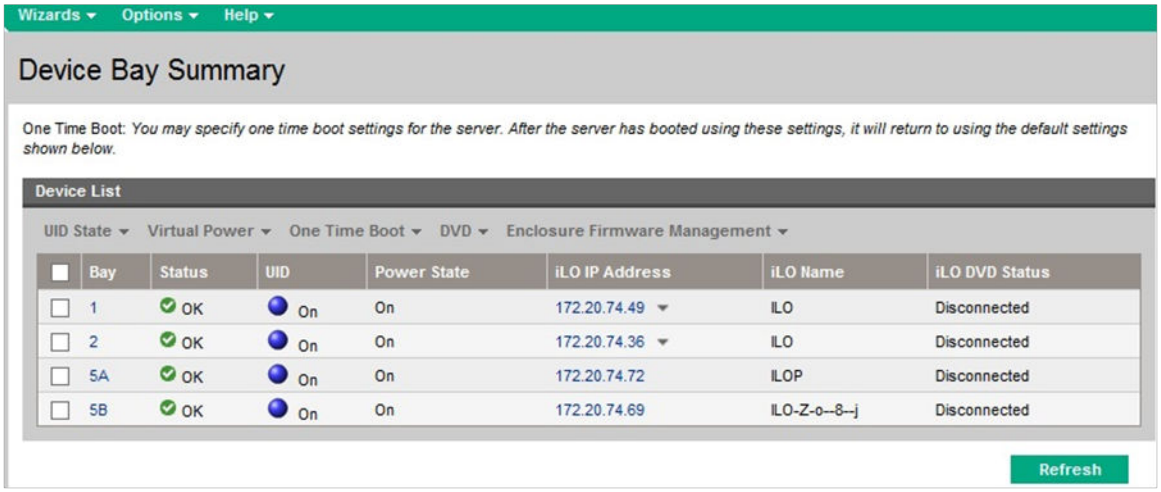
Diagnostic Information	
Device Identification Data	✓ OK
Management Processor	✓ OK
I/O Configuration	✓ OK
Power Allocation Request	✓ OK
Cooling	✓ OK
Device Location	✓ OK
Device Operational	✓ OK
Device Degraded	✓ OK
iLO Network	✓ OK
Mezzanine Card	✓ OK

Temperature Sensors

Location	Status	Temperature
Ambient Zone - 01-Inlet Ambient	✓	19°C Caution: 42°C Critical: 46°C
CPU Zone - 02-CPU 1	✓	40°C Caution: 70°C
CPU Zone - 03-CPU 2		N/A

Category summary pages

Category summary pages contain information for each of the devices in that category. For example, clicking the **Device Bays** link opens a bay summary page. Each parent element in the tree works in this manner. When you click a category summary link, no devices are selected in the graphical view navigation.



Device Bay Summary

One Time Boot: *You may specify one time boot settings for the server. After the server has booted using these settings, it will return to using the default settings shown below.*

☐	Bay	Status	UID	Power State	iLO IP Address	iLO Name	iLO DVD Status
☐	1	✓ OK	● On	On	172.20.74.49	iLO	Disconnected
☐	2	✓ OK	● On	On	172.20.74.36	iLO	Disconnected
☐	5A	✓ OK	● On	On	172.20.74.72	iLOP	Disconnected
☐	5B	✓ OK	● On	On	172.20.74.69	iLO-Z-o--8--j	Disconnected

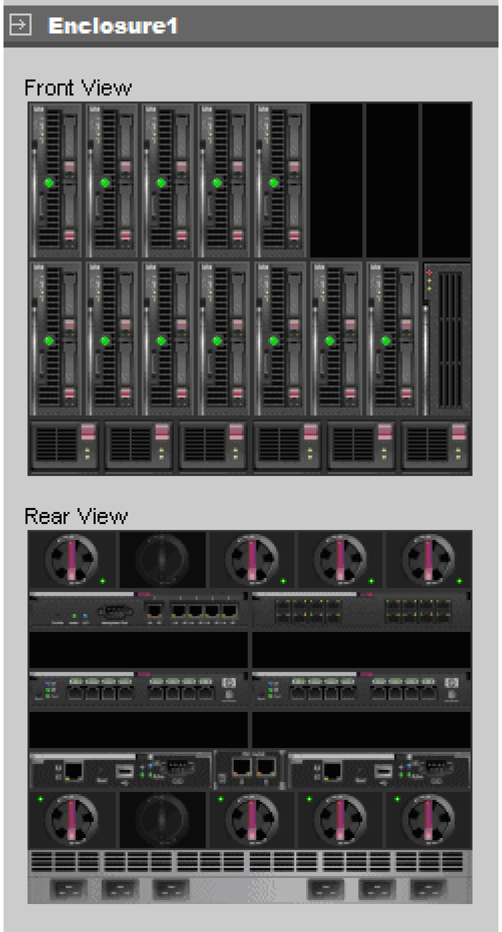
System forms pages

Some devices, particularly the Onboard Administrator, can have links to various system forms pages listed beneath their main links in the left tree navigation view. Form pages contain input text boxes, radio buttons, and other HTML input element and are used to administer settings related to the device to which they belong. For example, you can use the Onboard Administrator system forms page to change IP address settings or update firmware. These forms are all linked under the Onboard Administrator parent element. When you click a system forms link, the device to which the form page belongs is selected in the graphical view. For example, clicking the **Firmware Update** link for the Active Onboard Administrator selects the Active Onboard Administrator device in the graphical view. Links to system forms do not display status icons.

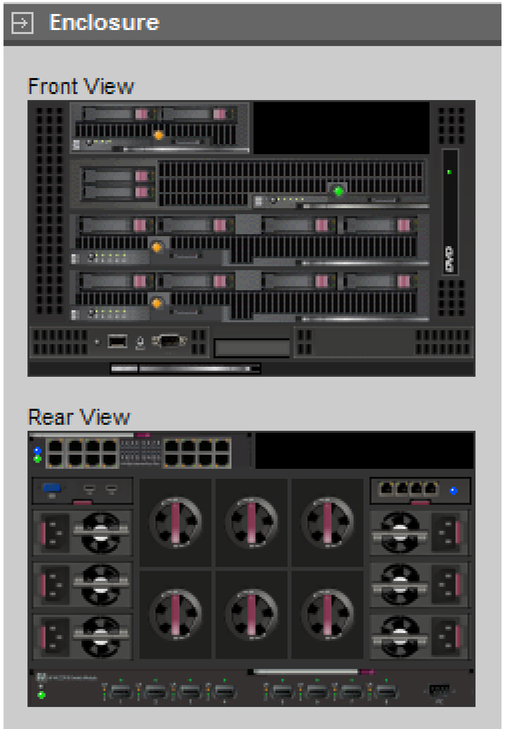
Graphical view navigation

The second component of the Onboard Administrator GUI navigation system is a graphical representation of the physical enclosure, called the graphical view. The graphical view consists of two subcomponents: a front view and a rear view.

The following image shows the graphical view of a typical c7000 Enclosure.



The following image shows the graphical view of a typical c3000 Enclosure.



All functions and features for the graphical view navigation are the same for both the c3000 and the c7000 Enclosures, except where noted.

Selecting a device

To select a device, click the graphical representation of the device in the front or rear graphical view. When you select a device, the surrounding border changes from gray to light blue to indicate it is the currently selected device. Selecting a device in the graphical view selects the corresponding device in the left navigation tree view. Every time you select a device from any part of the navigation system, the rest of the navigation reflects that device selection event and updates accordingly.

Status reporting

The graphical view reports the status of every device in the enclosure. The status of each device is indicated on the device by a small status icon. No status icon appears for a device that is working properly and has an OK status. However, any other status codes appear as status icons on the device.

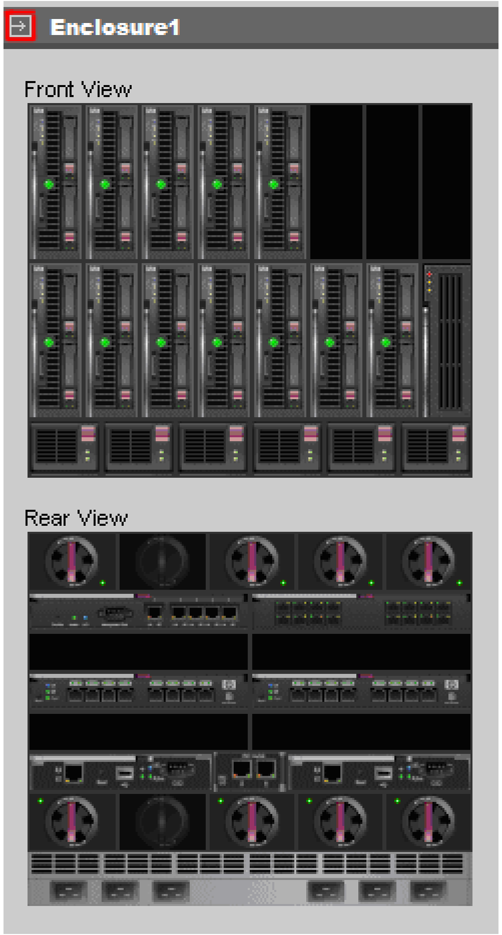
The graphical view does not report the presence or absence of hard drives in the server blade or storage blade.

Device security

Although the front and rear graphical views are both affected by user permissions, security on the graphical view is handled differently from the left tree view. If the user does not have permission to access a device, a blank bay appears regardless of whether a device is present in that bay, and a padlock icon in the bay table cell appears, indicating that the bay is locked to the current user.

Minimizing the graphical view

To minimize the graphical view from the main display, click the small box that contains an arrow located directly to the left of the name of the enclosure in the Graphical View box. This option minimizes the Graphical View and gives more room for the main section of the display. This is useful when viewing the Onboard Administrator on a small monitor or on a monitor using low resolution.

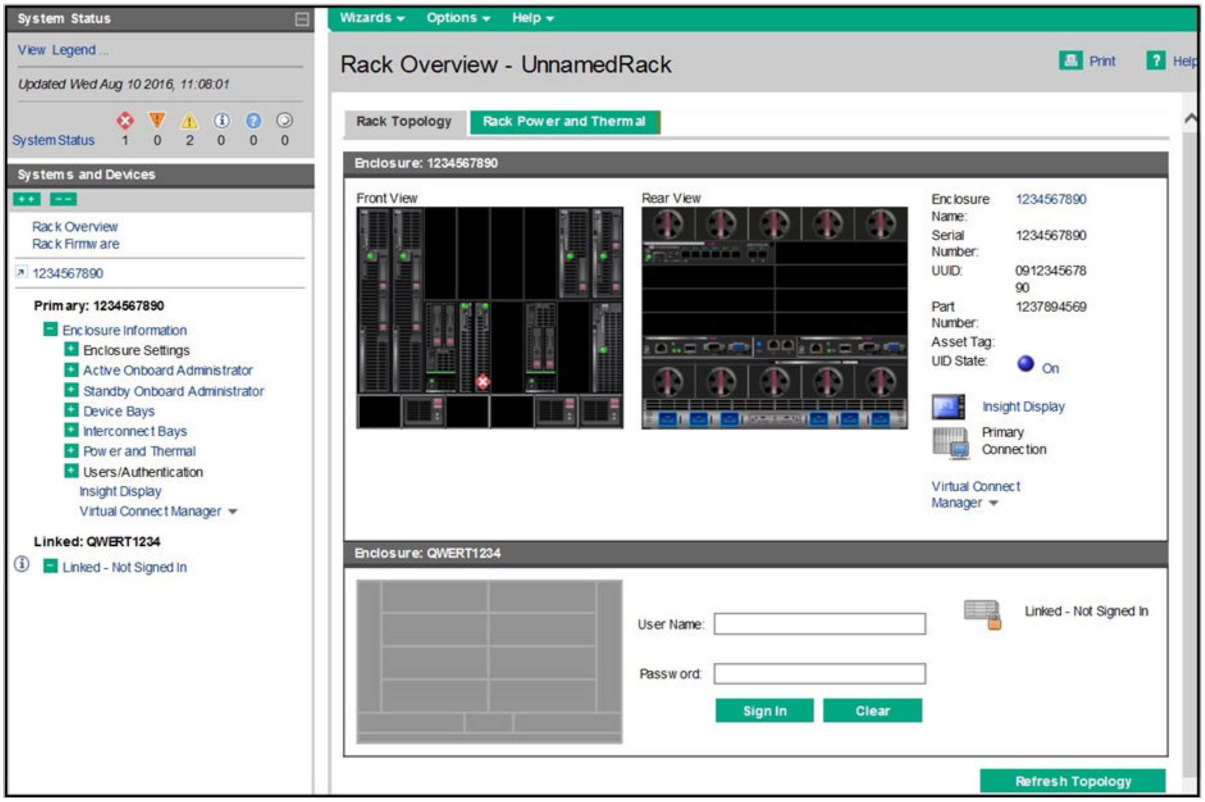

Enclosure1
Front View
Rear View

Rack View

Rack Overview screen

The Rack Topology tab shows a graphical representation of the physical enclosure, called the graphical view. The graphical view consists of a front view and a rear view. When you mouse over a device in the graphical view, a window appears with information on that device. The graphical view provides status on each device in the enclosure and gives you the option of selecting an individual device for more detailed information.

If you have multiple enclosures, some might appear in the Rack Overview as grayed out. To view contents and information for these enclosures, enter a user name and password in the text boxes, and then click **Sign In.** A graphical view of the enclosure appears. The following figure shows the Rack Overview with an enclosure that is grayed out.



Updated Wed Aug 10 2016, 11:08:01

Rack Overview - UnnamedRack

Enclosure: 1234567890

Enclosure Name: 1234567890
Serial Number: 1234567890
UUID: 091234567890
Part Number: 1237894569
Asset Tag:
UID State: ● On

Enclosure: QWERT1234

User Name:
Password:

Linked - Not Signed In

After signing in, the enclosure contents become available, as shown in the following screen example. To connect to a VCM, click the down arrow button next to "Virtual Connect Manager." A popup displays the web address links that you can use to connect to a VCM. If FQDN link support is enabled and certain DNS configuration requirements are met, an FQDN-based VCM web address is the default selection, as shown. For information about enabling FQDN link support, see **Network Access**.

Rack Information

Row	Description
Enclosure Name	The user-configured name of the enclosure in the rack.
Enclosure Rack U Position	The location on the enclosure in the rack.
Serial Number	The unique serial number for the enclosure.

Table Continued

Row	Description
UUID	The Universally Unique Identifier assigned to the enclosure.
Part Number	The part number of the enclosure used when obtaining a new or replacement enclosure.
Asset Tag	The asset tag is used for inventory control.
UID State	Displays On or Off, depending on whether the UID is active.

Rack Location Information

Row	Description
Rack Name	The name of the rack.
Rack Product Description	The common descriptive name of the rack.
Rack Part Number	The part number to be used when ordering a replacement rack.
Rack Identifier	A unique string that identifies the rack.
Rack U Height	The U height of the rack.

Location Discovery Services

Location Discovery Services is a component of HPE Discovery Services. Location Discovery Services automatically reports server locations to HPE SIM and Insight Control, eliminating this manual task for server administrators. Administrators can use the location information and system data with HPE Asset Manager to obtain more precise and complete asset data.

Location Discovery Services is a rack U location discovery solution for G3 and later racks. It enables HPE iLO, BL Onboard Administrator, and SL Chassis firmware to report and display the rack ID and the server U position in the rack. Supported racks are programmed with unique U values in 7U and/or 8U modules, and are installed with the tag version number, rack identifier, part number, product name, rack height, and U position. Location Discovery Services supports 14U, 22U, 36U, 42U, and 47U racks.

The rack device reads the rack U location tag each time iLO receives AC power or iLO is reset. The U position value denotes the U position read by the device. The contact position offset is a fixed value for each model that indicates the position of the contact relative to the bottom U position of the device. It is normally 0, but can be a positive value if the contact cannot be placed at the bottom U position of the device. The bottom-most U position occupied by the device is calculated by subtracting the U offset from the U position.

You can view the discovered data in certain Onboard Administrator screens, such as the Rack Information table in the Enclosure Information tab. In addition, several Onboard Administrator CLI commands display the discovered data, such as the `SHOW ENCLOSURE INFO` and `SHOW TOPOLOGY INFO` commands. For more information on these commands, see the Onboard Administrator Command Line Interface User Guide.

Topology modes

Onboard Administrator supports three topology modes which are determined by the selection made on the sign in screen prior to signing in. The three topology modes are:

- Local Mode—Used to manage a single enclosure when more than one enclosure can be selected. Onboard Administrator ignores all topology changes. This mode is useful when you do not want to change topology by adding linked enclosures.
- Linked Mode—Used to manage a single enclosure when no other enclosures are attached. You can use Linked Mode to allow the addition of new enclosures as they are added to the interlink. As long as no new enclosures are connected, Onboard Administrator appears to be in Local Mode. All topology changes that

occur while signed in are displayed by Onboard Administrator. This mode provides an unrestricted view of enclosures connected to the interlink.

- Fixed Mode—Used to manage more than one, but not all enclosures. Only the topology changes affecting the current topology are displayed by Onboard Administrator. This mode is useful when monitoring a subset of the total enclosures connected to the interlink.

If the active mode is set for a single enclosure and one or more enclosures are connected, if you want to ensure that the additional enclosures are not visible in the enclosure topology, you must sign out and back in without selecting a linked enclosure.

Rack Topology tab

The Rack Topology tab shows a graphical representation of the physical enclosure, called the graphical view. The graphical view consists of a front view and a rear view. When you mouse over a device in the graphical view, a window appears with information on that device. The graphical view provides status on each device in the enclosure and gives you the option of selecting an individual device for more detailed information.

Selecting a device

To select a device, click the graphical representation of the device in the front or rear graphical view. When you select a device, the surrounding border changes from gray to light blue to indicate it is the currently selected device. Selecting a device in the graphical view selects the corresponding device in the left navigation tree view. When you select a device from any part of the navigation system, the rest of the navigation reflects that device selection event and updates accordingly.

Status reporting

The graphical view reports the status of every device in the enclosure. The status of each device is indicated on the device by a small status icon. No status icon appears for a device that is working properly and has an OK status. However, any other status codes appear as status icons on the device.

The graphical view does not report the presence or absence of hard drives in the server blade or storage blade.

Device security

Although the front and rear graphical views are both affected by user permissions, security on the graphical view is handled differently from the left tree view. If the user does not have permission to access a device, a blank bay appears regardless of whether a device is present in that bay, and a padlock icon in the bay table cell appears, indicating that the bay is locked to the current user.

The user cannot select a locked bay. When the user's mouse hovers over the locked bay, a message appears, indicating that the user does not have permission to access the device in that bay.

Rack information

Row	Description
Enclosure Name	The user-configured name of the enclosure in the rack.
Enclosure Rack U Position	The location on the enclosure in the rack.
Serial Number	The unique serial number for the enclosure.
UUID	The Universally Unique Identifier assigned to the enclosure.
Part Number	The part number of the enclosure used when obtaining a new or replacement enclosure.
Asset Tag	The asset tag is used for inventory control.
UID State	Displays On or Off, depending on whether the UID is active.

To update the rack topology information, click **Refresh Topology.** When you select Refresh Topology, the Rack Topology screen switches to the Linked Mode, and all linked enclosures appear.

Some rack topology information is provided through Location Discovery Services. For more information about using Location Discovery Services, see **Rack Overview screen**.

Linked enclosures

The Rack Topology tab displays all linked enclosures, which have one of the following states:

- Linked—Not Signed In. Enter a user name and password in the text boxes, and click **Sign In.** A graphical view of the enclosure appears.
- Linked—Not Signed In with a card reader icon. This state indicates the linked enclosure is Two-Factor or CAC Authentication enabled but is not authenticated. This state occurs under three conditions:
  - The configuration is not supported. You must enable the primary enclosure for Two-Factor Authentication, and both the primary and linked enclosure must have the same credentials in order for the linked enclosure to authenticate using Two-Factor Authentication.
  - If the configuration is not supported. The primary enclosure must be enabled for CAC Authentication, and both the primary and linked enclosures must have same the credentials for the linked enclosure to authenticate using CAC Authentication. If the primary enclosure does not have CAC Authentication enabled , then you cannot select the linked enclosure with CAC Authentication enabled.
  - If you click the Sign Out link on a Two-Factor or CAC Authenticated enclosure that is already authenticated, this state displays. To re-authenticate this enclosure, you must refresh the GUI or re-authenticate the primary enclosure.
- Linked—Signed In with the Load Enclosure Information button. Click **Load Enclosure Information** to display the graphical view of the enclosure.
- Linked—Signed In with a graphical view of the enclosure displayed.

On the right side of the linked enclosure name bar, click **Sign Out** to sign out of a linked enclosure.

NOTE:

When OAs in FIPS mode are configured in a Linked enclosure configuration, for seamless access all the OAs will have to be in the same FIPS mode (FIPS ON/FIPS TOP SECRET).

When multiple enclosures with Onboard Administrator in FIPS mode are connected together in a linked enclosure configuration, for seamless access to Onboard Administrators in the link, all Onboard Administrators have to be running same firmware version.

Rack Power and Thermal tab

The Power and Thermal tab displays information about the temperature inside the enclosure as well as the thermal and power subsystem health status. A graphical view of the present power and power limit helps you determine power status.

Rack cooling requirements

Row	Description
Current Btu/hr	The sum of the amount of heat being generated by the linked enclosures measured in Btu per hour.
Max Btu/hr	The maximum amount of heat that can be generated by the linked enclosures under load measured in Btu per hour.

Enclosure thermal and power status

Row	Description
Enclosure Ambient Temperature	This field displays the highest ambient temperature being reported by the installed blade devices. If no blade devices are installed, then this field displays the temperature of the Onboard Administrator module as an approximation of the ambient temperature.
Thermal Subsystem Status	The overall thermal status of the enclosure. Possible values are Unknown, OK, Degraded, or Critical Error.
Power Subsystem Status	The overall power status of the enclosure. Possible values are Unknown, OK, Degraded, or Critical Error.
Power Mode	A user setting to configure the enclosure DC power capacity and the input power redundancy mode of the enclosure. See Power Management for possible values.
Present Power	The amount of watts being consumed by all devices in the enclosure.
Power Limit	The maximum amount of power available for consumption by the enclosure measured in watts.
Enclosure Dynamic Power Cap	A power cap on a group of servers in the enclosure. As the servers run, the demand for power varies for each server. A power cap for each server is set to provide the server with enough power to meet its workload demands while still conforming to the Enclosure Dynamic Power Cap. Continuous monitoring of power demands and automatic adjustments to server power caps ensure there is minimal performance degradation. Information for the Enclosure Dynamic Power Cap appears only if a cap has been defined.

IMPORTANT:

If redundancy mode is set to AC Redundant, or Power Supply Redundant, and power redundancy is lost, then you must either add additional power supplies or change the redundancy mode setting in the Onboard Administrator to restore Power Subsystem status. See the Insight Display for corrective steps.

Present Power/Enclosure Dynamic Power Cap/Power Limit

The Present Power is the number of watts being consumed by all the devices in the enclosure. The Enclosure Dynamic Power Cap automatically adjusts power caps on servers in the enclosure to meet workload demands on the servers while still conforming to the Enclosure Dynamic Power Cap. The Power Limit is the maximum amount of input power available for consumption by the enclosure. The Power Limit is dependent on the enclosure power redundancy setting and the number and location of the power supplies in the enclosure. If a Static Power Limit has been specified, the Power Limit displays that limit.

Linked enclosures

This section displays information for all linked enclosures you are signed in to.

NOTE:

When multiple enclosures with Onboard Administrator in FIPS mode are connected together in a linked enclosure configuration, for seamless access to Onboard Administrators in the link, all Onboard Administrators have to be running same firmware version.

When OAs in FIPS mode are configured in a Linked enclosure configuration, for seamless access all the OAs will have to be in the same FIPS mode (FIPS ON/FIPS TOP SECRET).

Rack Firmware screen

Rack Firmware Summary

NOTE:

To view complete firmware version information, a manual discovery must be performed first, using Enclosure Firmware Management.

Onboard Administrator Firmware information

Column	Description
Bay	The physical bay number where the Onboard Administrator is installed
Model	The model number of the Onboard Administrator
Manufacturer	The name of the company that manufactured the Onboard Administrator
Serial Number	The unique serial number of the Onboard Administrator
Part Number	The part number used when ordering an additional or replacement Onboard Administrator
Spare Part Number	The spare part number to be used when ordering an additional or replacement Onboard Administrator
Firmware Version	The version of the firmware image on the Onboard Administrator

Enclosure Component Firmware information

Column	Description
Bay	The physical bay number where the component is installed
Device Model	The model number of the device
Current Firmware Version	The version of the firmware installed on the component
Available Firmware Version	The latest version of firmware available for installation on the component

Device Firmware information

Column	Description
Bay	The physical bay number where the device is located in the enclosure.
Device Model	The model of the device. The date of the latest firmware discovery appears, or if no discovery has been performed on that device, then `No` appears.
Firmware Component	The name of each component is listed on separate lines. Components supported by the Firmware DVD are listed, including: • System ROM • iLO • Power Management Controller • NICs • HBAs • Smart Array and attached hard drives For components with multiple internal firmware versions such as NICs, each of those versions is listed separately.

Table Continued

Column	Description
Current Version	Current version of firmware for that component.
Firmware DVD Version	Firmware DVD version for that component.

Interconnect Firmware information

Column	Description
Bay	The physical bay number where the interconnect is located in the enclosure
Device Model	The model of the interconnect
Firmware Version	The firmware version of the interconnect module. `Not Available` appears when the interconnect module does not provide the firmware version information.

Export Firmware information

To export the firmware version information that appears on this screen to CSV or XML format, click **XML** or **CSV.**

NOTE:

The CSV option is only available with Internet Explorer.

If the blade firmware does not match the DVD ISO firmware after a server is discovered or updated, an informational icon is displayed.

A letter included after the firmware version indicates a smart component release note revision. This revision is not a functional firmware update.

Configuring HPE BladeSystem enclosures and enclosure devices

Viewing the status screens

Each enclosure can be selected from the left navigation tree. Clicking the enclosure name opens the main status page for the enclosure.

On this page, four tabs are available at the top of the main page: Status, Information, Virtual Buttons, and Component Firmware.

The Status tab displays one of the following values as the overall Enclosure Status:

- Critical/Failed
- Major
- Minor/Degraded
- Normal/OK
- Unknown
- Informational

The Active Onboard Administrator Status and Standby Onboard Administrator Status are similar to the Enclosure Status and display a status for the Onboard Administrator. If a standby Onboard Administrator is not present in the system, its status value is Absent.

Power Mode displays the current power mode of the enclosure. The following values are possible:

- AC Redundant
- Power Supply Redundant
- Not Redundant

The Enclosure Status Overview is divided into four sections:

- Device Bay Overview
- Interconnect Bay Overview
- Power Subsystem
- Thermal Subsystem

For each of these sections, the following values are possible:

- Critical/Failed
- Major
- Minor/Degraded
- Normal/OK
- Unknown
- Informational

Enclosure settings

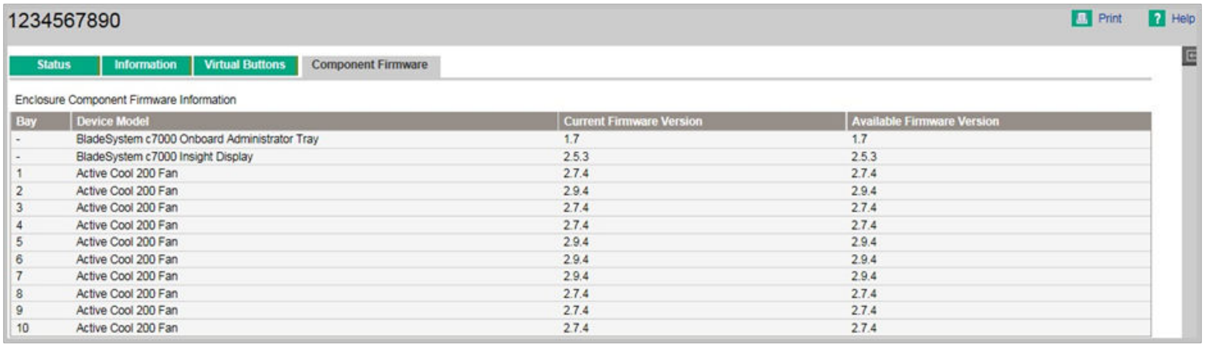
Selecting enclosures

The primary interlink ports are displayed in the rack topology table. The primary enclosure is selected by default, and cannot be deselected.

When linked enclosures are displayed, the topology mode that the application uses during your session is determined by the check box selections made before signing in, as described below:

- Local Mode—This is the default topology mode, and is enabled if none of the linked enclosures are selected. All topology changes that occur while signed in are ignored by the application.
- Fixed Mode—This topology mode is enabled when some of the linked enclosures are selected, but not all of them. Only topology changes that affect the selected enclosures while signed in are displayed by the application.
- Linked Mode—This topology mode is enabled if all displayed enclosures are selected. All topology changes that occur while signed in are displayed by the application.

Enclosure Information screen

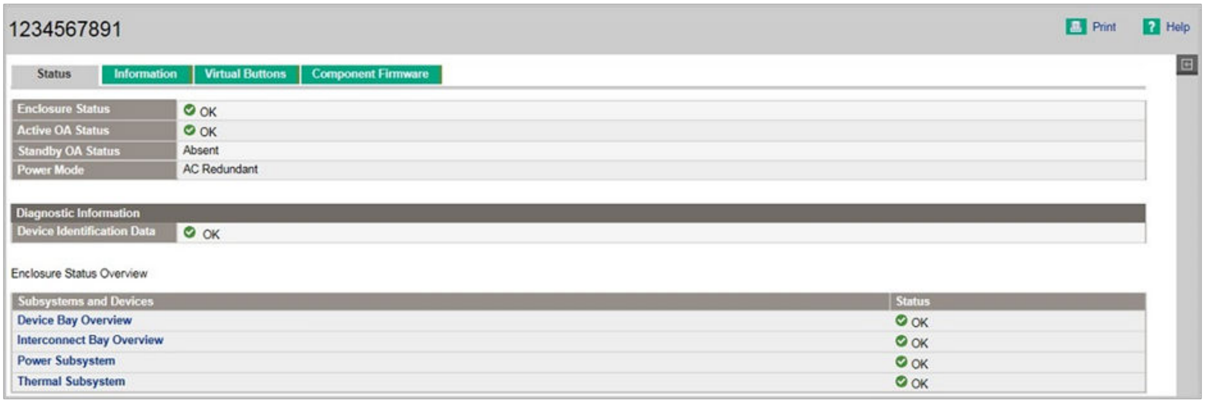


1234567890

Enclosure Component Firmware Information

Bay	Device Model	Current Firmware Version	Available Firmware Version
-	BladeSystem c7000 Onboard Administrator Tray	1.7	1.7
-	BladeSystem c7000 Insight Display	2.5.3	2.5.3
1	Active Cool 200 Fan	2.7.4	2.7.4
2	Active Cool 200 Fan	2.9.4	2.9.4
3	Active Cool 200 Fan	2.7.4	2.7.4
4	Active Cool 200 Fan	2.7.4	2.7.4
5	Active Cool 200 Fan	2.9.4	2.9.4
6	Active Cool 200 Fan	2.9.4	2.9.4
7	Active Cool 200 Fan	2.9.4	2.9.4
8	Active Cool 200 Fan	2.7.4	2.7.4
9	Active Cool 200 Fan	2.7.4	2.7.4
10	Active Cool 200 Fan	2.7.4	2.7.4

To view information about the enclosure, select **Enclosure Information** from the tree view. The Enclosure Information screen includes four tabs: **Status**, **Information**, **Virtual Buttons**, and **Component Firmware**.



1234567891

Enclosure Status	✓ OK
Active OA Status	✓ OK
Standby OA Status	Absent
Power Mode	AC Redundant

Diagnostic Information	
Device Identification Data	✓ OK

Enclosure Status Overview

Subsystems and Devices	Status
Device Bay Overview	✓ OK
Interconnect Bay Overview	✓ OK
Power Subsystem	✓ OK
Thermal Subsystem	✓ OK

Enclosure Status tab

Status information

Row	Description
Enclosure Status	The overall status of the enclosure. Possible values are Unknown, OK, Degraded, N/A, or Critical Error. [1]
Active OA Status	The overall status of the Active Onboard Administrator. Possible values are Unknown, OK, Degraded, or Failed.
Standby OA Status	The overall status of the Standby Onboard Administrator. Possible values are Absent, Unknown, OK, Degraded, or Failed.
Power Mode	A user setting to configure the enclosure DC power capacity and the input power redundancy mode of the enclosure. See Power Management for possible values.

[1] *The enclosure status appears as N/A if the Enable Extended Data on GUI Login Page setting is disabled. This setting is accessible at Enclosure Settings>Network Access>Anonymous Data.*

Enclosure Diagnostic Information

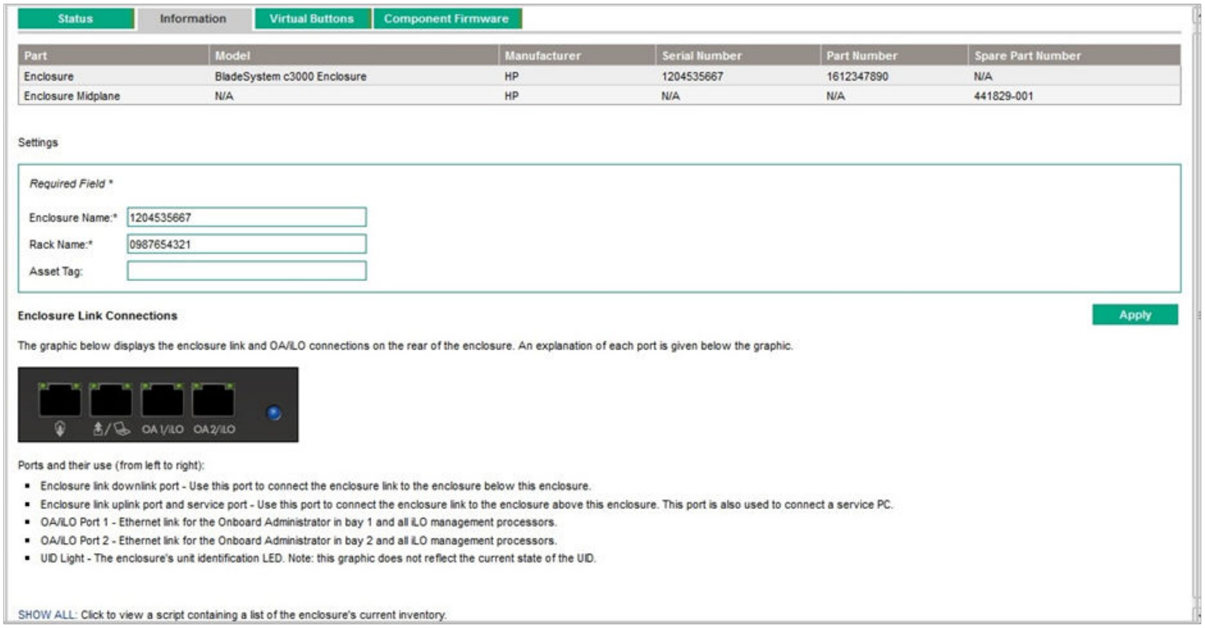
Diagnostic information is gathered by polling a device microcontroller (resulting in a degraded status if a failure has occurred) or is sent by the device microcontroller, without being polled to report a failure.

Row	Description
Device Identification Data	Information such as model name, part number, serial number, and other information used to identify the device is checked. This data is also referred to as FRU data. If the data is not present or not readable by the Onboard Administrator, a device identification data error displays. Possible values are OK or Error.
Redundancy	Possible values are OK or Error. An error indicates the redundant Onboard Administrators are having problems syncing up. Check the syslog for errors. Possible reasons for the error are mismatched firmware or a software or hardware failure.
Location Services	Possible values are OK or Other. Other indicates a location services error has occurred. Data might be corrupted.

Enclosure Status Overview

Subsystems and Devices	Description
Device Bay Overview	The overall status of all device bays. The status is an aggregate status of all the devices in the enclosure. If more than one device has a status other than OK, then they are displayed in a list in this table.
Interconnect Bay Overview	The overall status of the interconnect bays. The status is an aggregate status of all the interconnects in the enclosure. If more than one interconnect has a status other than OK, then they are displayed in a list in this table.
Power Subsystem	The overall status of the Power Subsystem of the enclosure. The status is an aggregate status of all the power supplies in the enclosure. If more than one power supply has a status other than OK, then they are displayed in a list in this table.
Thermal Subsystem	The overall status of the Thermal Subsystem of the enclosure. The status is an aggregate status of all the fans in the enclosure. If more than one fan has a status other than OK, then they are displayed in a list in this table.

Enclosure Information tab



Part	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
Enclosure	BladeSystem c3000 Enclosure	HP	1204535667	1612347890	N/A
Enclosure Midplane	N/A	HP	N/A	N/A	441829-001

Settings

*Required Field **

Enclosure Name:* 1204535667

Rack Name:* 0987654321

Asset Tag:

Enclosure Link Connections

The graphic below displays the enclosure link and OA/iLO connections on the rear of the enclosure. An explanation of each port is given below the graphic.

Ports and their use (from left to right):

- Enclosure link downlink port - Use this port to connect the enclosure link to the enclosure below this enclosure.
- Enclosure link uplink port and service port - Use this port to connect the enclosure link to the enclosure above this enclosure. This port is also used to connect a service PC.
- OA/iLO Port 1 - Ethernet link for the Onboard Administrator in bay 1 and all iLO management processors.
- OA/iLO Port 2 - Ethernet link for the Onboard Administrator in bay 2 and all iLO management processors.
- UID Light - The enclosure's unit identification LED. Note: this graphic does not reflect the current state of the UID.

SHOW ALL: Click to view a script containing a list of the enclosure's current inventory.

Hardware information

Column	Description
Part	The name of the part
Model	The model number of the part
Manufacturer	The name of the company that manufactured the part
Serial Number	The unique serial number of the part
Part Number	The part number to be used when ordering an additional part. The Power Input Module has no part number and always shows N/A in the Part Number column.
Spare Part Number	The part number to be used when ordering a replacement part

Rack information

Row	Description
Enclosure Rack U Position	The location of the enclosure in the rack.
Rack Product Description	The common descriptive name of the rack.
Rack Part Number	The part number to be used when ordering a replacement rack.
Rack Identifier	A unique string that identifies the rack.
Rack U Height	The U height of the rack.

This includes information gathered by Location Discovery Services. For more information on using Location Discovery Services, see **Rack Overview screen**.

Changing settings

Enclosure settings can be changed from this screen. To save the settings after making changes, click **Apply**.

Field	Possible value	Description
Enclosure Name	1 to 32 characters including all alphanumeric characters, the dash (-), and the underscore (_)	The name of the selected enclosure
Rack Name	1 to 32 characters including all alphanumeric characters, the dash (-), and the underscore (_)	The name of the rack in which the enclosure is installed
Asset Tag	0 to 32 characters including all alphanumeric characters, the dash (-), and the underscore (_)	The asset tag is used for inventory control. The default asset tag is blank

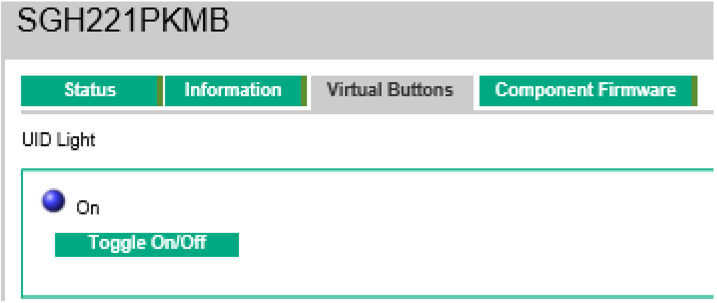
Enclosure Link Connections

This section provides a graphical view of the Enclosure Link Connections, located on the rear of the enclosure, and detailed information on each enclosure link port.

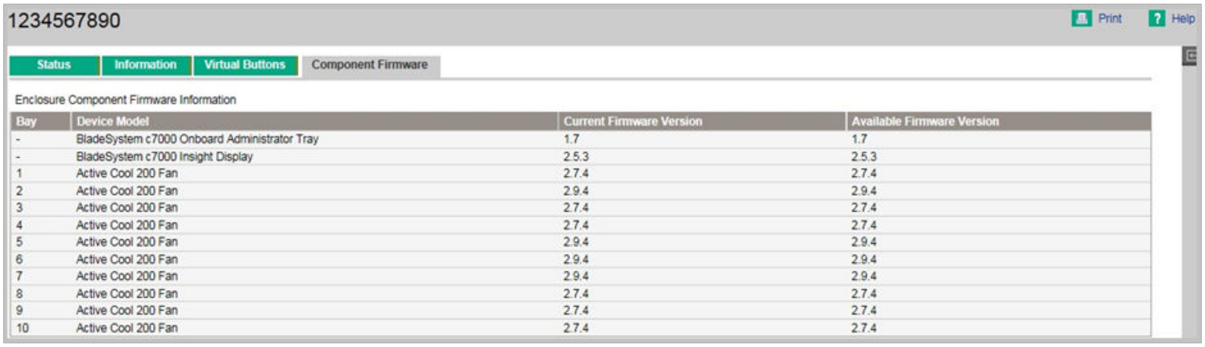
To view a script containing a list of the current inventory of the enclosure, click **SHOW ALL**.

Virtual Buttons

To change the state of the enclosure UID light, which is located next to the enclosure link and Onboard Administrator/iLO connections, click **Toggle On/Off**.



Component Firmware



Enclosure Component Firmware Information

Bay	Device Model	Current Firmware Version	Available Firmware Version
-	BladeSystem c7000 Onboard Administrator Tray	1.7	1.7
-	BladeSystem c7000 Insight Display	2.5.3	2.5.3
1	Active Cool 200 Fan	2.7.4	2.7.4
2	Active Cool 200 Fan	2.9.4	2.9.4
3	Active Cool 200 Fan	2.7.4	2.7.4
4	Active Cool 200 Fan	2.7.4	2.7.4
5	Active Cool 200 Fan	2.9.4	2.9.4
6	Active Cool 200 Fan	2.9.4	2.9.4
7	Active Cool 200 Fan	2.9.4	2.9.4
8	Active Cool 200 Fan	2.7.4	2.7.4
9	Active Cool 200 Fan	2.7.4	2.7.4
10	Active Cool 200 Fan	2.7.4	2.7.4

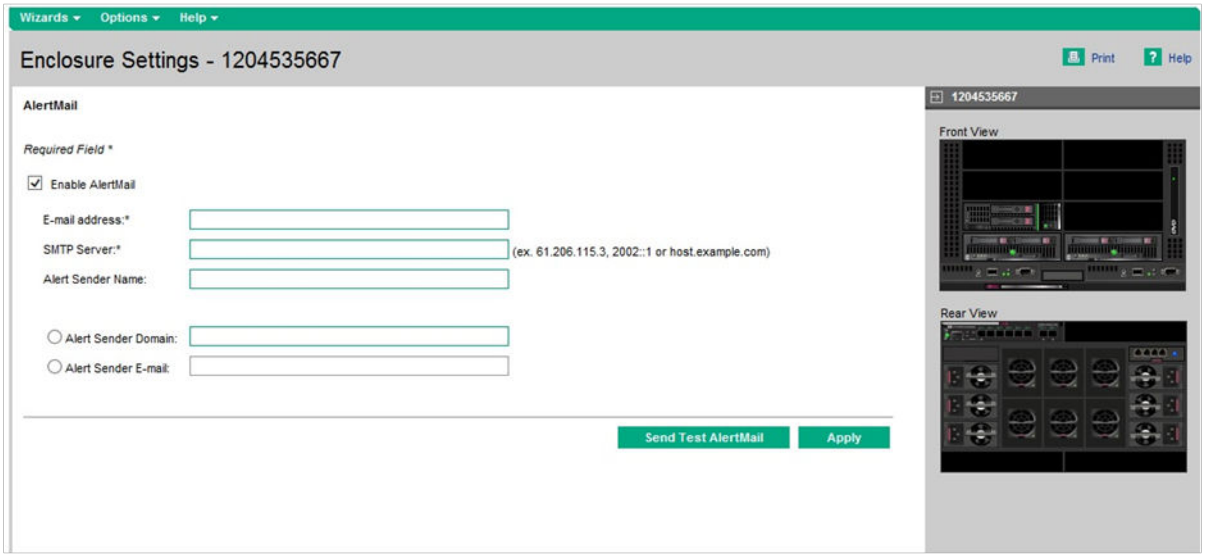
Column	Description
Bay	The device bay within the enclosure
Device Model	The model number of the device
Current Firmware Version	The installed firmware version of the device
Available Firmware Version	The latest version of firmware currently available for the device

The Enclosure Component Firmware tab also shows the firmware version of the location PIC (BladeSystem Location Device), as provided by Location Discovery Services. For more information on using Location Discovery Services, see **Rack Overview screen**.

AlertMail

AlertMail enables users to receive system events by e-mail instead of using SNMP traps. AlertMail is completely independent from SNMP, and both can be enabled at the same time. AlertMail uses standard SMTP commands to communicate with an SMTP-capable mail server. The “reply to” address for each e-mail sent by AlertMail will be <Enclosure Name>@<Alert Sender Domain>. To enable the AlertMail feature, select the **Enable AlertMail** check box.

To test the AlertMail function, ensure that the email address, alert sender domain, and SMTP server settings are correct. Select **Send Test AlertMail**. To confirm the test completed successfully, verify the recipient email account.



Enclosure Settings - 1204535667

AlertMail

*Required Field **

☑ Enable AlertMail

E-mail address:*

SMTP Server:* (ex. 61.206.115.3, 2002::1 or host.example.com)

Alert Sender Name:

○ Alert Sender Domain:

○ Alert Sender E-mail:

NOTE:

The Alert Sender Domain might not be needed. This field depends on the mail server setup.

Field	Possible value	Description
E-Mail address	<account>@<domain>	A valid email address for the administrator or other designated individual receiving the alert mail
SMTP Server	• IPv4 address—###.###.###.### where ### ranges from 0 to 255 • IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. • DNS name—1 to 64 characters including all alphanumeric characters and the dash (-)	An IPv4 address, IPv6 address, or the DNS name for the SMTP server

Table Continued

Field	Possible value	Description
Alert Sender Name	A character string including all alphanumeric characters, the dash (-), the underscore (_), and space. The field is optional with a limit of 40 characters.	Onboard Administrator name
Alert Sender Domain	A character string including all alphanumeric characters, the dash (-), and the period (.)	The domain in which the Onboard Administrator resides. Mutually exclusive with Sender Email.
Alert Sender E-mail	<account>@<domain>	Sender's valid email address for the administrator or other designated individual receiving the alert mail.

1. Select the **Enable AlertMail** checkbox to enable the AlertMail feature.
2. Enter values for the e-mail address, alert sender domain, and SMTP server.
3. Click **Apply** to save settings.

AlertMail, if enabled, sends alerts by e-mail for the following events:

- Enclosure status change
- Enclosure information change
- Fan status change
- Fan inserted
- Fan removed
- Power supply status
- Power supply inserted
- Power supply removed
- Power supply overload
- Blade inserted
- Blade removed
- Blade status
- Blade thermal condition
- Blade fault
- Blade information change
- Tray status change
- Tray reset
- Switch connect
- Switch disconnect

All e-mails have the following header:

From: Enclosure ENCLOSURE-NAME <enclosure-name@serverdomain>

Date: Date in standard format

Subject: HP AlertMail-SEQ: <SEVERITY> SUBJECT

To: RECEIVER MAILBOX

Where SEVERITY is one of the following (from highest to lowest):

- # FATAL
- # CRITICAL
- # WARNING MAJOR

- # WARNING MINOR
- # WARNING
- # NORMAL

Each subject line contains a unique sequence number to easily identify the order of events in case the mail server distributes them in the wrong order. Sequence numbers range from 0 to 999 and start again at 0.

The mail body is used to give more detailed information regarding the event issued. It also contains information on what the user should do to correct any issue and what the current enclosure status is.

> **NOTE:**
>
> The enclosure status is displayed as the status at the time the event was processed which can cause the status to show up as OK in an e-mail saying a Fan has Failed, if the user has already replaced the fan at the time the event was sent out by AlertMail.

Sample e-mail

Subject: HP AlertMail-010: (CRITICAL) Power Supply #1: Failed

Date: Wed, 23 Apr 2006 15:02:22 +0200

From: Enclosure EM-00508BEBA571 <EM-00508BEBA571@hp.com>

To: user@domain

X-OS: HP BladeSystem Enclosure Manager

X-Priority: 1

Content-Type: text/plain; charset=us-ascii

EVENT (26 May 07:09): Power Supply #1 Status has changed to: Failed.

Enclosure, EM-00508BEBA571, has detected that a power supply in bay 1 has changed from status OK to Failed.

The power supply should be replaced with the appropriate spare part. You can ensure that the center wall assembly is operating correctly by swapping the two power supplies. Make sure that there are no bent pins on the power supply connectors before reinserting and that each power supply is fully seated.

An amber LED on the power supply indicates either an over-voltage, over-temperature, or loss of AC power has occurred. A blinking LED on the power supply indicates a current limit condition.

Enclosure Status: Degraded

Enclosure Management URL: https://16.181.75.213/

- PLEASE DO NOT REPLY TO THIS EMAIL -

Device Power Sequence Device Bays tabs

The enclosure power delay feature controls the order in which components are powered on if the entire enclosure has been power cycled. This feature is only enabled during the active Onboard Administrator boot process if the Onboard Administrator detects that the entire enclosure has been power cycled and power delay has been enabled on at least one component in the enclosure.

The active Onboard Administrator displays a message in the system log when power delay has been initiated, and also displays a message in the system log when power delay has completed after the longest power delay has passed. The Onboard Administrator factory default setting is to disable power delay for all components.

Typical use cases involving bay to bay dependencies that can be resolved by enabling the enclosure power delay feature include:

- Boot from network - Network interconnects must complete power on self test prior to servers that are configured to boot from the network (for example, PXE or iSCSI).
- Boot from SAN - SAN interconnects must complete power on self test prior to servers that are configured to boot from SAN.
- Critical service dependencies controlled by a server such as DHCP or licensing.
- Storage servers must be operational prior to servers requiring those resources.

The delay time setting must be determined empirically since some dependencies are outside the enclosure (boot from SAN might require additional delay to enable the datacenter SAN storage system to power up). Each interconnect module has different power up timing before it is operational.

The timer used for power delay is started at the time the Onboard Administrator enters the first system log message during Onboard Administrator initialization indicated by the system log message `Kernel: Network link up`. When the Onboard Administrator indicates `PowerDelay has been initiated for the selected devices` in the system log, the configured delay times for each bay are used to determine when that component is turned on. After the selected delay time has elapsed, that component is turned on.

Valid settings for each bay are: Disabled, Enabled, and No Poweron.

- Disabled - Disables powerdelay for this bay. Onboard Administrator grants power to this bay based on its power settings: for a device configured to auto power-on, the device is granted power following an enclosure power cycle after all the Onboard Administrator configuration checks are complete.
- Enabled - Enables powerdelay for this bay. The Onboard Administrator turns on this bay based on the number of seconds elapsed following the detection of an enclosure power cycle event.
- No Poweron - Prevents component power on for the bays with this configuration until after the Onboard Administrator logs `PowerDelay has completed for the selected devices`. At this time, if the device is configured to auto power-on, the device grants power following an enclosure power cycle after all the Onboard Administrator configuration checks are complete.

If the device is configured to disable auto poweron, the device remains off following an enclosure power cycle independent of the setting of power delay for that bay.

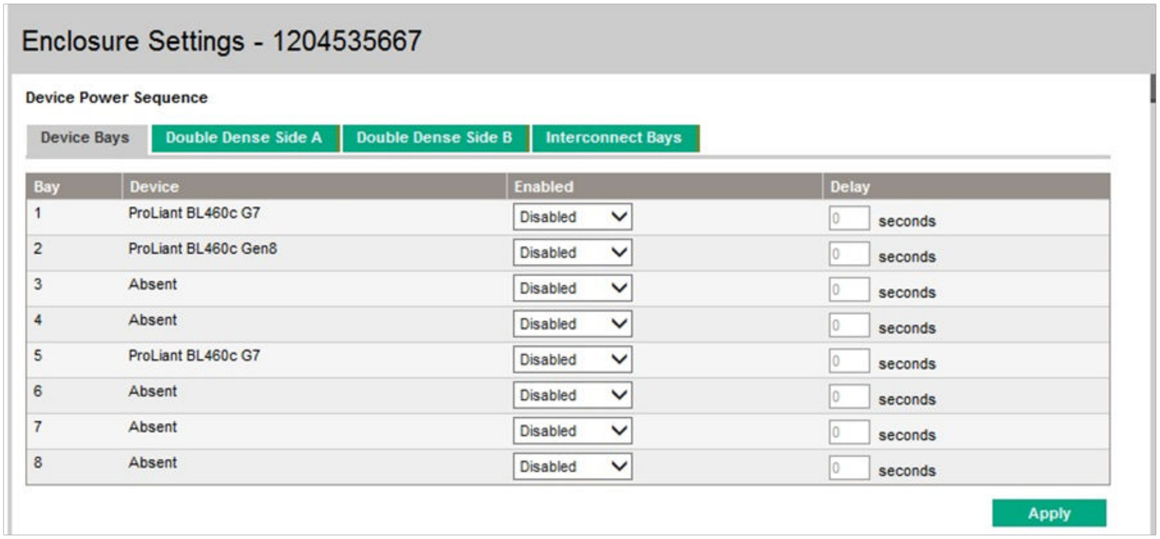
Device Bays Standard tab and Double Dense tabs

The Device Bays Standard tab indicates the current settings for all the primary bays based on the type of enclosure. To change a setting on a particular device bay, use the menu under the Enabled column and select Enabled, Disabled or No Poweron. If Enabled is selected, a power delay in seconds must be entered in the Delay column for this bay. The minimum value is 1 second; the maximum value is 3600 seconds.

If double dense servers are installed in an enclosure the power delay settings for Side A and Side B are controlled in the Double Dense Side A and Double Dense Side B tabs.

Interconnect Bays tab

Interconnect bays by default are for auto power-on. Enabling and setting a power delay for an interconnect bay delays the power on of that bay following an enclosure power cycle event.



Enclosure Settings - 1204535667

Device Power Sequence

Bay	Device	Enabled	Delay
1	ProLiant BL460c G7	Disabled	0 seconds
2	ProLiant BL460c Gen8	Disabled	0 seconds
3	Absent	Disabled	0 seconds
4	Absent	Disabled	0 seconds
5	ProLiant BL460c G7	Disabled	0 seconds
6	Absent	Disabled	0 seconds
7	Absent	Disabled	0 seconds
8	Absent	Disabled	0 seconds

Column	Description
Bay	Bay number of the device.
Device	The type of device in the bay, or Absent if no device is installed in the bay
Enabled	Enables power sequencing, disables power sequencing, or does not allow powering on of the device if No Poweron is selected.
Delay	The amount of delay, in seconds, before the device powers on.

Device Power Sequence Interconnect Bays tab

Column	Description
Bay	Bay number of the device
Device	The type of device in the bay or Absent if no device is installed in the bay
Enabled	Enables power sequencing, disables power sequencing, or does not allow powering on of the device if No Poweron is selected.
Delay	The amount of delay, in seconds, before the device powers on. Possible delay values are 1 to 3600.

Click **Apply** to save settings.

Date and Time

Static date and time settings

The date and time are static and not updated in real-time. The date and time can only be set if NTP is disabled.

Field	Possible value	Description
Date	yyyy-mm-dd • mm is an integer from 1 to 12 • dd is an integer from 1 to 31	The date assigned to the enclosure
Time	hh:mm:ss (24-hour time, ss is optional) • hh is an integer from 0 to 23 • mm is an integer from 0 to 59	The time assigned to the enclosure
Time Zone	Time zone settings • **Africa time zone settings** • **Americas time zone settings** • **Asia time zone settings** • **Universal time zone settings** • **Oceanic time zone settings** • **Europe time zone settings** • **Polar time zone settings**	The time zone assigned to the enclosure

NTP Settings

To enable this feature, select **Set time using an NTP server**.

Field	Possible value	Description
Primary NTP Server	• IPv4 address—###.###.###.### where ### ranges from 0 to 255 • IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. • DNS name—1 to 64 characters including all alphanumeric characters and the dash (-).	IP address or DNS name of primary NTP server that provides date and time information
Secondary NTP Server	• IPv4 address—###.###.###.### where ### ranges from 0 to 255 • IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. • DNS name—1 to 64 characters including all alphanumeric characters and the dash (-).	IP address or DNS name of secondary NTP server that provides date and time information

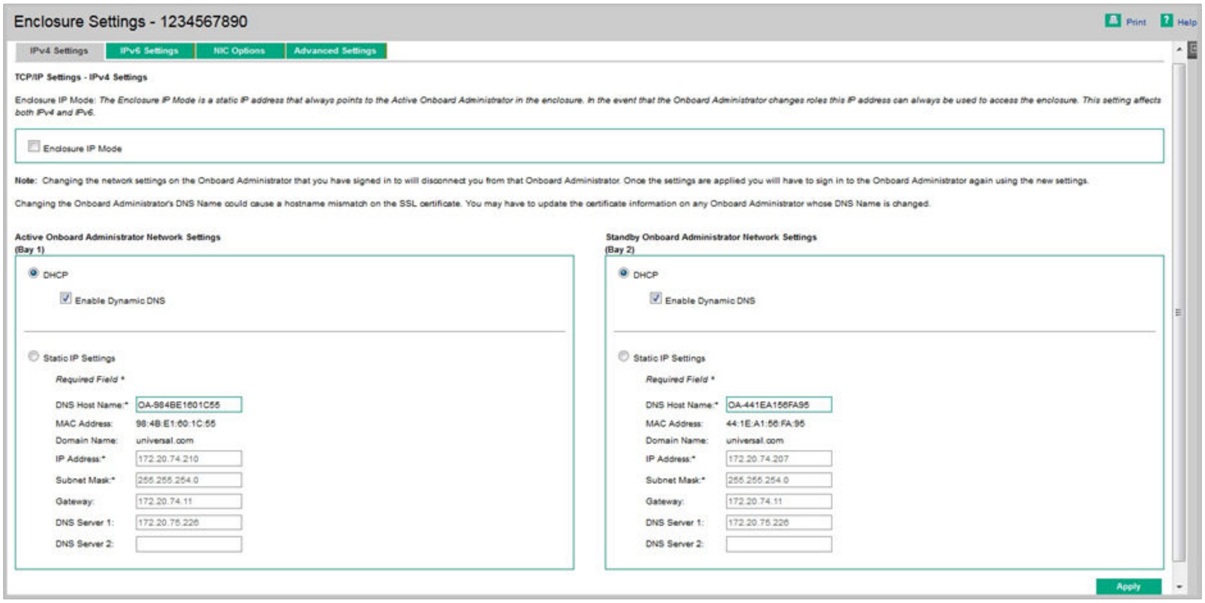
Table Continued

Field	Possible value	Description
Poll Interval	An integer from 60 to 86400	This is the interval at which the NTP server is polled in seconds
Time Zone	Time zone settings • **Africa time zone settings** • **Americas time zone settings** • **Asia time zone settings** • **Universal time zone settings** • **Oceanic time zone settings** • **Europe time zone settings** • **Polar time zone settings**	The time zone assigned to the enclosure

To save settings, click **Apply**.

Enclosure TCP/IP settings

IPv4 Settings tab



Enclosure Settings - 1234567890

TCP/IP Settings - IPv4 Settings

Enclosure IP Mode: *The Enclosure IP Mode is a static IP address that always points to the Active Onboard Administrator in the enclosure. In the event that the Onboard Administrator changes roles this IP address can always be used to access the enclosure. This setting affects both IPv4 and IPv6.*

□ Enclosure IP Mode

Note: Changing the network settings on the Onboard Administrator that you have signed in to will disconnect you from that Onboard Administrator. Once the settings are applied you will have to sign in to the Onboard Administrator again using the new settings.

Changing the Onboard Administrator's DNS Name could cause a hostname mismatch on the SSL certificate. You may have to update the certificate information on any Onboard Administrator whose DNS Name is changed.

Active Onboard Administrator Network Settings (Bay 1)

● DHCP

☑ Enable Dynamic DNS

○ Static IP Settings

*Required Field **

DNS Host Name:*	OA-984BE1601C55
MAC Address:	98:4B:E1:60:1C:55
Domain Name:	universal.com
IP Address:*	172.20.74.210
Subnet Mask:*	255.255.254.0
Gateway:	172.20.74.11
DNS Server 1:	172.20.75.226
DNS Server 2:	

Standby Onboard Administrator Network Settings (Bay 2)

● DHCP

☑ Enable Dynamic DNS

○ Static IP Settings

*Required Field **

DNS Host Name:*	OA-441EA156FA95
MAC Address:	44:1E:A1:56:FA:95
Domain Name:	universal.com
IP Address:*	172.20.74.207
Subnet Mask:*	255.255.254.0
Gateway:	172.20.74.11
DNS Server 1:	172.20.75.226
DNS Server 2:	

IPv4 Settings tab

Enclosure IP Mode

When enabled, the **Enclosure IP Mode** setting ensures all management applications point to the Active Onboard Administrator of the enclosure, using a single static IP address. This mode is for enclosures with an Active and Standby Onboard Administrator . When the Standby Onboard Administrator takes over the role of the Active Onboard Administrator, that Onboard Administrator assumes the IP address of the previous Active Onboard Administrator. This mode ensures the Enclosure IP Mode IP address is consistently pointing to the Active Onboard Administrator.

Enclosure IP Mode requires the Active Onboard Administrator to have a static IPv4 address or a static IPv6 address (IPv6 must be enabled). The Standby Onboard Administrator can be configured for DHCP or static IP settings. This mode is optional and is disabled by default.

To ensure that the Enclosure IP Mode setting is not changed when removing an Onboard Administrator module from the enclosure, do not remove the module while it is in the failover transition phase (about six minutes after a failover). After you remove a module, to ensure that all settings are transferred to the Standby module, add a replacement module and leave it in place for five minutes. If both the Active and Standby Onboard Administrator modules are powered off or removed from the enclosure at the same time, the Standby Onboard Administrator returns to the default network settings and all manually configured static network addresses are lost.

NOTE:

This feature is disabled while in the FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug.

Enabling **Enclosure IP Mode** on either the IPv4 Settings tab or the IPv6 Settings tab automatically enables this mode on both tabs.

Active and Standby Onboard Administrator Network Settings

The Onboard Administrator allows the IPv4 network configuration to be based either on dynamically assigned IP addresses obtained from a DHCP server or on static IP addresses that you specify manually. You choose the basis for network configuration by selecting either the **DHCP** radio button or the **Static IP Settings** radio button. If you select **DHCP** , you can enable Dynamic DNS.

NOTE:

Changing network settings on the Onboard Administrator that you are signed in to might disconnect you from that Onboard Administrator, in which case after you apply settings, you must sign in to the Onboard Administrator again.

- **DHCP**—Obtains the IP address for the Onboard Administrator from a DHCP server.
- **Enable Dynamic DNS** —With DHCP enabled, Dynamic DNS allows you to use the same host name for the Onboard Administrator over time, although the dynamically assigned IP address might change. The host name is registered with a DNS server. Dynamic DNS updates the DNS server with new or changed records for IP addresses.

  Disabling Dynamic DNS on the Onboard Administrator stops the Onboard Administrator's updates to the DNS server. However, note that some DHCP servers may have a provision to update DNS servers directly. To completely disable Dynamic DNS updates, disable Dynamic DNS both at the Onboard Administrator as well as at the DHCP server.
- **Static IP Settings** —Enables you to set up static IP settings for the Onboard Administrator manually.

  CAUTION:

  When enabling DHCP for IPv4, any static IPv4 settings are lost.

Field	Possible value	Description
DNS Host Name	Can be 1 to 32 characters including all alphanumeric characters and the dash (-).	The DNS Name of the Onboard Administrator. This setting applies to both IPv4 and IPv6 environments. The DNS host name can be assigned when using either DHCP or static IP settings. Changing the Onboard Administrator DNS Name could cause a host name mismatch on the SSL certificate. You may have to update the certificate information on the affected Onboard Administrator, using the **Active Onboard Administrator Certificate Administration screen** or the **Standby Onboard Administrator Certificate Administration screen** , as appropriate.
MAC Address	This is an informational field and cannot be changed.	The Onboard Administrator MAC address.
Domain Name	This is an informational field and cannot be changed.	Displays the current domain name by each particular Onboard Administrator.
IP Address	###.###.###.### where ### ranges from 0 to 255	Static IP address for the Onboard Administrator (required if static IP settings is selected).
Subnet Mask	###.###.###.### where ### ranges from 0 to 255	Subnet mask for the Onboard Administrator (required if static IP settings is selected).
Gateway	###.###.###.### where ### ranges from 0 to 255	Gateway address for the Onboard Administrator (required if static IP settings is selected).
IPv4 DNS 1	###.###.###.### where ### ranges from 0 to 255	The IPv4 address for the first IPv4 DNS server. [1]
IPv4 DNS 2	###.###.###.### where ### ranges from 0 to 255	The IPv4 address for the second IPv4 DNS server. [1]

[1] *The order in which the Onboard Administrator uses DNS servers is described after this table.*

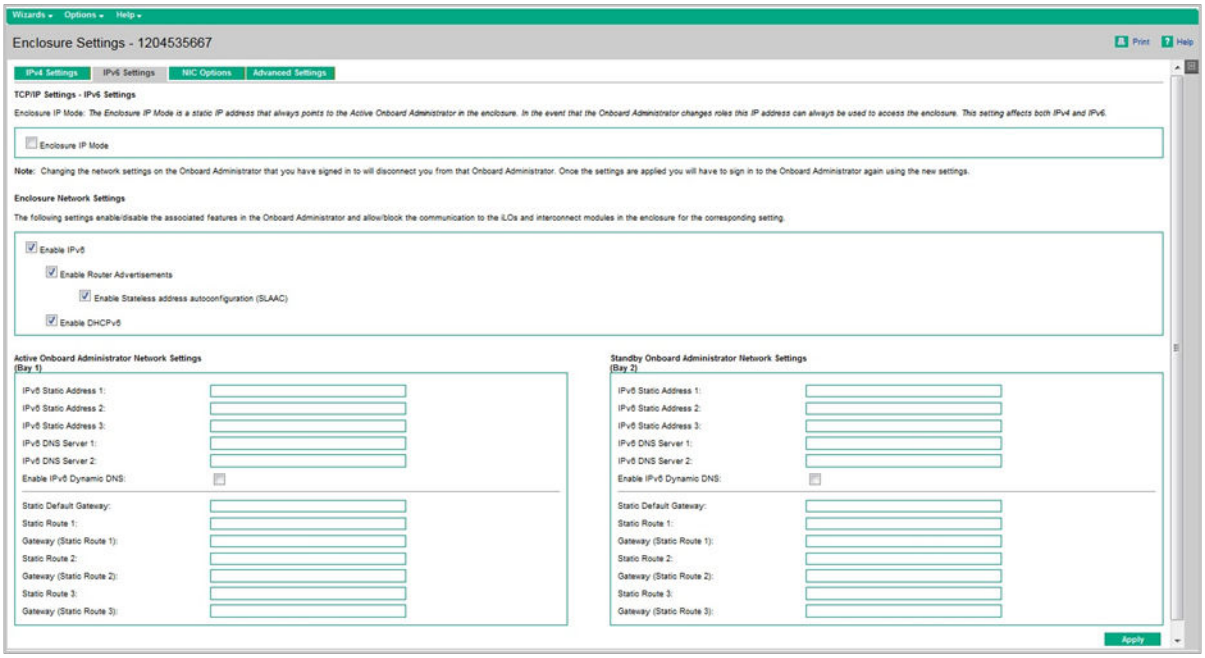
Depending on how many DNS servers are configured, the Onboard Administrator can use up to six DNS servers to look up an IP address: two IPv4 DNS servers (either static or DHCP assigned, but not both) and four IPv6 DNS servers (static or DHCP assigned, or both). The Onboard Administrator uses DNS servers in the following order:

1. IPv4 DNS server 1 (static)
2. IPv6 DNS server 1 (static)
3. IPv4 DNS server 2 (static)
4. IPv6 DNS server 2 (static)
5. IPv4 DNS server 1 (DHCP assigned)
6. IPv6 DNS server 1 (DHCP assigned)
7. IPv4 DNS server 2 (DHCP assigned)
8. IPv6 DNS server 2 (DHCP assigned)

If any of the DNS servers in this list are not configured, the DNS servers that follow them in the list move up in order, accordingly. For example, if the DHCP-assigned IPv4 DNS servers 1 and 2 are not configured, the two DHCP-assigned IPv6 DNS servers move up to 5th and 6th in the list. As noted previously, IPv4 DNS servers can either be static or DHCP assigned, not both; so the maximum number of DNS servers that the Onboard Administrator can use is 6.

To save new IPv4 settings, click **Apply**.

IPv6 Settings tab



Enclosure Settings - 1204535667

TCP/IP Settings - IPv6 Settings

Enclosure IP Mode: *The Enclosure IP Mode is a static IP address that always points to the Active Onboard Administrator in the enclosure. In the event that the Onboard Administrator changes roles this IP address can always be used to access the enclosure. This setting affects both IPv4 and IPv6.*

□ Enclosure IP Mode

Note: Changing the network settings on the Onboard Administrator that you have signed in to will disconnect you from that Onboard Administrator. Once the settings are applied you will have to sign in to the Onboard Administrator again using the new settings.

Enclosure Network Settings

The following settings enable/disable the associated features in the Onboard Administrator and allow/block the communication to the iLOs and interconnect modules in the enclosure for the corresponding setting.

☑ Enable IPv6

☑ Enable Router Advertisements

☑ Enable Stateless address autoconfiguration (SLAAC)

☑ Enable DHCPv6

Active Onboard Administrator Network Settings (Bay 1)

IPv6 Static Address 1:
IPv6 Static Address 2:
IPv6 Static Address 3:
IPv6 DNS Server 1:
IPv6 DNS Server 2:
Enable IPv6 Dynamic DNS: □
Static Default Gateway:
Static Route 1:
Gateway (Static Route 1):
Static Route 2:
Gateway (Static Route 2):
Static Route 3:
Gateway (Static Route 3):

Standby Onboard Administrator Network Settings (Bay 2)

IPv6 Static Address 1:
IPv6 Static Address 2:
IPv6 Static Address 3:
IPv6 DNS Server 1:
IPv6 DNS Server 2:
Enable IPv6 Dynamic DNS: □
Static Default Gateway:
Static Route 1:
Gateway (Static Route 1):
Static Route 2:
Gateway (Static Route 2):
Static Route 3:
Gateway (Static Route 3):

Enclosure IP Mode

When enabled, the **Enclosure IP Mode** setting ensures all management applications point to the Active Onboard Administrator of the enclosure, using a single static IP address. This mode is for enclosures with an Active and Standby Onboard Administrator. When the Standby Onboard Administrator takes over the role of the Active Onboard Administrator, that Onboard Administrator is assigned the IP address of the previous Active Onboard Administrator. This ensures the **Enclosure IP Mode** IP address is consistently pointing to the Active Onboard Administrator.

The **Enclosure IP Mode** requires the Active Onboard Administrator to have a static IPv4 address or a static IPv6 address (IPv6 must be enabled). The Standby Onboard Administrator can be configured for DHCP or static IP settings. This mode is optional and is disabled by default.

To ensure that the **Enclosure IP Mode** setting is not changed when removing an Onboard Administrator module from the enclosure, do not remove the module while it is in the failover transition phase (about six minutes after a failover). After you remove a module, to ensure that all settings are transferred to the Standby module, add a replacement module and leave it in place for five minutes. If both the Active and Standby Onboard Administrator modules are powered off or removed from the enclosure at the same time, the Standby Onboard Administrator returns to the default network settings and all manually configured static network addresses are lost.

NOTE:

This feature is disabled while in the FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug.

Enabling **Enclosure IP Mode** on either the IPv4 Settings tab or the IPv6 Settings tab automatically enables this mode on both tabs.

Enclosure Network Settings

IPv6 supports multiple addresses. You can enable any combination of the network settings. With IPv6, SLAAC and/or DHCPv6 enabled, the Onboard Administrator can obtain IP addresses from all the selected sources. It can have both automatically assigned IP addresses and user-specified static IP addresses. The

Enable SLAAC, **Enable DHCPv6**, and **Enable Router Advertisements** settings take effect only if IPv6 is enabled.

- **Enable IPv6**—Enables IPv6 protocol for all Onboard Administrator, interconnect, and server iLO modules in the enclosure. When enabled, one link-local address is auto configured.

  NOTE:

  After disabling IPv6 to convert to an IPv4-only environment, if the Firmware ISO URL on the Enclosure Firmware Management Settings tab specifies a USB key or an IPv6-based URL for a web server, you must reenter the location of the USB key or provide an IPv4-based URL for the web server. If this is not done, EFM cannot access the ISO image.

- **Enable Router Advertisements**—Allows IPv6 router advertisements from the external management network onto the internal enclosure management network. If you disable this setting, the Onboard Administrator blocks IPv6 router advertisements sent from the external management network, preventing them from entering the internal enclosure management network.
- **Enable SLAAC**—Enables IPv6 Stateless address autoconfiguration messages to all Onboard Administrator, interconnect, and server iLO modules in the enclosure. This feature affects only global IPv6 addresses. When IPv6 and SLAAC are both enabled, the Onboard Administrator can obtain up to 11 SLAAC IP addresses.
- **Enable DHCPv6**—Enables the active (and standby, if configured) Onboard Administrator to request a DHCPv6 IP address. Allows DHCPv6 traffic on the enclosure management network.

  △ **CAUTION:**

  If you disable IPv6 in an IPv6-only environment, you will lose your connection to the Onboard Administrator GUI and any SSH sessions. To reestablish your connection, you must perform the initial enclosure configuration via IPv4 networking, the Insight Display, or the Onboard Administrator serial console interface. When disabling IPv6, SLAAC, or DHCPv6, all connections that depend on the disabled protocol are closed. For example, if you are connected to the Onboard Administrator using its DHCPv6-assigned address, disabling the enclosure DHCPv6 setting results in your session being closed.

  NOTE:

  For SLAAC addresses to be successfully configured, the **Enable SLAAC** and **Enable Router Advertisements** settings must be enabled on the enclosure. In addition, an IPv6 router must be configured on the enclosure management network to provide the SLAAC addresses via router advertisements. Any iLOs may need to be configured separately to obtain SLAAC addresses. The **Enable SLAAC**, **Enable Router Advertisements**, and **Enable IPv6** settings must be enabled to allow the necessary traffic on the enclosure management network.

  For DHCPv6 addresses to be successfully configured, the **Enable IPv6** enclosure setting must be enabled and a DHCPv6 server configured on the management network. Any iLOs and interconnects must be configured separately to request a DHCPv6 address. If they are configured to request DHCPv6 addresses, the **Enable IPv6** and **Enable DHCPv6** settings must be enabled to allow the necessary traffic on the enclosure management network.

  After a factory reset, the enclosure IPv6 network settings for IPv6, SLAAC, DHCPv6, and Router Advertisements are enabled by default.

  When the Enable DHCPv6, Enable Router Advertisements, or Enable SLAAC enclosure IPv6 settings are disabled on the Onboard Administrator, the respective DHCPv6 or SLAAC addresses of the iLOs in the enclosure are retained until these addresses expire automatically based on their respective configurations. A manual reset of the iLO releases these addresses immediately.

Active and Standby Onboard Administrator Network Settings

NOTE:

Changing network settings on the Onboard Administrator that you are signed in to might disconnect you from that Onboard Administrator, in which case after you apply settings, you must sign in to the Onboard Administrator again.

Field	Possible value	Description
IPv6 Static Address 1	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128. [1] [2]	Onboard Administrator external NIC IPv6 address 1.
IPv6 Static Address 2	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1,2]	Onboard Administrator external NIC IPv6 address 2.
IPv6 Static Address 3	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1,2]	Onboard Administrator external NIC IPv6 address 3.
IPv6 DNS Server 1	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128. The prefix is optional.[1]	The IPv6 address for the first Static IPv6 DNS server. [3]
IPv6 DNS Server 2	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128. The prefix is optional.[1]	The IPv6 address for the second Static IPv6 DNS server.[3]
Enable IPv6 Dynamic DNS	Enabled (check box selected) or disabled (check box cleared).	Enables you to use a host name for the Onboard Administrator that persists even when the dynamically assigned IP address might change. The host name is registered with a DNS server. Dynamic DNS updates the DNS server with new or changed records for IP addresses. [4] Disabling Dynamic DNS on the Onboard Administrator stops the Onboard Administrator's updates to the DNS server. However, note that some DHCP servers may have a provision to update DNS servers directly. To completely disable Dynamic DNS updates, disable Dynamic DNS both at the Onboard Administrator as well as at the DHCP server.

Table Continued

Field	Possible value	Description
Static Default Gateway	####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. Do not specify a prefix. The gateway must be reachable from within the Onboard Administrator network.[1]	The static IPv6 address for the default gateway. This setting is required in an IPv6 network environment configured to be fully static. The Onboard Administrator can accept IPv6 gateway configuration directly via this setting and, if router advertisements are configured, via router advertisements from IPv6 routers on the management network. If router advertisements provide IPv6 gateway configuration, the gateway configuration provided by router advertisements overrides the static IPv6 gateway setting. The IPv6 gateway currently in use by the Onboard Administrator is displayed in the Current Default Gateway field on the **Active Onboard Administrator TCP/IP Settings** screen and the Standby Onboard Administrator TCP/IP Settings screen.
Static Route 1	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1]	Adds an IPv6 static route to the Onboard Administrator's routing table (manual configuration). [5] The static route defines an explicit path that the Onboard Administrator uses to reach an external network through a gateway. In a static network configuration, the static route removes the need to configure the router to send route information via router advertisements. If router advertisements are active in the network, and the default gateway is already configured, the router informs all nodes about the available static routes, thereby making manual configuration of the static routes unnecessary. If you specify the Static Route 1, you must also specify the associated Gateway (Static Route 1).
Gateway (Static Route 1)	####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. Do not specify a prefix. The gateway must be reachable from both the Onboard Administrator network and the external network.[1]	The IPv6 address of the gateway using the path defined by Static Route 1. You must also specify Static Route 1.
Static Route 2	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1]	Adds a second IPv6 static route to the Onboard Administrator's routing table (manual configuration). If you specify the Static Route 2, you must also specify the associated Gateway (Static Route 2).

Table Continued

Field	Possible value	Description
Gateway (Static Route 2)	####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. Do not specify a prefix. The gateway must be reachable from both the Onboard Administrator network and the external network.[1]	The IPv6 address of the gateway using the path defined by Static Route 2. You must also specify Static Route 2.
Static Route 3	####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF and the prefix /### ranges from 1 to 128.[1]	Adds a third IPv6 static route to the Onboard Administrator's routing table (manual configuration). If you specify the Static Route 3, you must also specify the associated Gateway (Static Route 3).
Gateway (Static Route 3)	####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. Do not specify a prefix. The gateway must be reachable from both the Onboard Administrator network and the external network.[1]	The IPv6 address of the gateway, using the path defined by Static Route 3. You must also specify Static Route 3.

[1] A compressed version of the same IPv6 address is also supported.

[2] The Onboard Administrator does not accept a link local address as an IPv6 Static address.

[3] The order in which the Onboard Administrator uses DNS servers is described after this table.

[4] IPv6 Dynamic DNS requires that a valid DNS server (either IPv4 or IPv6) be configured on the Onboard Administrator .

CAUTION:
Adding or removing a static route can result in loss of connectivity for clients accessing the Onboard Administrator.

5

Depending on how many DNS servers are configured, the Onboard Administrator can use up to six DNS servers to look up an IP address: two IPv4 DNS servers (either static or DHCP assigned, but not both) and four IPv6 DNS servers (static or DHCP assigned, or both). The Onboard Administrator uses DNS servers in the following order:

1. IPv4 DNS server 1 (static)
2. IPv6 DNS server 1 (static)
3. IPv4 DNS server 2 (static)
4. IPv6 DNS server 2 (static)
5. IPv4 DNS server 1 (DHCP assigned)
6. IPv6 DNS server 1 (DHCP assigned)
7. IPv4 DNS server 2 (DHCP assigned)
8. IPv6 DNS server 2 (DHCP assigned)

If any of the DNS servers in this list are not configured, the DNS servers that follow them in the list move up in order, accordingly. For example, if the DHCP-assigned IPv4 DNS servers 1 and 2 are not configured, the two DHCP-assigned IPv6 DNS servers move up to 5th and 6th in the list. As noted previously, IPv4 DNS servers can either be static or DHCP assigned, not both; so the maximum number of DNS servers that the Onboard Administrator can use is 6.

To save new IPv6 settings, click **Apply**.

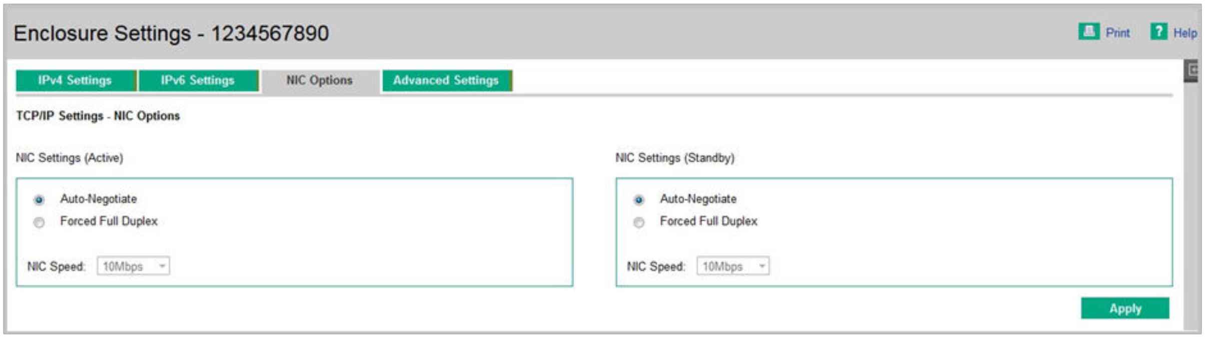
CAUTION:

Certain browsers such as Mozilla Firefox and Google Chrome might include a check box to popup dialogs that, if selected, will prevent future dialogs on the page. Do not select the check box on any of these dialogs. If you do, dialogs will remain hidden until the application is closed and reloaded in a new tab window.

NOTE:

When you change settings and click **Apply**, a popup message warns that changing your network settings could disconnect you from the Onboard Administrator. When you click **OK**, if the changes will disable certain protocols, another popup message warns that all connections using those protocols will be closed and you might lose your session. You are asked to confirm whether you want to perform this action (click **OK** or **Cancel**).

NIC Options tab



Enclosure Settings - 1234567890

TCP/IP Settings - NIC Options

NIC Settings (Active)

● Auto-Negotiate
○ Forced Full Duplex

NIC Speed: 10Mbps

NIC Settings (Standby)

● Auto-Negotiate
○ Forced Full Duplex

NIC Speed: 10Mbps

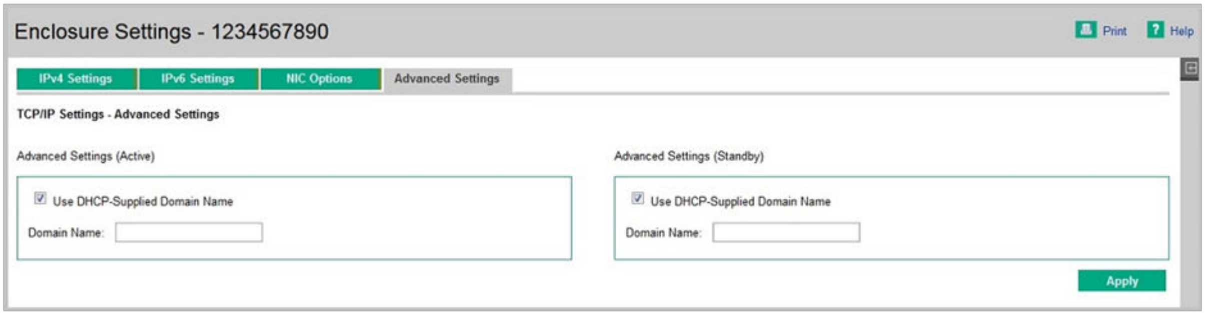
TCP/IP settings - NIC options

NIC settings

- **Auto-Negotiate**—Automatically configures the best link. This is the default setting. This option supports a NIC speed of 10Mb/s, 100Mb/s, or 1000Mbps. The 1000Mb/s setting is only available when Auto-Negotiate is selected.
- **Forced Full Duplex**—Enables you to manually specify which settings the external NIC uses when trying to establish a link. Onboard Administrator does not verify that the forced Ethernet settings are valid on the network. The loss of communications might occur if the wrong or incompatible settings are used. Forced settings take effect 3 seconds after enabling or disabling the settings. The forced option only supports NIC speeds of 10Mbps or 100Mb/s.
- **NIC Speed**—Selects a NIC speed of 10Mb/s or 100Mb/s

To save the new settings, click **Apply**.

Advanced Settings tab



Enclosure Settings - 1234567890

TCP/IP Settings - Advanced Settings

Advanced Settings (Active)

☑ Use DHCP-Supplied Domain Name

Domain Name:

Advanced Settings (Standby)

☑ Use DHCP-Supplied Domain Name

Domain Name:

This screen displays the current enclosure TCP/IP settings (Advanced settings) for the Active Onboard Administrator. The Advanced Settings tab allows you to enable or disable the **DHCP-Supplied Domain Name** option and to input User-Supplied Domain Names for both Active and Standby if the **DHCP-Supplied Domain Name** option is disabled. To enable or disable the **DHCP-Supplied Domain Name** option, or to set User-Supplied Domain Names, Dynamic DNS must be enabled. To enable Dynamic DNS, use the **IPv4 Settings tab** or the **IPv6 Settings tab**.

To override the DHCP-supplied domain name manually, clear the **Use DHCP-Supplied Domain Name** check box, and then enter the domain name. Click **Apply**.

NOTE:

When the **Use DHCP-Supplied Domain Name** check box is selected, you cannot edit the domain name field.

Network Access

Using these settings, an administrator can configure settings relating to network access to the Onboard Administrator . These settings are specific to the enclosure and do not affect the network configurations for server blades.

Protocols tab

You can select the following protocol settings to allow or restrict access to the Onboard Administrator.

- **Enable Web Access (HTTP/HTTPS)**

  This check box is selected by default. Clearing this check box disables HTTP/HTTPS access to the Onboard Administrator. Port 80 is used for HTTP, and port 443 is used for HTTPS.

  CAUTION:

  Disabling Web Access (HTTP/HTTPS) disconnects all users attached to the Onboard Administrator through HTTP/HTTPS, including the administrator.

- **Enable Secure Shell**

  This check box is selected by default. Clearing this check box disables Secure Shell connections to the Onboard Administrator. SSH is disabled when Two-Factor or CAC Authentication is enabled. Disabling Two-Factor Authentication does not automatically re-enable SSH. To re-enable SSH, you must select the check box, and then click **Apply**.Disabling CAC will automatically re-enable SSH. Port 22 is used for SSH.

- **Enable Telnet**

  This check box is not selected by default. Selecting this check box enables Telnet connections to the Onboard Administrator . Telnet is disabled when Two-Factor or CAC Authentication is enabled. Disabling Two-Factor or CAC Authentication does not automatically re-enable Telnet. To re-enable Telnet, you must select the check box, and then click **Apply**. Port 23 is used for Telnet.

  NOTE:

  When the Onboard Administrator is operating in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug, the Telnet protocol cannot be used.

  Telnet is disabled after a factory reset or when Two-Factor or CAC Authentication is enabled.

- **Enable XML Reply**

  This check box is selected by default. This check box enables XML data to be shared between the Onboard Administrator and other Hewlett Packard Enterprise management tools such as Systems Insight Manager. To display the information that is shared by the Onboard Administrator if this protocol is enabled, click **View**.

XML Reply will be disabled when CAC Authentication is enabled. When CAC Authentication is enabled you will not be allowed to enable back XML Reply. But disabling CAC Authentication will automatically re-enable XML Reply.

- **Enable Enclosure iLO Federation Support**

  This check box is selected by default. This check box enables the Onboard Administrator support required to allow peer-to-peer network communication necessary for iLO Federation among suitably capable iLOs within the enclosure. When iLO Federation support is enabled for the enclosure, the active Onboard Administrator displays the device bay number of each bay for which the peer-to-peer network communication required for iLO Federation is enabled.

  IMPORTANT:

  Enable Enclosure iLO Federation Support only enables Onboard Administrator support to allow the peer-to-peer network communication necessary for iLO Federation among iLOs within the enclosure. To fully enable iLO Federation, each iLO must have the appropriate firmware and be configured to participate in iLO Federation. For more information, see the *HPE iLO 4 User Guide* at the **Hewlett Packard Enterprise website**.

- **Enable FQDN link support for accessing iLOs and interconnects**

  This check box is not selected by default. Selecting this check box causes the Onboard Administrator to display an FQDN-based web address link in addition to the usual IP-based web address links for accessing an iLO or interconnect from the Onboard Administrator GUI. The Onboard Administrator queries a DNS server that performs a reverse lookup for the FQDN of the device and generates the FQDN-based web address (formatted as host-name.domain-name.com). An IPv4 DNS server must be configured on the Onboard Administrator, and the devices to be accessed must be registered for reverse lookup with the DNS name server. A DNS IP address must be configured on the Onboard Administrator (use the Enclosure TCP/IP **IPv4 Settings tab**).

  When the FQDN setting is enabled, the lists of URL links for all the appropriate devices (iLOs and interconnects) are automatically refreshed and updated with the corresponding FQDNs. When the FQDN setting is disabled, the FQDN links of all the enclosure devices are removed from the Onboard Administrator and hence are not displayed.

  FQDN link support is useful in IPv6-based remote access environments that depend on an IPv4-based enclosure management network with IPv4 DNS. It is not meant for pure IPv6 environments with IPv6 DNS.

To save the settings, click **Apply.**

Trusted Hosts tab

Trusted Hosts

Use the Trusted Hosts feature to restrict access to the Onboard Administrator.

This subcategory contains one dialog box, one entry field, and one display box, that if enabled, is used to list trusted IP addresses.

The **Enable IP address access restriction** check box is not selected by default. Selecting this check box allows only those IP addresses listed as Trusted Addresses to connect to the Onboard Administrator.

CAUTION:

Enabling IP address access restriction without first entering the user's IP address in the Trusted Addresses list will disconnect the user from the Onboard Administrator.

When using the Trusted Hosts feature in an environment with multiple enclosures connected via enclosure link cables, ensure that all linked enclosures have the same Trusted Hosts settings. Linked enclosures that do not have the same Trusted Hosts settings may allow a web GUI user to access a protected enclosure from a non-trusted client.

RFC 4941 describes an IPv6 SLAAC extension that allows for generation of global-scope temporary IPv6 addresses using interface identifiers that change over time. When an OS that supports RFC 4941 reboots or the current address expires, a new temporary IPv6 address is generated. Windows 7 is an example of an OS that supports RFC 4941.

With trusted hosts enabled, if you are accessing the Onboard Administrator from a client hosted on an OS with RFC 4941 support, a reboot of the client OS can result in the inability to reconnect to the Onboard Administrator. The connection fails because the client’s new temporary IPv6 address does not match the IPv6 address configured for the client in the Trusted Addresses list. To avoid this issue, either disable generation of global-scope temporary IPv6 addresses in the OS, or reconfigure the Trusted Host IP address with the newly generated client IPv6 address.

The Trusted Addresses field is used to enter the IP addresses of all hosts that are to be trusted and allowed to connect remotely to the Onboard Administrator through the protocols set up in the Protocol Restrictions subcategory. This field allows for IP addresses only. When specifying an IPv6 address, do not specify the prefix length.

Below the Trusted Addresses field is the list box of all trusted IP addresses, if trusted IP addresses are configured.

To add a trusted host, enter the IP address in the Trusted Addresses field, and then click **Add**. You can add a maximum of five Trusted Addresses.

To remove a trusted host, select the IP address in the Trusted Addresses list, and then click **Remove**.

To save the settings, click **Apply**.

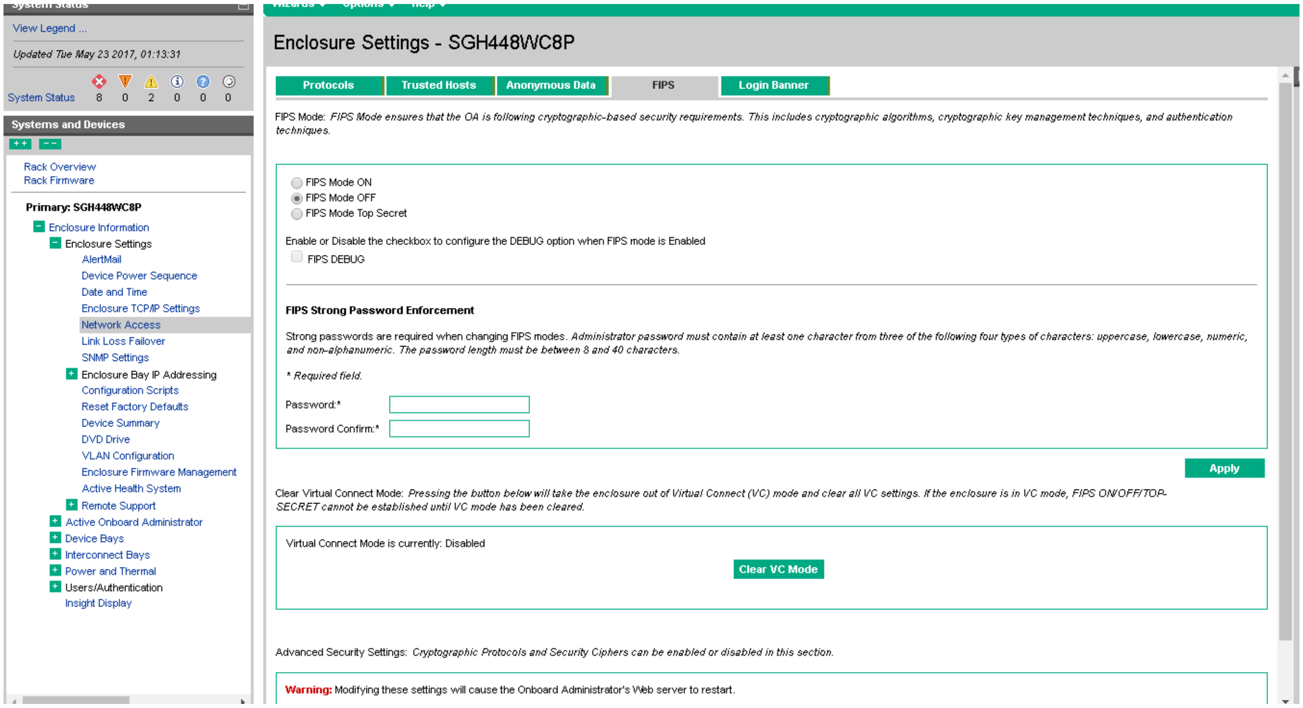
Anonymous Data tab

Enable Extended Data on GUI Login Page—This check box is selected by default. Clearing this check box disables the + functionality in the topology view on the sign in page for this enclosure. Also, the Onboard Administrator health status appears as `N/A` on the sign in page.

Disabling the extended data on the GUI sign in page prevents unauthenticated users from viewing additional information. To prevent additional information from appearing for each linked enclosure, you must clear this check box for each enclosure.

Click **Apply** to save settings.

FIPS tab



Enclosure Settings - SGH448WC8P

FIPS Mode: *FIPS Mode ensures that the OA is following cryptographic-based security requirements. This includes cryptographic algorithms, cryptographic key management techniques, and authentication techniques.*

○ FIPS Mode ON
● FIPS Mode OFF
○ FIPS Mode Top Secret

Enable or Disable the checkbox to configure the DEBUG option when FIPS mode is Enabled

□ FIPS DEBUG

FIPS Strong Password Enforcement

Strong passwords are required when changing FIPS modes. *Administrator password must contain at least one character from three of the following four types of characters: uppercase, lowercase, numeric, and non-alphanumeric. The password length must be between 8 and 40 characters.*

** Required field.*

Password:*

Password Confirm:*

Clear Virtual Connect Mode: *Pressing the button below will take the enclosure out of Virtual Connect (VC) mode and clear all VC settings. If the enclosure is in VC mode, FIPS ON/OFF/TOP-SECRET cannot be established until VC mode has been cleared.*

Virtual Connect Mode is currently: Disabled

Advanced Security Settings: *Cryptographic Protocols and Security Ciphers can be enabled or disabled in this section.*

Warning: Modifying these settings will cause the Onboard Administrator's Web server to restart.

FIPS Mode

NOTE:

FIPS Mode changes to ON/DEBUG/Top-Secret/Top-Secret Debug or OFF do not take effect unless VC Mode is disabled.

When the Onboard Administrator is operating in FIPS Mode ON, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. In FIPS Top-Secret Mode - certificates must have a minimum RSA key length of 3072 bits or ECDSA 384 bits, and the signature hash algorithm must be SHA-384.

- **FIPS Mode OFF**—Enables the use of non-FIPS-140-2-approved algorithms.
- **FIPS Mode ON**—Enforces the use of the Onboard Administrator in a FIPS 140-2-approved mode. This setting supports the use of approved cryptographic protocols and ciphers.
- **FIPS Mode TOP-SECRET**—Enforces the use of the Onboard Administrator in CNSA approved mode. This setting supports the use of approved cryptographic protocols and ciphers. FIPS mode DEBUG will no longer be a separate FIPS mode. Instead, DEBUG option can be enabled or disabled by an OA administrator when switching between FIPS Mode ON and FIPS Top-Secret.

The Onboard Administrator restarts after all changes are made.

IMPORTANT:

All existing settings are lost when you run this operation. Any change to the FIPS Mode setting performs a Restore to Factory Default operation.

NOTE:

When in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug, ensure that a strong password is set.

FIPS Mode status icons

With FIPS Mode ON or Top-Secret enabled , the current status of FIPS Mode is indicated by an icon displayed on the Onboard Administrator header bar on GUI screens. It is also displayed on the Onboard Administrator Sign-in page in the Connection column of the enclosure table. The status icons are described in the following table:

FIPS Mode icon	Description
FIPS	FIPS Mode is enabled (ON).
FIPS ⚠	FIPS Mode ON has one or more warnings. To determine the nature of the warning, hover the mouse pointer over the icon.
FIPS	FIPS Mode DEBUG is enabled.
FIPS ⚠	FIPS Mode DEBUG has one or more warnings. To determine the nature of the warning, hover the mouse pointer over the icon.
FIPS	FIPS Mode is enabled (Top-Secret).
FIPS	FIPS Mode Top-Secret Debug is enabled.

FIPS Strong Password Enforcement

When changing between available FIPS modes, strong passwords are enabled, minimum password length is set to eight characters, and a new Administrator account password is requested. Additionally, if changing to either FIPS Mode ON or FIPS Mode Top-Secret, the Enclosure IP Mode, Telnet, SNMPv1 and SNMPv2 protocols are disabled .In case of FIPS mode Top-Secret SNMPv3 is also disabled.

> **NOTE:**
>
> Entering and exiting FIPS Mode performs a factory restore operation and locks the Insight Display (LCD). If the Onboard Administrator was previously configured with a static IP address, it defaults to a DHCP address until reconfigured with a static IP address. Recovery requires access to the Onboard Administrator serial console to perform the `SHOW OA NETWORK` command to discover the new Onboard Administrator IP address.

The term "FIPS Mode" used in this document and within the product is to describe the feature, and not its validation status. The FIPS validation process is lengthy, so not all versions are FIPS validated. For information about the current FIPS status of this or any other firmware version, see the following documents:

- **Cryptographic Module Validation Program FIPS 140-1 and FIPS 140-2 Modules In Process List**
- **FIPS 140-1 and FIPS 140-2 Vendor List**
- **Commercial National Security Algorithm Suite**

Clear VC Mode

Clearing the VC mode removes all VC settings from the enclosure. Before clearing the VC mode, power off all VC-configured servers. If servers are not powered down, they might maintain the VC settings until they are rebooted. You must clear the VC mode before changing the FIPS Mode setting from OFF to ON/DEBUG/Top-Secret/Top-Secret Debug or vice versa.

To clear the VC Mode:

1. Click **Clear VC Mode**. A confirmation screen appears, stating `All servers should be powered off and not configured by Virtual Connect prior to clearing VC mode. Are you sure that you wish to clear VC mode?`
2. Click **OK**.

Advanced Security Settings

FIPS security requirements may change for a particular environment or as existing ciphers become vulnerable to attack. The OA administrator can customize security settings by enabling or disabling selected TLS cryptographic protocols and ciphers that the Onboard Administrator can use for negotiating secure connections. Supported protocols and ciphers are listed in "Cryptographic security capabilities and defaults."

CAUTION:

Disabling one or more ciphers might cause some clients to lose connectivity to the Onboard Administrator GUI, depending on the order and list of ciphers supported by the client.

NOTE:

After you apply settings, the Onboard Administrator web service restarts.

To change advanced security settings:

1. Display the list of supported cryptographic protocols and ciphers by clicking **Edit Advanced Security Settings**.
2. To enable or disable a protocol or cipher, select or deselect the corresponding check box. You cannot disable all protocols or all ciphers. At least one protocol and one cipher must be enabled at all times.
3. Click **Apply**.

NOTE:

In FIPS OFF mode, when OA versions 4.70 and later are downgraded, the selection of protocols and ciphers will revert to the default list.

Login Banner tab

Enabling the Login Banner option requires Onboard Administrator users to acknowledge the banner text before they can log in.

Enable Display of Banner on User Login—Select this check box to enable the Login Banner option. Acknowledgment of the Login Banner text provides access to all systems connected to the primary Onboard Administrator.

Banner Text—The field size is limited to 1,500 printable characters, excluding the % \ < > ( ) and # characters. While spaces and line feeds are accepted, using only white-space characters within this text field is not allowed.

NOTE:

The Login Banner accepts English (ASCII) characters only.

Apply—Click to validate the Banner Text field. If the Banner Text field is empty or contains only white-space characters, but the Enable Display of Banner on User Login check box is selected, you are prompted to disable this feature.

Link Loss Failover

This screen enables you to configure automatic Onboard Administrator redundancy failover based on network link status. For Link Loss Failover to function correctly, the redundancy status of the Onboard Administrators must be OK. An OK status means that both Onboard Administrators have the same firmware version (firmware version 2.20 or higher), and that they are communicating properly.

Enable Link Loss Failover—This check box enables or disables automatic Link Loss Failover.

Failover Interval—The failover interval is the amount of time the active Onboard Administrator must be without a link on the external Ethernet interface before the system considers an automatic failover. The interval must be between 30 and 86400 seconds.

Click **Apply** to save the settings.

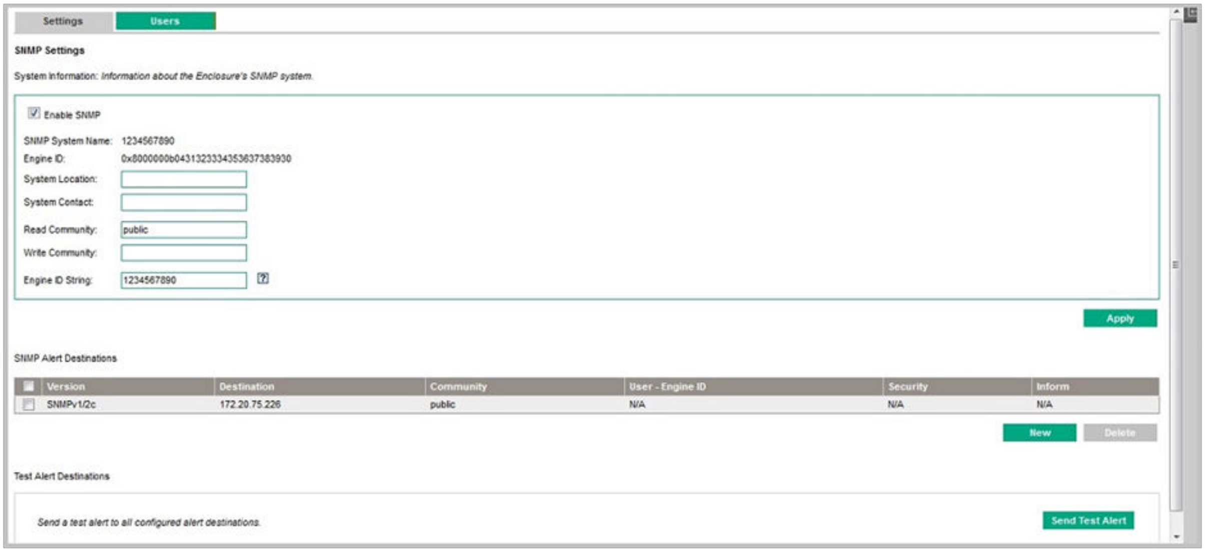
SNMP overview

SNMP is a protocol used to communicate management information between network management applications and Onboard Administrator. The Onboard Administrator supports SNMP Version 1, Version 2, and Version 3, and several groups from the standard MIB-II MIB. Additional information about the enclosure infrastructure is available in the HPE Rack Information MIB. The Rack Information MIB (CPQRACK-MIB) is part of the Insight Management MIBs and is found on the Management CD in the ProLiant Essentials Foundation Pack.

OA generates SNMPv1 traps when configured in SNMPv1/v2c mode or SNMPv3 traps when configured in SNMPv3 mode. OA acts as a pass through for the SNMP v2 traps generated by VC or iLO. SNMPv3 provides support for encryption of the agent data via either DES or AES128, using a user-provided password. A dedicated set of SNMP users is maintained each with a set of authorization and authentication passwords, along with another set of per user permissions.

SNMP Settings

The SNMP Settings screen enables you to enter system information and community strings and designate the management stations that can receive SNMP traps from the Onboard Administrator. If you select **Enable SNMP**, then the Onboard Administrator responds to SNMP requests over UDP port 162. Port 162 is the standard UDP port used to send and retrieve SNMP messages.



SNMP Settings

System information: *Information about the Enclosure's SNMP system.*

☑ Enable SNMP

SNMP System Name: 1234567890
Engine ID: 0x8000000b0431323334353637383930
System Location:
System Contact:
Read Community: public
Write Community:
Engine ID String: 1234567890

SNMP Alert Destinations

□	Version	Destination	Community	User - Engine ID	Security	Inform
□	SNMPv1/2c	172.20.75.226	public	N/A	N/A	N/A

Test Alert Destinations

Send a test alert to all configured alert destinations.

In the System Information subcategory, information about the Onboard Administrator SNMP system can be enabled and configured.

The **Enable SNMP** check box is not selected by default. When this check box is selected, the Onboard Administrator can be polled for status and basic information. A SNMP client can clear SNMP alerts and status only when you enable the Write Community string. To disable SNMP access to the Onboard Administrator, clear the **Enable SNMP** check box.

NOTE:

While in FIPS Mode ON, the SNMPv1 and SNMPv2 are disabled, and you can create only SNMPv3 traps only in FIPS Mode ON. In TOP-SECRET mode SNMPv1 ,SNMPv2 and SNMPv3 are disabled.

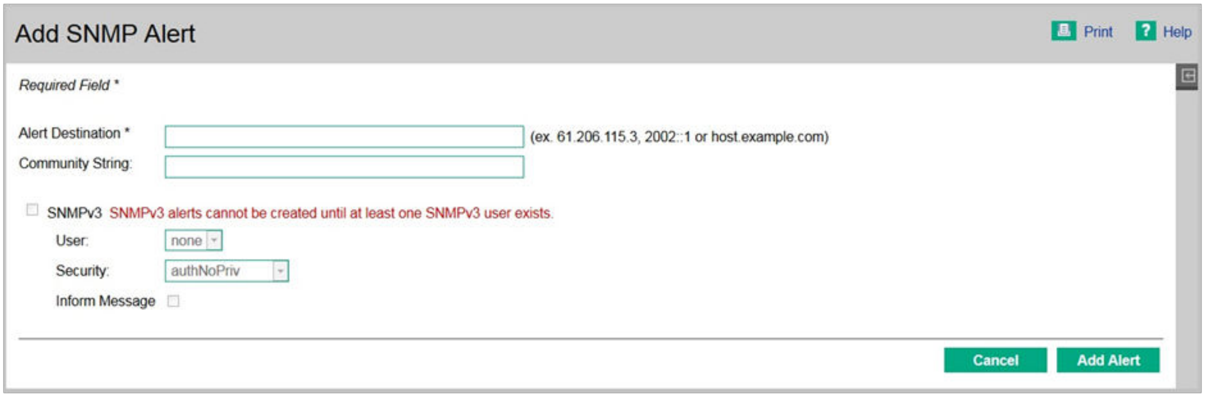
Field	Possible value	Description
System Location	0 to 20 characters including all printable characters and the space	The SNMP location of the enclosure typically used to identify the physical or topographical location of the Onboard Administrator.
System Contact	0 to 20 characters including all printable characters and the space	The name of the system contact, used to identify an individual or group of individuals who are to be contacted in the event of any status change in the Onboard Administrator.
Read Community	0 to 20 characters including all printable characters and the space	The Read Community string enables the client to read information but not to manipulate the alerts or status of the Onboard Administrator through SNMPv1 or SNMPv2. The default community name is "public" and will allow a user to receive notification traps and alerts, but not to change or manipulate the status.
Write Community	0 to 20 characters including all printable characters and the space	The Write Community string enables the client to manipulate alerts of Onboard Administrator status through SNMPv1 or SNMPv2. You can remotely clear alerts and mark them as "viewed" or otherwise through their SNMP management client thrugh the SNMP agents.
Engine ID String	1 to 27 printable characters, final Engine ID will be a hexadecimal string that begins with '0x' and is derived from this string	The Engine ID String is used to create the engine ID hex value. The engine ID is combined with the user name to create a SNMPv3 user for each enclosure. When the engine ID is unique to an enclosure, users with the same name on different enclosures are unique. The Engine ID string defaults to the serial number of the enclosure.

Adding SNMP alert destinations

Procedure

1. Click **New** on the SNMP Settings screen.

   The Add SNMP Alert screen appears.



Add SNMP Alert

Required Field *

Alert Destination * (ex. 61.206.115.3, 2002::1 or host.example.com)

Community String:

□ SNMPv3 SNMPv3 alerts cannot be created until at least one SNMPv3 user exists.

User: none

Security: authNoPriv

Inform Message □

2. Make entries in the following fields:

- **Alert Destination** (required)
- **Community String** (optional)

The following table defines the entries that can be made in these fields.

Field	Possible value	Description
Alert Destination	Protocol: • udp—For IPv4 udp traps • udp6 or udpv6 or udpipv6—For ipv6 udp traps • tcp—For IPv4 tcp traps (only for snmpv3) • tcp6 or tcpv6 or tcpipv6—For ipv6 tcp traps (only for snmpv3) Destination: • IPv4 address—###.###.###.### where ### ranges from 0 to 255 • IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. • DNS name—1 to 64 characters including all alphanumeric characters and the dash (-). Port: The port number is any valid and available udp/tcp port number in the range of [1;65535] (both inclusive). If port is specified for an IPv6 address, the IPv6 address must be enclosed in [...]; for example, [####:####::####]:162 to specify port 162.	The management station IP address or DNS name. Alert destination can be specified in [protocol:]destination[:port] format. Both protocol and port are optional parameters.
Community String	0 to 20 characters including all printable characters and the space	A text string that acts as a password. It is used to authenticate messages that are sent between management server and Onboard Administrator.

3. Select the **SNMPv3** check box to configure the remaining fields.

   If this check box has been selected, proceed to step 4. Otherwise, proceed to step 5.

4. In the **User** field, select the user account to be used to send the trap/inform.

   The desired user-engineID must be created before the alert destination can be added.

5. In the **Security** field, enter the security level used to send the trap/inform.

   The following security options are available:

   - No authorization or encryption (noAuthNoPriv)
   - Authorization but no encryption (authNoPriv)
   - Authorization and encryption (authPriv)

   The default option is authNoPriv.

6. Select the **Inform Message** check box to receive notification that the trap has been received.

If Inform Message is enabled, the agent expects to receive notification from the management application that the trap has been received. If no inform acknowledgment is received, the agent retries to send traps.

Alerts with Inform Message enabled must have a remote user, which is available on a management solution.

7. Click **Add Alert** to proceed with adding the SNMP alert.

   To send a test SNMP trap to all of the configured trap destinations, click **Send Test Alert**. You must enable SNMP to use this function.

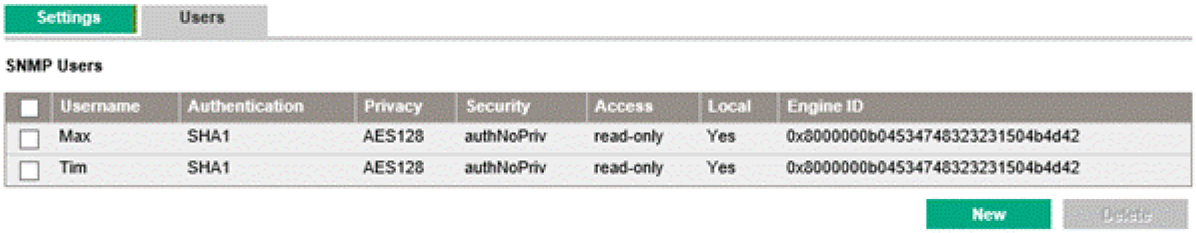
Removing an SNMP alert destination

Procedure

1. On the SNMP Settings screen, select the check box corresponding to the SNMP alert destination to delete.
2. Click **Delete**.

Adding SNMP users

To add a new SNMP user, click **New** on the SNMP Users tab.



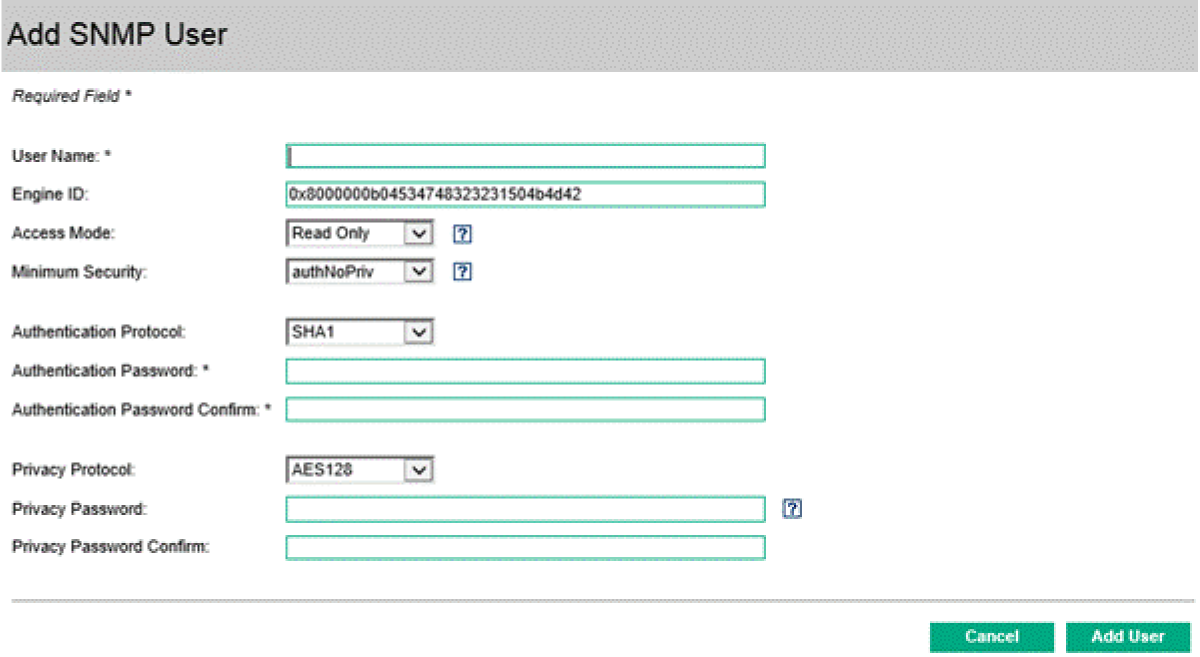
SNMP Users

□	Username	Authentication	Privacy	Security	Access	Local	Engine ID
□	Max	SHA1	AES128	authNoPriv	read-only	Yes	0x8000000b04534748323231504b4d42
□	Tim	SHA1	AES128	authNoPriv	read-only	Yes	0x8000000b04534748323231504b4d42

Figure 3: SNMP Users tab

To remove a current SNMP user, select the check box, and click **Delete**.

When New is selected, the Add SNMP User screen displays.



Add SNMP User

*Required Field **

User Name: *	
Engine ID:	0x8000000b04534748323231504b4d42
Access Mode:	Read Only
Minimum Security:	authNoPriv
Authentication Protocol:	SHA1
Authentication Password: *	
Authentication Password Confirm: *	
Privacy Protocol:	AES128
Privacy Password:	
Privacy Password Confirm:	

To set up your new SNMP user's information, use the following fields.

Field	Possible value	Description
User Name	A unique string containing 1 to 32 characters; all characters must be either alphanumeric or dash or underscore and the first character must be alphabetic.	User account name used for SNMPv3 queries, traps, and informs. Each username/ engine id pair must be unique and cannot be duplicated.
Engine ID	Must begin with '0x' followed by an even number of up to 64 hexadecimal digits.	The engine ID is combined with the user name to create a SNMPv3 user for each enclosure. When the engine ID is unique to an enclosure, users with the same name on different enclosures are unique. Defaults to a unique Engine ID for the enclosure. Only used for creating remote accounts used with INFORM messages.
Access Mode	• Read Only • Read Write	Only applies to local users. Specifies this user has read/write access to the OID tree. If not specified the user will have read-only access.
Minimum Security	• noAuthNoPriv—Allows unauthenticated operations • authNoPriv—Requires authentication • authPriv—Requires encryption	Only applies to local users. Minimal level of security required for operation. By default, operation is required to be signed but not encrypted (authNoPriv).
Authentication Protocol	• SHA1 • MD5	Use the MD5 or SHA1 algorithm along with the passphrase to authenticate or ‘sign’ each operation. MD5 cannot be specified in FIPS Mode ON.
Authentication Password	8 to 40 characters, including all printable characters	The password associated with the user.
Authentication Password Confirm	8 to 40 characters, including all printable characters	The password associated with the user. This value must match the Authentication Password value.
Privacy Protocol	• AES128 • DES	Use the DES or AES128 algorithm along with the passphrase to encrypt the trap. DES cannot be specified in FIPS Mode ON.
Privacy Password	Must contain 8 to 40 printable characters.	Used to encrypt operations. If not specified, the authentication password is used.
Privacy Password Confirm	Must contain 8 to 40 printable characters.	Used to encrypt operations. If not specified, the authentication password is used.

To proceed with adding the SNMP user, click **Add User**.

Enclosure Bay IP Addressing

The EBIPA screens allow you to configure IPv4 and IPv6 fixed addresses for Onboard Administrator enclosure bays. The Onboard Administrator EBIPA feature helps you provision a fixed IP address based on bay number, which preserves the IP address for a particular bay even if a device is replaced. The management interface for components plugged into the bays must be set for DHCP. EBIPA can only be used if the devices are set to boot from DHCP. If a device is configured for static IP, then it must be manually reconfigured to DHCP to change the EBIPA IP address.

NOTE:

The Onboard Administrator documentation refers to EBIPA IP addresses as "fixed IP addresses" or "fixed DHCP addresses," meaning that each of these addresses is an IP address permanently associated with a specific bay number independent of the actual device currently attached to the bay.

The server blade iLO bays and interconnect module management bays can obtain IP addresses on the management network in several ways: dynamic IP addressing using an external DHCP server, static IP addressing, SLAAC via router advertisements (IPv6 only), or EBIPA. If your network has a DHCP service or if you want to manually assign static IP addresses one by one to the server blades iLO and interconnect modules, bypass configuring Enclosure Bay IP Addressing.

EBIPA only assigns fixed DHCP IP addresses to the management interface for server iLOs and interconnect modules on the management network internal to the enclosure. EBIPA does not assign IP addresses for any other devices on the management network external to the enclosure and cannot be used as a DHCP server on the production network.

The server blade iLO defaults to DHCP addressing, which is obtained through the network connector of the Active Onboard Administrator. Interconnect modules that have an internal management network connection to the Onboard Administrator might also default to DHCP addressing.

NOTE:

EBIPA enforces unique IP addresses for all bays, even if bays are on a different VLAN.

EBIPA configuration guidelines

This provides general configuration information. For configuration information specific to IPv4 and IPv6, see **EBIPA for IPv4** and **EBIPA for IPv6**.

If your facility prefers fixed IP address assignment, you can specify unique fixed addresses individually for each of the server blade iLO bays and interconnect module management bays, or you can use EBIPA to assign a range of fixed IP addresses to individual server blade and interconnect module bays. If you specify fixed addresses individually, the subnet mask (IPv4), gateway, DNS servers, NTP servers (IPv4 interconnect), and domain name can be the same or different for each bay. If you use EBIPA to assign a range of fixed addresses, you must specify the first IP address in a range and the subnet mask. When you click the **Autofill** down arrow button for that bay, the bays listed below that bay are automatically assigned consecutive IP addresses. The subnet mask, gateway, DNS servers, NTP servers, and domain name are also copied to each of the consecutive bays in the list.

For example, if you specify IPv4 address 16.100.226.21 for EBIPA bay 1, then using the Autofill feature, bays 1 through 16 are assigned consecutive IP addresses in the range 16.100.226.21 to 16.100.226.36. If you specify 16.200.139.51 for interconnect bay 3 and use the feature, interconnect bays 3 through 8 are assigned consecutive IP addresses in the range 16.200.139.51 to 16.200.139.56.

NOTE:

The **Autofill** button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on.

When using Autofill, specify an IPv4 subnet mask or IPv6 subnet prefix that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a subnet mask or prefix that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.

If you use fixed IP addresses for management processors, then the Onboard Administrator `hponcfg` command can be used to send the iLO network settings RIBCL script to an iLO if that iLO already has an IP address. EBIPA can be used to bootstrap IP addresses to iLOs, so that Onboard Administrator `hponcfg` command can be used to send configuration scripts to those iLOs. Changes to iLO network settings results in that iLO resetting the network interface and breaking the current connections for a few seconds.

If you have double dense server blades, do not configure EBIPA settings for the base bays (Bay 1, 2, and so forth). Configure the side A bays (1A, 2A, and so on) and side B bays (1B, 2B, and so on). Using the Autofill feature assigns consecutive IP addresses to the bays listed below the bay where you specify the first IP address in the range (for example, if you specify the IP address for bay 1A and use the Autofill feature, bays 2A, 3A, and so on are assigned consecutive addresses).

To configure the interconnect bays, use the **Interconnect Bays** tab.

To apply settings, click **Apply**.

Servers in the device bays automatically acquire the device bay EBIPA addresses within a few minutes, but the interconnect switch modules must be manually restarted by clicking the **Virtual Power** button on each Onboard Administrator Interconnect Module information page.

⚠ **CAUTION:**

EBIPA configuration changes on a server bay that is already using EBIPA addressing causes a reset of the EBIPA-configured iLO. The iLO then attempts to obtain an IP address, which might result in loss of connectivity for clients currently accessing the iLO using the previously configured address. For an interconnect bay, an automatic reset does not occur but configuration changes might result in loss of connectivity for clients currently accessing the interconnect using the previously configured address.

Disabling EBIPA-configured addressing causes the affected devices to lose their current EBIPA-configured address. Any clients accessing the devices via that address will lose connectivity. To ensure client access, the devices should be configured with an address, such as through an external DHCP service or assigning a static IP address.

Setting up your enclosure using EBIPA without an active network connection

Procedure

1. Configure a static IP for each Onboard Administrator using Insight Display, and note the active OA Service IP address on the Insight Display Enclosure Info screen. Attach the client PC to the enclosure Service Port (Enclosure Link Up connector) between the OA bays with a standard Ethernet patch cable. The client PC NIC must be configured for DHCP because it acquires an IP address in the range 169.254.x.y approximately 1 minute later.
2. Launch a web browser (or alternatively a Telnet or SSH session), and select the Onboard Administrator Service IP address as displayed in the enclosure Insight Display on the Enclosure Info screen.
3. Using the administrative password attached to the active Onboard Administrator, log in to the Onboard Administrator as Administrator.
4. Enable Device Bay EBIPA with a starting fixed IP address and enable Interconnect Bay EBIPA with a different starting IP address.

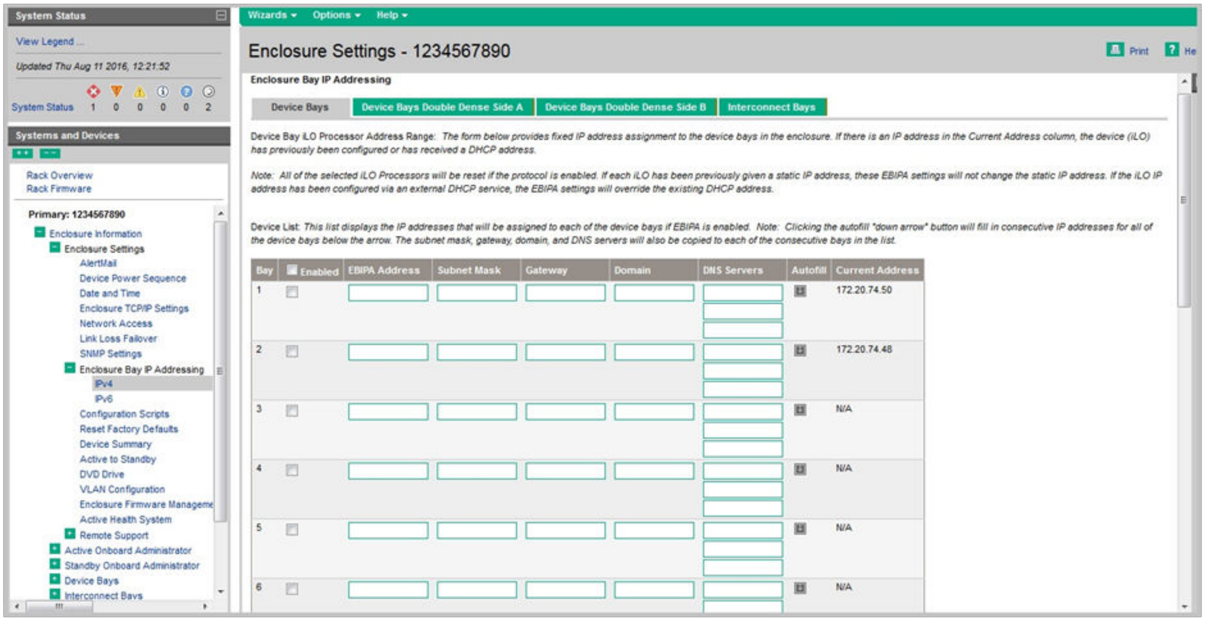
   Clicking the **Autofill** button creates as many sequential, fixed IP addresses as needed. The subnet mask, gateway, DNS servers, NTP servers, and domain name are also copied to each of the consecutive bays in the list. Alternatively, you can assign individual fixed IP addresses by manually entering the desired IP address in the EBIPA Address field for the specific bay. The subnet mask, gateway, DNS servers, NTP servers, and domain can be same or different for each bay.

After you apply settings, servers in the device bays automatically acquire the device bay EBIPA addresses within a few minutes, but the interconnect switch modules must be manually restarted by clicking the **Virtual Power** button on each Onboard Administrator Interconnect Module information page.

5. To verify that the server blade iLO addresses have been set according to the EBIPA starting IP address and range, use the Onboard Administrator Device list.

EBIPA for IPv4

EBIPA for IPv4 Device Bays tab



Enclosure Settings - 1234567890

Enclosure Bay IP Addressing

Device Bay iLO Processor Address Range: *The form below provides fixed IP address assignment to the device bays in the enclosure. If there is an IP address in the Current Address column, the device (iLO) has previously been configured or has received a DHCP address.*

Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IP address, these EBIPA settings will not change the static IP address. If the iLO IP address has been configured via an external DHCP service, the EBIPA settings will override the existing DHCP address.

Device List: *This list displays the IP addresses that will be assigned to each of the device bays if EBIPA is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IP addresses for all of the device bays below the arrow. The subnet mask, gateway, domain, and DNS servers will also be copied to each of the consecutive bays in the list.*

Bay	□ Enabled	EBIPA Address	Subnet Mask	Gateway	Domain	DNS Servers	Autofill	Current Address
1	□							172.20.74.50
2	□							172.20.74.48
3	□							N/A
4	□							N/A
5	□							N/A
6	□							N/A

IMPORTANT:

Do not use the 169.254.x.x range when configuring EBIPA-assigned addresses, as this network address range is reserved for use by the Onboard Administrator.

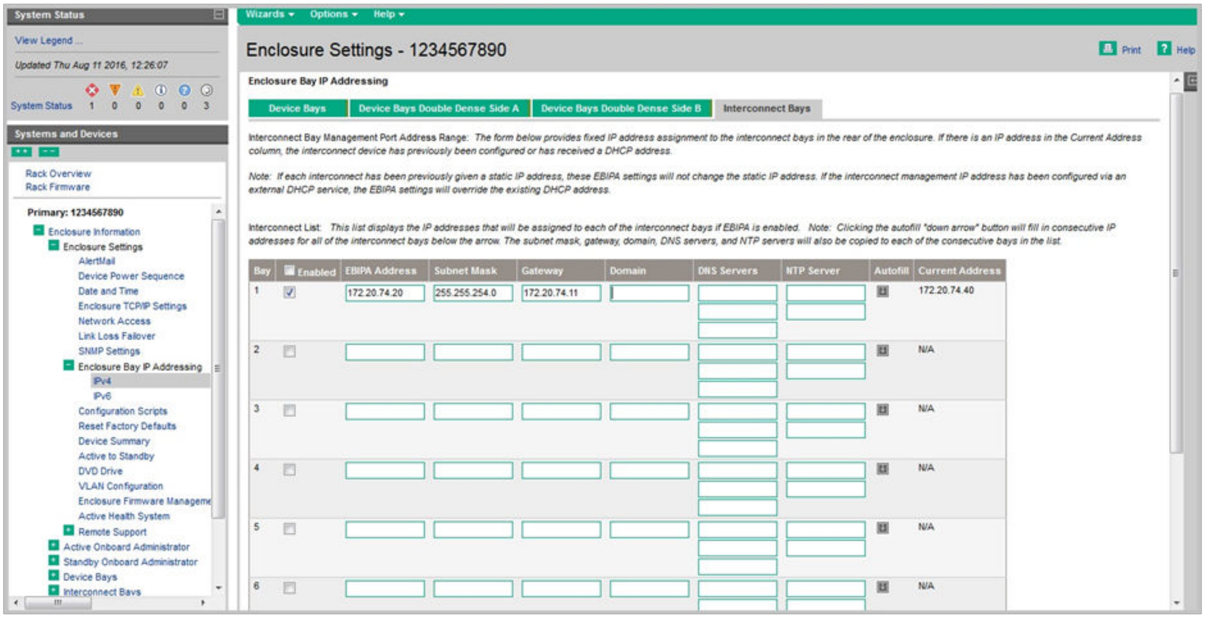
Device list

Column	Description
Bay	The bay in the enclosure of the device.
Enabled	Enables EBIPA settings for the device bay. EBIPA settings for all device bays can be enabled by selecting the check box next to Enabled in the heading row or individual device bays can be selected by clicking the check box for that particular device bay.
EBIPA Address	The fixed IP address you want to assign to the device bay. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Subnet Mask	Subnet mask for the device bays. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Gateway	The fixed gateway IP address that you want to assign for the device bays. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Domain	Domain name for the device bays. Possible values are a character string with a maximum of 64 characters, including all alphanumeric characters, the dash (-), and the period (.).

Table Continued

Column	Description
DNS Servers	IP addresses for primary, secondary, and tertiary DNS servers. Possible values are ###.###.###.### where ### ranges from 0 to 255.
Autofill	Assigns consecutive IP addresses for the selected device bays below in the device list. To assign the IP addresses, click the **Autofill** down arrow. The **Autofill** button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on. When using Autofill, specify an IPv4 subnet mask that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a subnet mask that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.
Current Address	The current IP address of the device bay.

EBIPA for IPv4 Interconnect Bays tab



Enclosure Settings - 1234567890

Enclosure Bay IP Addressing

Interconnect Bay Management Port Address Range: *The form below provides fixed IP address assignment to the interconnect bays in the rear of the enclosure. If there is an IP address in the Current Address column, the interconnect device has previously been configured or has received a DHCP address.*

Note: *If each interconnect has been previously given a static IP address, these EBIPA settings will not change the static IP address. If the interconnect management IP address has been configured via an external DHCP service, the EBIPA settings will override the existing DHCP address.*

Interconnect List: *This list displays the IP addresses that will be assigned to each of the interconnect bays if EBIPA is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IP addresses for all of the interconnect bays below the arrow. The subnet mask, gateway, domain, DNS servers, and NTP servers will also be copied to each of the consecutive bays in the list.*

Bay	□ Enabled	EBIPA Address	Subnet Mask	Gateway	Domain	DNS Servers	NTP Server	Autofill	Current Address
1	☑	172.20.74.20	255.255.254.0	172.20.74.11					172.20.74.40
2	□								N/A
3	□								N/A
4	□								N/A
5	□								N/A
6	□								N/A

Interconnect List

IMPORTANT:

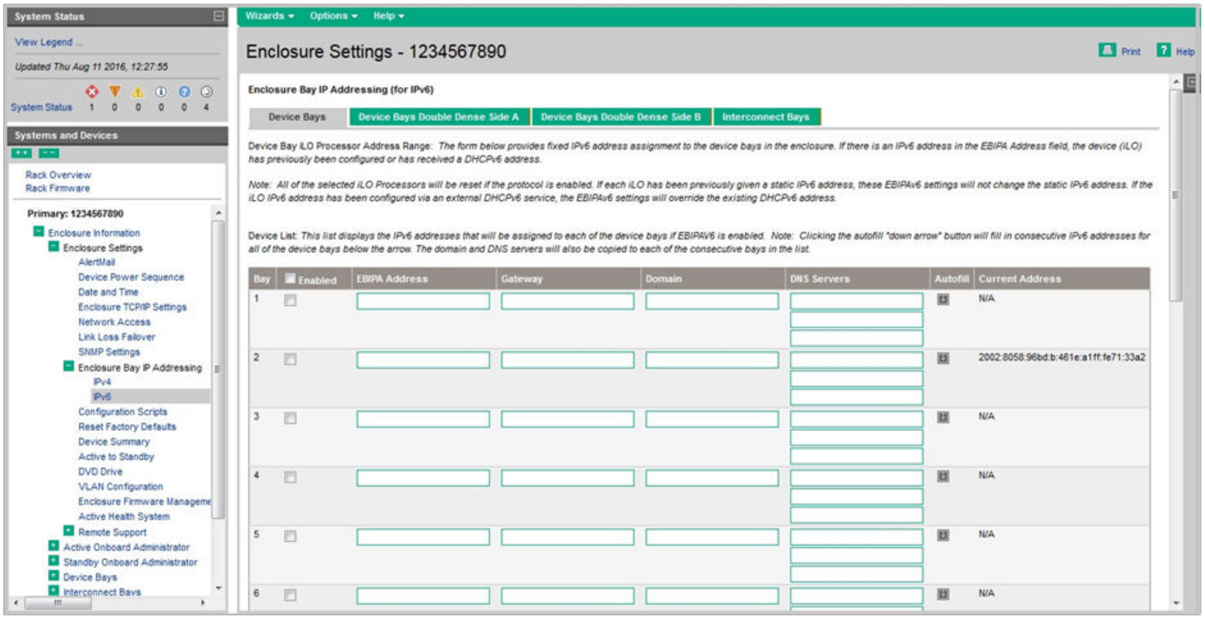
Do not use the 169.254.x.x range when configuring EBIPA-assigned addresses, as this network address range is reserved for use by the Onboard Administrator.

Column	Description
Bay	The bay in the enclosure of the interconnect device.
Enabled	Enables EBIPA for IPv4 settings for the interconnect bay. EBIPA for IPv4 settings for all interconnect bays can be enabled by selecting the check box next to Enabled in the heading row or individual interconnect bays can be enabled by selecting the check box for that particular interconnect bay.
EBIPA Address	The fixed DHCP IP address you want to assign to the device bay.
Subnet Mask	Subnet mask for the device bays. Possible values are ###.###.###.###, where ### ranges from 0 to 255.
Gateway	Gateway address for the device bays. Possible values are ###.###.###.###, where ### ranges from 0 to 255.
Domain	Domain name for the device bays. Possible values are a character string with a maximum of 64 characters, including all alphanumeric characters, the dash (-), and the period (.).
DNS Servers	IPv4 addresses for primary, secondary, and tertiary DNS servers. Possible values are ###.###.###.### where ### ranges from 0 to 255.
NTP Server	The IPv4 address of the server used for synchronizing time and date using the NTP protocol. ###.###.###.###, where ### ranges from 0 to 255.
Autofill	Assigns consecutive IPv4 addresses for the selected interconnect bays below in the interconnect list. To assign the IP addresses, click the **Autofill** down arrow. The Autofill button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on. When using Autofill, specify an IPv4 subnet mask that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a subnet mask that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.
Current Address	The current IPv4 address of the interconnect bay.

To save the EBIPA for IPv4 settings for the interconnect bays, click **Apply.**

EBIPA for IPv6

EBIPA for IPv6 Device Bays tab



Enclosure Settings - 1234567890

Enclosure Bay IP Addressing (for IPv6)

Device Bay iLO Processor Address Range: *The form below provides fixed IPv6 address assignment to the device bays in the enclosure. If there is an IPv6 address in the EBIPA Address field, the device (iLO) has previously been configured or has received a DHCPv6 address.*

Note: *All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IPv6 address, these EBIPAv6 settings will not change the static IPv6 address. If the iLO IPv6 address has been configured via an external DHCPv6 service, the EBIPAv6 settings will override the existing DHCPv6 address.*

Device List: *This list displays the IPv6 addresses that will be assigned to each of the device bays if EBIPAV6 is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the device bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.*

Bay	☐ Enabled	EBIPA Address	Gateway	Domain	DNS Servers	Autofill	Current Address
1	☐						N/A
2	☐						2002:8058:96bd:b:461e:a1ff:fe71:33a2
3	☐						N/A
4	☐						N/A
5	☐						N/A
6	☐						N/A

IMPORTANT:

Do not use the fe80::/10 prefix when configuring EBIPA-assigned addresses, as this network prefix is reserved for link local SLAAC addresses.

NOTE:

For EBIPA IPv6 fixed addresses to be successfully configured, the **Enable IPv6** setting must be enabled. To enable this setting, use the First Time Setup Wizard Network IPv6 Settings screen or the Enclosure Settings IPv6 Settings tab.

The **Enable SLAAC** and **Enable DHCPv6** settings have no effect on EBIPA IPv6 functionality.

Device list

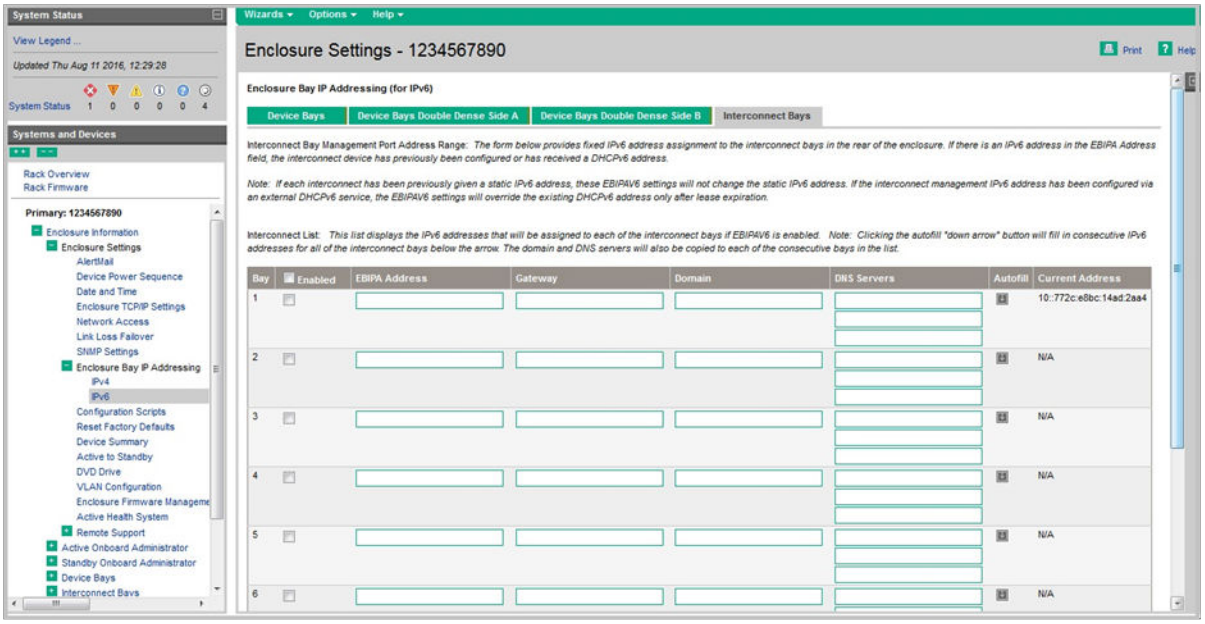
Column	Description
Bay	The bay in the enclosure of the device.
Enabled	Enables EBIPA settings for the device bay. EBIPA settings for all device bays can be enabled by selecting the check box next to Enabled in the heading row or individual device bays can be selected by clicking the check box for that particular device bay.
EBIPA Address	The fixed IPv6 address you want to assign to the device bay. Possible values are ####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. The prefix /### ranges from 1 to 128; the prefix length is mandatory.

Table Continued

Column	Description
Gateway	The fixed IPv6 gateway address you want to assign for the device bays. Possible values are ####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. Do not specify a prefix. The gateway is assumed reachable from within the network. If this gateway is specified as a Link-Local address, the gateway will always be configured on the enclosure device using this address. If the gateway is specified with any other type of IPv6 address, the Onboard Administrator sends neighbor solicitation requests to identify the Link-Local address of the gateway device for use in configuring the enclosure device. If the gateway does not exist or does not respond to neighbor solicitation requests, no gateway is configured.
Domain	Domain name for the device bays. Possible values are a character string with a maximum of 64 characters, including all alphanumeric characters, the dash (-), and the period (.).
DNS Servers	IPv6 addresses for primary, secondary, and tertiary DNS servers. Possible values are ####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.
Autofill	Assigns consecutive IPv6 addresses for the selected device bays below in the device list. To assign the IP addresses, click the **Autofill** down arrow. The Autofill button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on. When using Autofill, specify an IPv6 subnet prefix that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a prefix that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.
Current Address	The current IPv6 address of the device bay.

To save the EBIPA for IPv6 settings for the device bays, click **Apply**.

EBIPA for IPv6 Interconnect Bays tab



Enclosure Settings - 1234567890

Enclosure Bay IP Addressing (for IPv6)

Interconnect Bay Management Port Address Range: *The form below provides fixed IPv6 address assignment to the interconnect bays in the rear of the enclosure. If there is an IPv6 address in the EBIPA Address field, the interconnect device has previously been configured or has received a DHCPv6 address.*

Note: *If each interconnect has been previously given a static IPv6 address, these EBIPAV6 settings will not change the static IPv6 address. If the interconnect management IPv6 address has been configured via an external DHCPv6 service, the EBIPAV6 settings will override the existing DHCPv6 address only after lease expiration.*

Interconnect List: *This list displays the IPv6 addresses that will be assigned to each of the interconnect bays if EBIPAV6 is enabled.* Note: *Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the interconnect bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.*

Bay	☐ Enabled	EBIPA Address	Gateway	Domain	DNS Servers	Autofill	Current Address
1	☐						10::772c:e8bc:14ad:2aa4
2	☐						N/A
3	☐						N/A
4	☐						N/A
5	☐						N/A
6	☐						N/A

Interconnect List

IMPORTANT:

Do not use the fe80::/10 prefix when configuring EBIPA-assigned addresses, as this network prefix is reserved for link local SLAAC addresses.

Column	Description
Bay	The bay in the enclosure of the interconnect device.
Enabled	Enables EBIPA for IPv6 settings for the interconnect bay. EBIPA for IPv6 settings for all interconnect bays can be enabled by selecting the check box next to Enabled in the heading row or individual interconnect bays can be enabled by selecting the check box for that particular interconnect bay.
EBIPA Address	The fixed DHCP IPv6 IP address you want to assign to the interconnect bay. Possible values are ####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. The prefix /### ranges from 1 to 128; the prefix length is mandatory.
Gateway	The fixed gateway IPv6 address you want to assign for the interconnect bays. Possible values are ####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. Do not specify a prefix. The gateway is assumed reachable from within the network. If this gateway is specified as a Link-Local address, the gateway will always be configured on the enclosure device using this address. If the gateway is specified with any other type of IPv6 address, the Onboard Administrator sends neighbor solicitation requests to identify the Link-Local address of the gateway device for use in configuring the enclosure device. If the gateway does not exist or does not respond to neighbor solicitation requests, no gateway is configured.
Domain	Domain name for the device bays. Possible values are a character string with a maximum of 64 characters, including all alphanumeric characters, the dash (-), and the period (.).

Table Continued

Column	Description
DNS Servers	IPv6 addresses for primary, secondary, and tertiary DNS servers. Possible values are ####:####:####:####:####:####:####:####, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.
Autofill	Assigns consecutive IPv6 addresses for the selected interconnect bays below in the interconnect list. To assign the IP addresses, click the **Autofill** down arrow. The Autofill button only fills all address fields if the associated address field with the first address in the list is clicked. For example, Autofill for address 1 will fill addresses 1-16, Autofill for address 2 will fill 2-16, and so on. When using Autofill, specify an IPv6 subnet prefix that allows for enough available addresses on the associated subnet to fill all address fields corresponding to the total number of bays selected. If you specify a prefix that does not meet that requirement, "Invalid IP Address" displays in the address field of each bay for which an address could not be generated.
Current Address	The current IPv6 address of the interconnect bay.

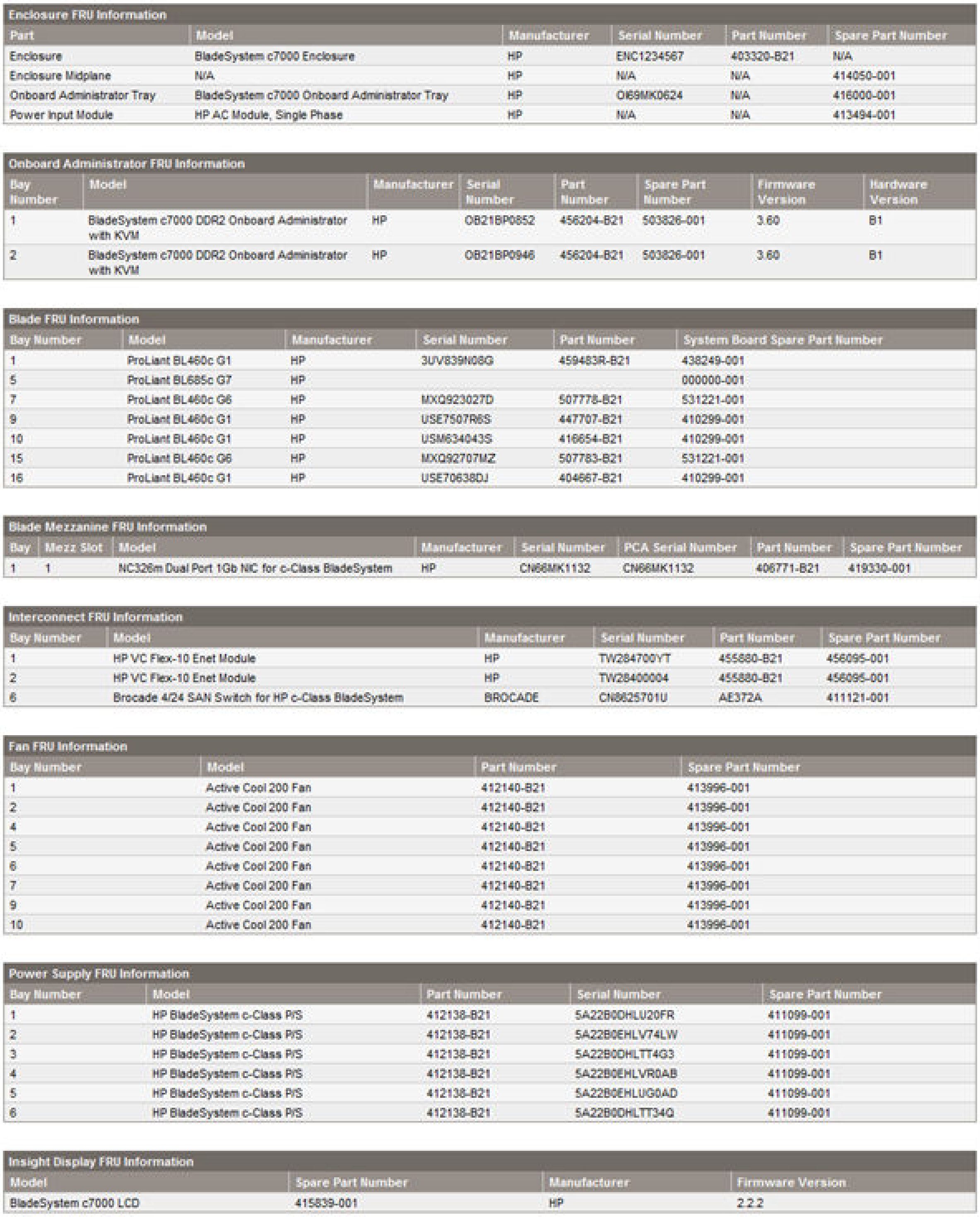
To save the EBIPA for IPv6 settings for the interconnect bays, click **Apply**.

Device Summary

The FRU Summary section provides information on all field replaceable units within the enclosure. Information provided in this section can quickly aid the administrator in contacting Hewlett Packard Enterprise Customer Service for troubleshooting, repair, and ordering replacements.

The information is organized in table format and divided into subcategories within the Device Summary section:

- Enclosure
- KVM Module Onboard Administrators
- Blades
- Blade Mezzanines
- Interconnects
- Fans
- Power supplies
- Insight Display



Enclosure FRU Information

Part	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
Enclosure	BladeSystem c7000 Enclosure	HP	ENC1234567	403320-B21	N/A
Enclosure Midplane	N/A	HP	N/A	N/A	414050-001
Onboard Administrator Tray	BladeSystem c7000 Onboard Administrator Tray	HP	OI69MK0624	N/A	416000-001
Power Input Module	HP AC Module, Single Phase	HP	N/A	N/A	413494-001

Onboard Administrator FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	Spare Part Number	Firmware Version	Hardware Version
1	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB21BP0852	456204-B21	503826-001	3.60	B1
2	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB21BP0946	456204-B21	503826-001	3.60	B1

Blade FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	System Board Spare Part Number
1	ProLiant BL460c G1	HP	3UV839N08G	459483R-B21	438249-001
5	ProLiant BL685c G7	HP			000000-001
7	ProLiant BL460c G6	HP	MXQ923027D	507778-B21	531221-001
9	ProLiant BL460c G1	HP	USE7507R6S	447707-B21	410299-001
10	ProLiant BL460c G1	HP	USM634043S	416654-B21	410299-001
15	ProLiant BL460c G6	HP	MXQ92707MZ	507783-B21	531221-001
16	ProLiant BL460c G1	HP	USE70638DJ	404667-B21	410299-001

Blade Mezzanine FRU Information

Bay	Mezz Slot	Model	Manufacturer	Serial Number	PCA Serial Number	Part Number	Spare Part Number
1	1	NC326m Dual Port 1Gb NIC for c-Class BladeSystem	HP	CN66MK1132	CN66MK1132	406771-B21	419330-001

Interconnect FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
1	HP VC Flex-10 Enet Module	HP	TW284700YT	455880-B21	456095-001
2	HP VC Flex-10 Enet Module	HP	TW28400004	455880-B21	456095-001
6	Brocade 4/24 SAN Switch for HP c-Class BladeSystem	BROCADE	CN8625701U	AE372A	411121-001

Fan FRU Information

Bay Number	Model	Part Number	Spare Part Number
1	Active Cool 200 Fan	412140-B21	413996-001
2	Active Cool 200 Fan	412140-B21	413996-001
4	Active Cool 200 Fan	412140-B21	413996-001
5	Active Cool 200 Fan	412140-B21	413996-001
6	Active Cool 200 Fan	412140-B21	413996-001
7	Active Cool 200 Fan	412140-B21	413996-001
9	Active Cool 200 Fan	412140-B21	413996-001
10	Active Cool 200 Fan	412140-B21	413996-001

Power Supply FRU Information

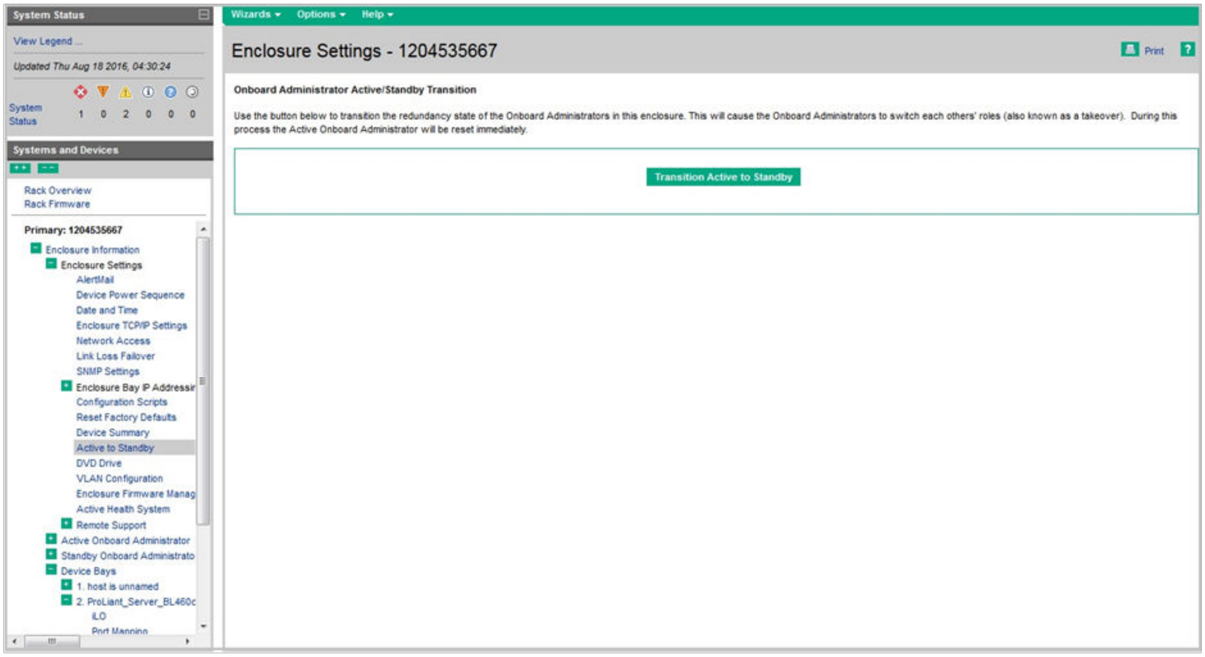
Bay Number	Model	Part Number	Serial Number	Spare Part Number
1	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLU20FR	411099-001
2	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLV74LW	411099-001
3	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLTT4G3	411099-001
4	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLVR0AB	411099-001
5	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLUG0AD	411099-001
6	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLTT34Q	411099-001

Insight Display FRU Information

Model	Spare Part Number	Manufacturer	Firmware Version
BladeSystem c7000 LCD	415839-001	HP	2.2.2

Active to Standby

When a second Onboard Administrator is installed, the menu item **Active to Standby** appears under the **Enclosure Settings** tree menu item, and both Onboard Administrators are visible in the tree menu and in the enclosure view under the Status tab.



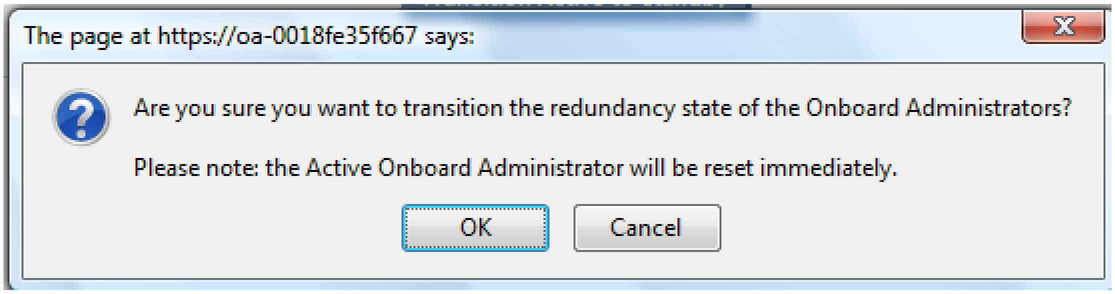
Enclosure Settings - 1204535667

Onboard Administrator Active/Standby Transition

Use the button below to transition the redundancy state of the Onboard Administrators in this enclosure. This will cause the Onboard Administrators to switch each others' roles (also known as a takeover). During this process the Active Onboard Administrator will be reset immediately.

If more than one Onboard Administrator is installed in the enclosure, you can manually change which Onboard Administrator is active. This feature can be useful when troubleshooting the Onboard Administrator or if a second Onboard Administrator is installed with an older firmware version (and automatic transition is disabled).

To perform a transition, click **Transition Active to Standby** to force the change. A confirmation screen appears, confirming the transition and advising you to close your browser if you are signed into the Active Onboard Administrator. To proceed, click **OK**. To exit without a change, click **Cancel**.



The page at https://oa-0018fe35f667 says:

Are you sure you want to transition the redundancy state of the Onboard Administrators?

Please note: the Active Onboard Administrator will be reset immediately.

You can also perform a transition using the `FORCE TAKEOVER` command from the Onboard Administrator CLI.

The transition times from Standby to Active and Active to Standby vary, depending on the configuration, enclosure population, and various other factors. Removing the previously Active Onboard Administrator early in the transition process forces the transition time of the Standby to Active to increase.

DVD drive

This screen enables you to connect multiple server blades in the enclosure to the shared DVD resource, launch the iLO Remote Console, and use virtual power commands on the selected server blades. Information on this page is current as of the last download. To view updated information, click **Refresh**.

NOTE:

The c-Class BladeSystem ProLiant and Integrity iLO virtual media performance will be limited based on the activity and number of simultaneous iLO virtual media sessions and the Onboard Administrator workload. The Enclosure DVD and Enclosure Firmware Management features also use the iLO virtual media feature and will have similar performance limitations. To prevent media timeout issues, Hewlett Packard Enterprise recommends that you limit the number of simultaneous sessions. If timeout issues are experienced during OS install or firmware updates, reduce the number of virtual media sessions in progress, and restart the operation.

Column	Description or action
Check box	To apply the Virtual Power, One Time Boot, or DVD features, select the bays.
Bay	This field displays the device bay number of the blade within the enclosure.
Power State	The power state of the server blade. Possible values are On or Off.
Remote Console	To launch the iLO Remote Console, select **Integrated Remote Console (IE)** or **Remote Console Applet (Java)**, and then click **Launch**.
iLO DVD Status	This field indicates whether the server blade has a Virtual Media connection. Possible values are Connected, Disconnected, or Unknown. A status of Incompatible Firmware indicates that the DVD feature is not supported with the iLO firmware installed on the device. A status of Unknown indicates an iLO connectivity issue exists.
Device or Image URL	This field displays the current Virtual Media connection of the blade. Possible values are: • Standby OA DVD • Enclosure Firmware Management • Virtual Media Applet is connected • Feature not supported on Integrity iLO version x.xx • SSH is disabled on this blade's iLO processor • Upgrade ProLiant iLO 2 version x.xx to 1.30 or higher • Enclosure DVD • Tray Open or No Media • iLO has no IP address

Virtual Power

The Virtual Power menu enables a Momentary Press or a Press and Hold of the power button, or a Cold Boot of the selected server blades.

Button	Description
Momentary Press	This button mimics a physical momentary press of the power button on the server blade. Clicking this button powers the server blade on or off gracefully.
Press and Hold	This button mimics a physical press and hold of the power button on the server blade. Clicking this button forces the server blade to shut power off without first shutting down the OS. This option is not available when the server blade is off.
Cold Boot	Clicking this button immediately removes power from the system. This command applies only to server blades that are powered on. Issuing a Cold Boot command to a powered off server blade acts to power on the server blade.

One Time Boot

Option	Description
Diskette Drive (A:)	Forces the server blade to reboot to the diskette drive. Be sure the diskette drive is attached to the server blade before selecting this option.
CD-ROM	Forces the server blade to reboot to the CD-ROM drive. Be sure the CD-ROM drive is attached to the server blade before selecting this option.
Hard Drive C:	Forces the server blade to reboot to the hard disk.
RBSU	Forces the server blade to boot to the ROM-Based Setup Utility.
PXE NIC	Forces the server blade to boot to PXE NIC.

DVD

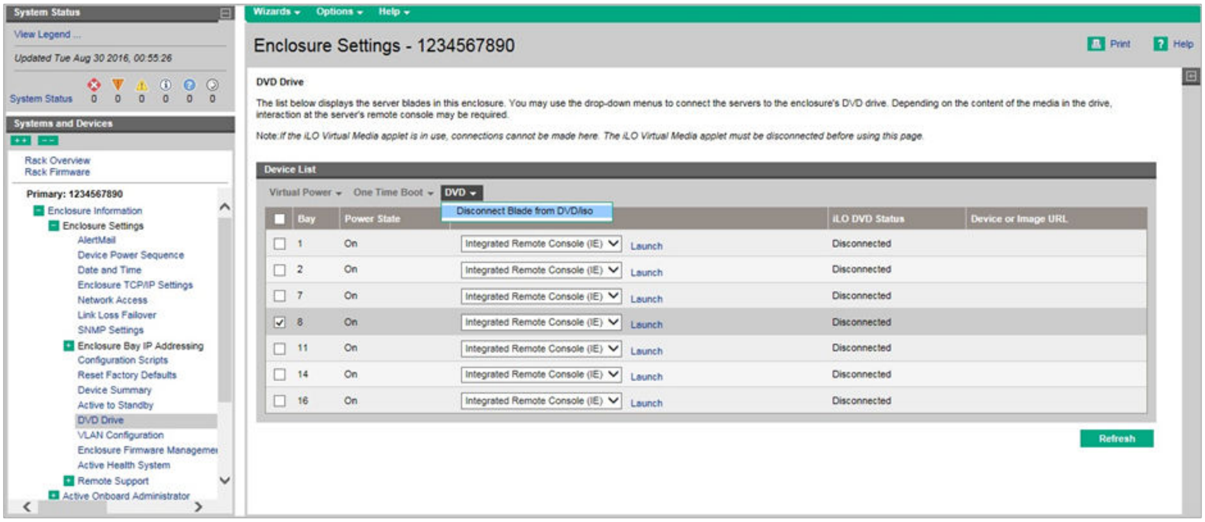
The DVD menu enables you to connect or disconnect the shared DVD drive by selecting Connect to Enclosure DVD or Disconnect DVD Hardware. You can connect the shared DVD drive to multiple server blades. After the shared DVD drive is connected, you can use the Virtual Power menu to reboot the server blades selected in the list. If multiple media disks are required for an installation, you might have to disconnect and reconnect for every server when the new media disk is inserted in the DVD.

When a USB key is detected in the Active Onboard Administrator USB port and ISO images are present, they appear on the DVD menu. Select the server blades to which you want to deploy an ISO image, and then select the ISO image from the menu. The ISO image deploys.

Interactive installation and configuration of DVD/CD-ROM drive

You can install and configure a blade operating system or software application interactively.

Blades can access media in the DVD drive first connecting the blade to the DVD drive and then by browsing to the DVD Drive or Device Bay Summary pages. To access media in the DVD drive, insert a disc into the drive, select the DVD menu, and then click **Connect to Enclosure DVD**.



Enclosure Settings - 1234567890

DVD Drive

The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.

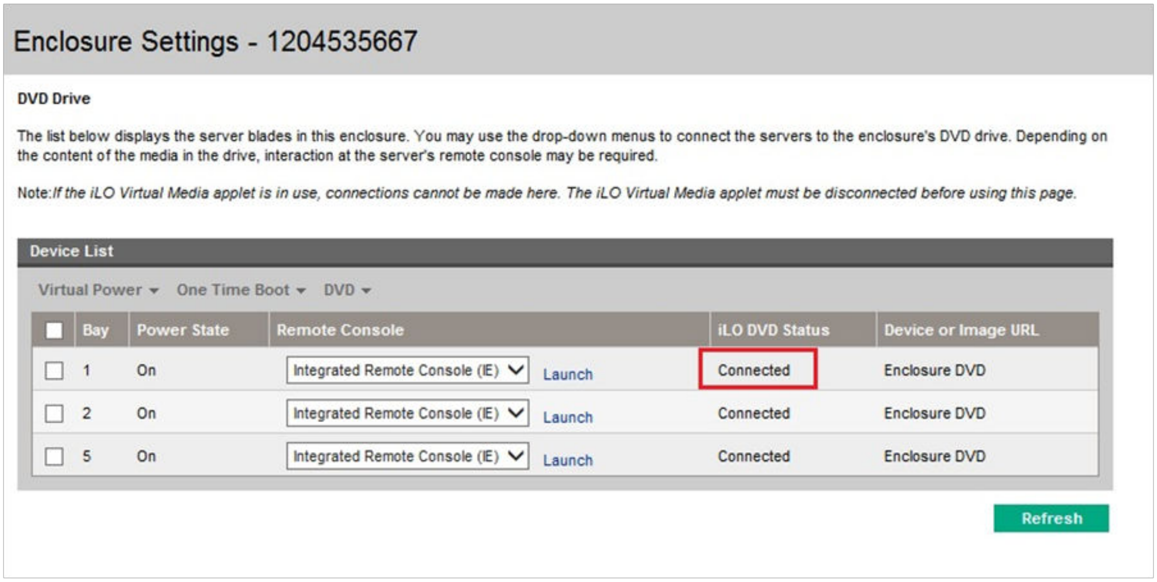
Note: *If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.*

Device List

□	Bay	Power State			iLO DVD Status	Device or Image URL
□	1	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	2	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	7	On	Integrated Remote Console (IE)	Launch	Disconnected	
☑	8	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	11	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	14	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	16	On	Integrated Remote Console (IE)	Launch	Disconnected	

After the disc is inserted into the DVD drive, you can power on or reboot the blade, using the corresponding menu items on the DVD Drive to Device List mapping page of Onboard Administrator. To start an iLO Remote Console session and view the selected blade console, click **Launch**. Performance might vary as the number of blades increases.

For more information about using the iLO Remote Console, see the iLO user guide.



Enclosure Settings - 1204535667

DVD Drive

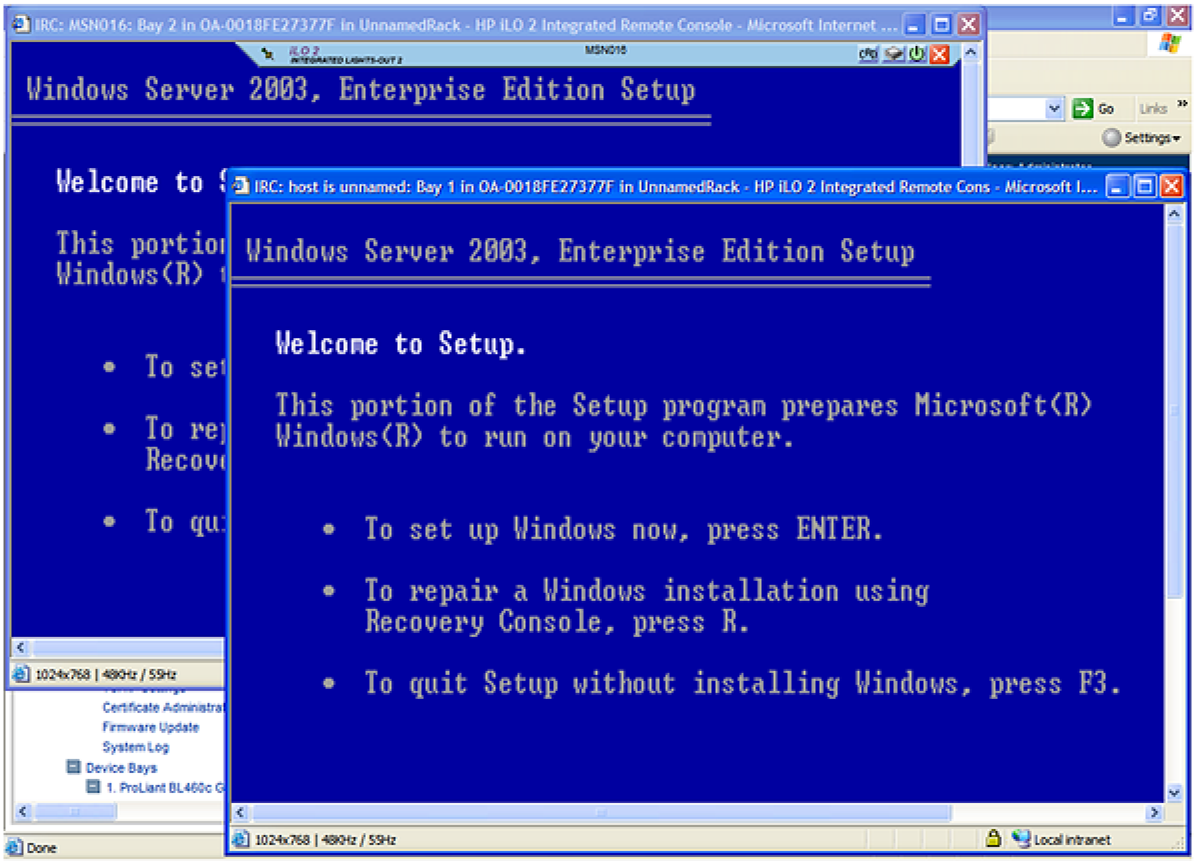
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.

Note:*If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.*

Device List

□	Bay	Power State	Remote Console		iLO DVD Status	Device or Image URL
□	1	On	Integrated Remote Console (IE)	Launch	Connected	Enclosure DVD
□	2	On	Integrated Remote Console (IE)	Launch	Connected	Enclosure DVD
□	5	On	Integrated Remote Console (IE)	Launch	Connected	Enclosure DVD

If a Windows installation CD is in the DVD Drive, the user can use the Integrated Remote Console display as shown in the following figure.

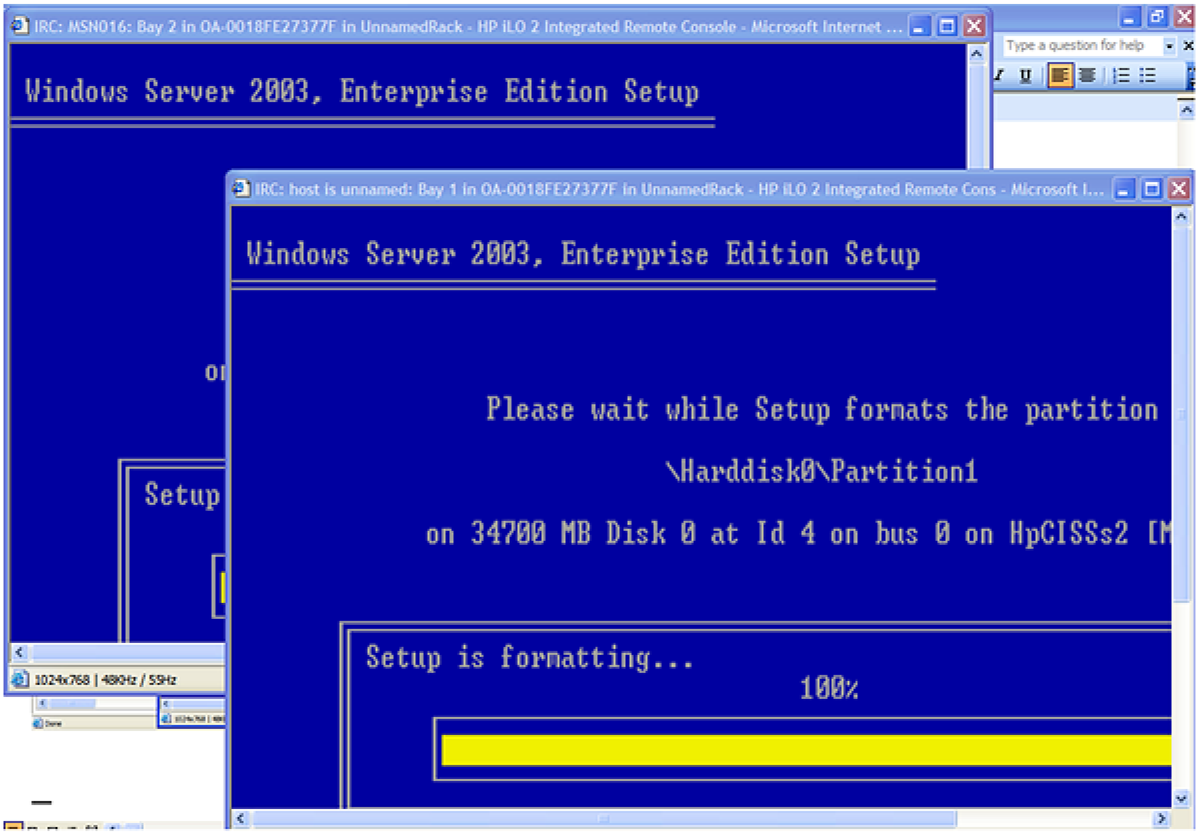


IRC: MSN016: Bay 2 in OA-0018FE27377F in UnnamedRack - HP iLO 2 Integrated Remote Console - Microsoft Internet ...

IRC: host is unnamed: Bay 1 in OA-0018FE27377F in UnnamedRack - HP iLO 2 Integrated Remote Cons - Microsoft I...

```
Windows Server 2003, Enterprise Edition Setup

  Welcome to Setup.

  This portion of the Setup program prepares Microsoft(R)
  Windows(R) to run on your computer.

     •  To set up Windows now, press ENTER.

     •  To repair a Windows installation using
        Recovery Console, press R.

     •  To quit Setup without installing Windows, press F3.
```

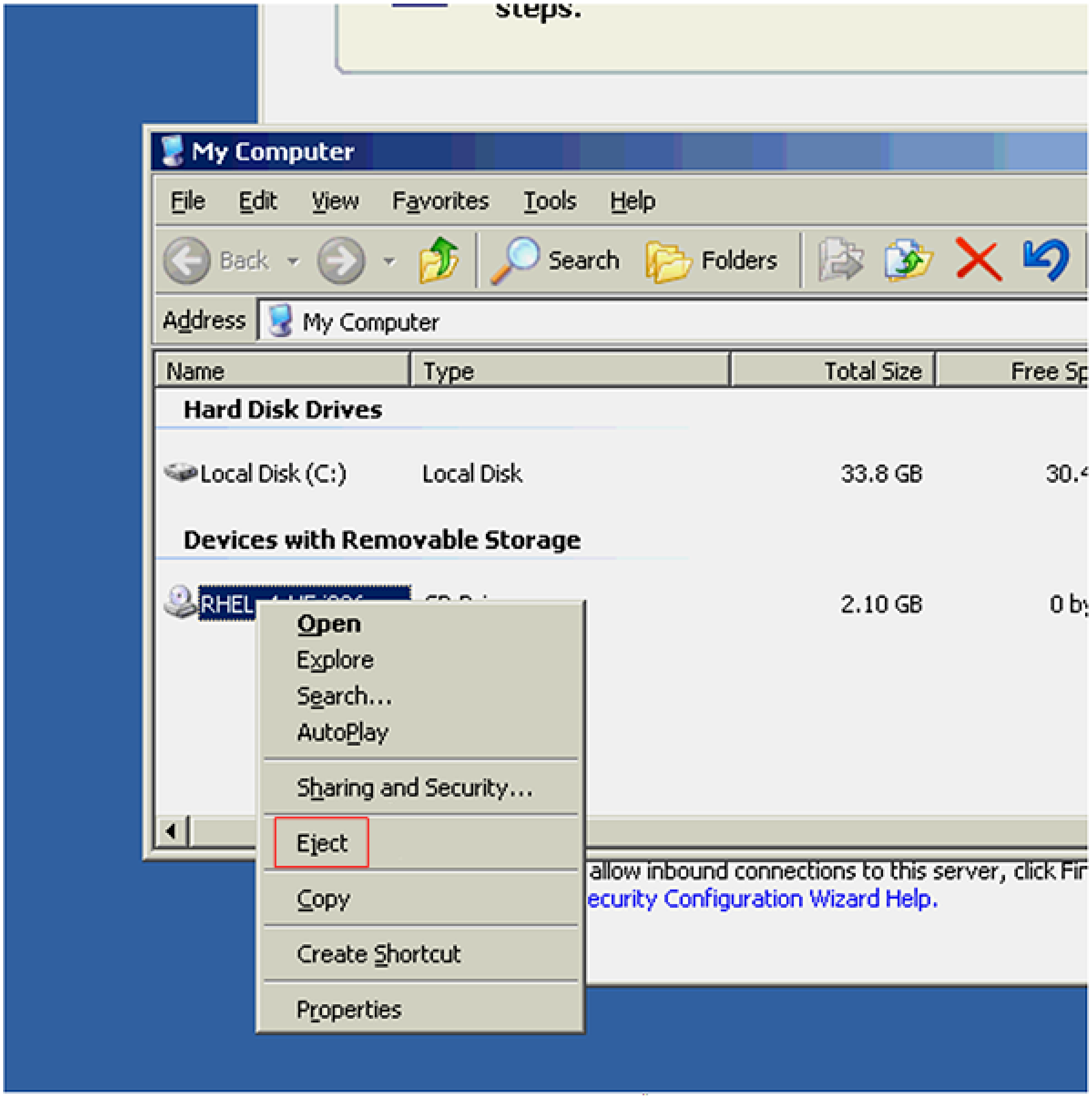
Windows Server 2003 installs on the blade.


IRC: MSN016: Bay 2 in OA-0018FE27377F in UnnamedRack - HP iLO 2 Integrated Remote Console - Microsoft Internet ...
Type a question for help
1024x768 | 480Hz / 55Hz
IRC: host is unnamed: Bay 1 in OA-0018FE27377F in UnnamedRack - HP iLO 2 Integrated Remote Cons - Microsoft I...

```
Windows Server 2003, Enterprise Edition Setup

Setup

Windows Server 2003, Enterprise Edition Setup

      Please wait while Setup formats the partition

               \Harddisk0\Partition1

   on 34700 MB Disk 0 at Id 4 on bus 0 on HpCISSs2 [M

  Setup is formatting...
                          100%
```

If required, eject the disc from the DVD drive, and then insert the next installation disc. If the DVD drive is not busy (for at least 16 seconds), click the **DVD Drive Tray Open** button. The enclosure DVD drive is neither accessible nor controllable from the IRC Virtual Media window.

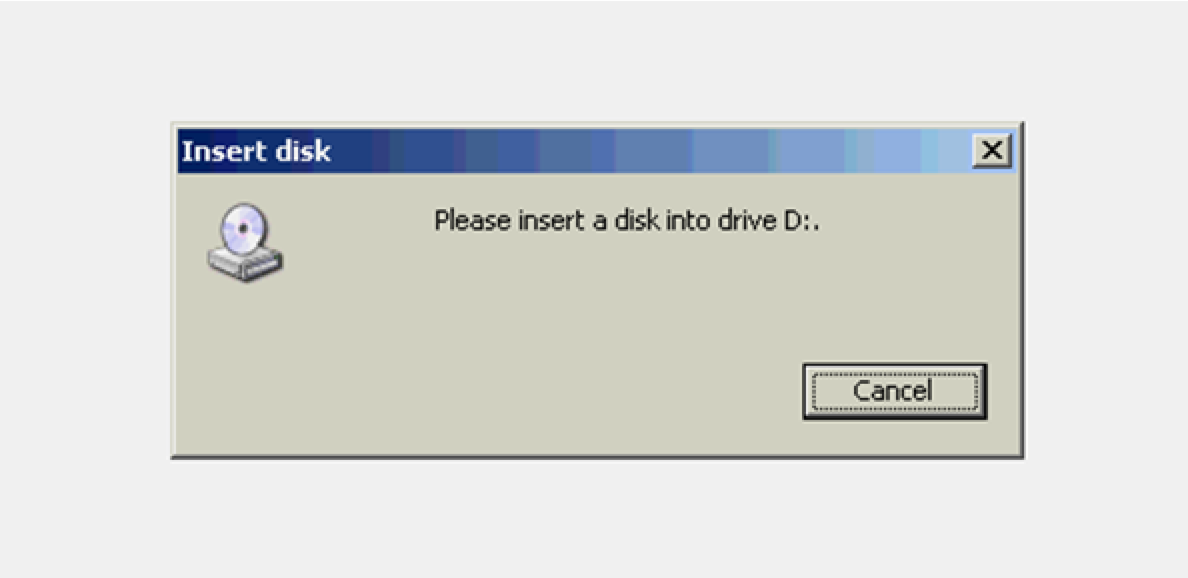
You can eject media from the DVD drive using the operating system Eject menu option on the blade connected to the drive.



Name	Type	Total Size	Free Sp
Hard Disk Drives			
Local Disk (C:)	Local Disk	33.8 GB	30.4
Devices with Removable Storage			
RHEL		2.10 GB	0 by

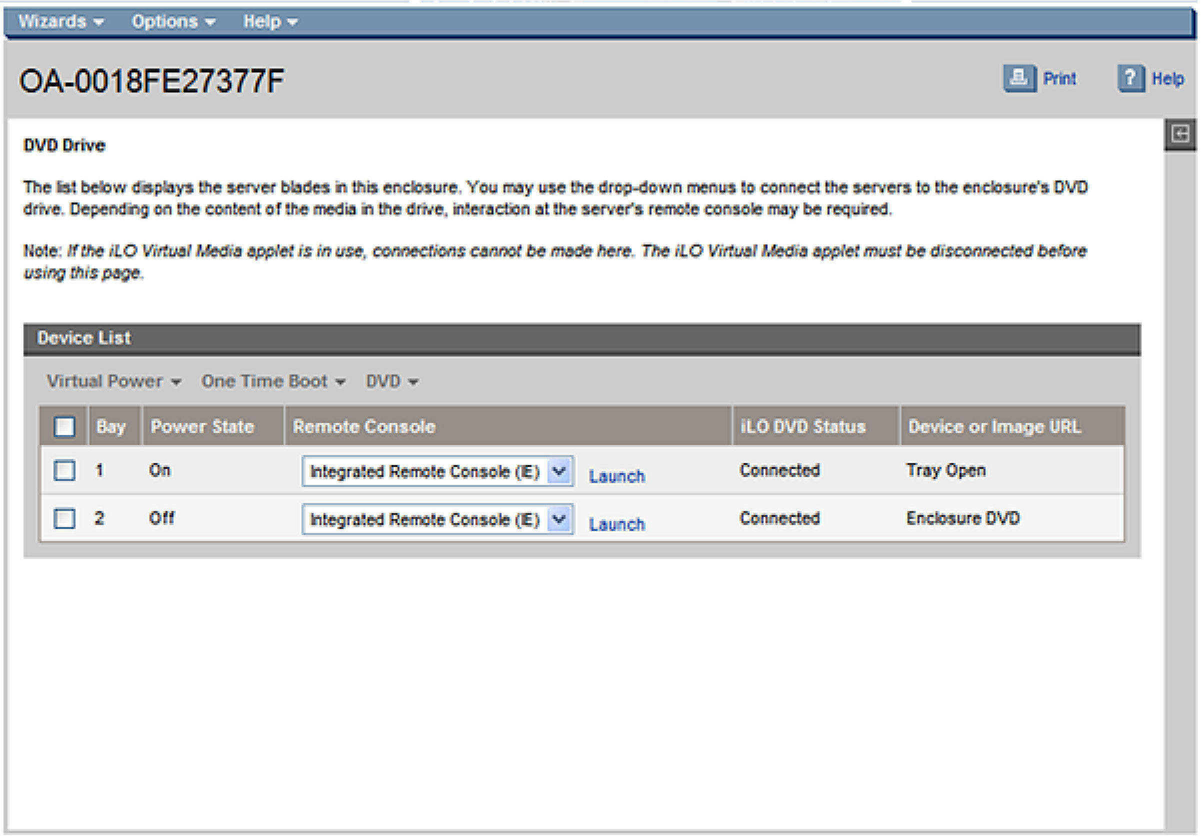
allow inbound connections to this server, click Fir
ecurity Configuration Wizard Help.

After the media is ejected from the DVD/CD-ROM drive, the operating system prompts you to insert a DVD or CD.



Please insert a disk into drive D:.

After issuing an eject command from the operating system, the blade Device or Image URL displays `Tray Open`. However, the physical drive does not open until you press the drive tray open button on the front of the DVD drive.



OA-0018FE27377F

DVD Drive

The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.

Note: *If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.*

Device List

□	Bay	Power State	Remote Console		iLO DVD Status	Device or Image URL
□	1	On	Integrated Remote Console (IE)	Launch	Connected	Tray Open
□	2	Off	Integrated Remote Console (IE)	Launch	Connected	Enclosure DVD

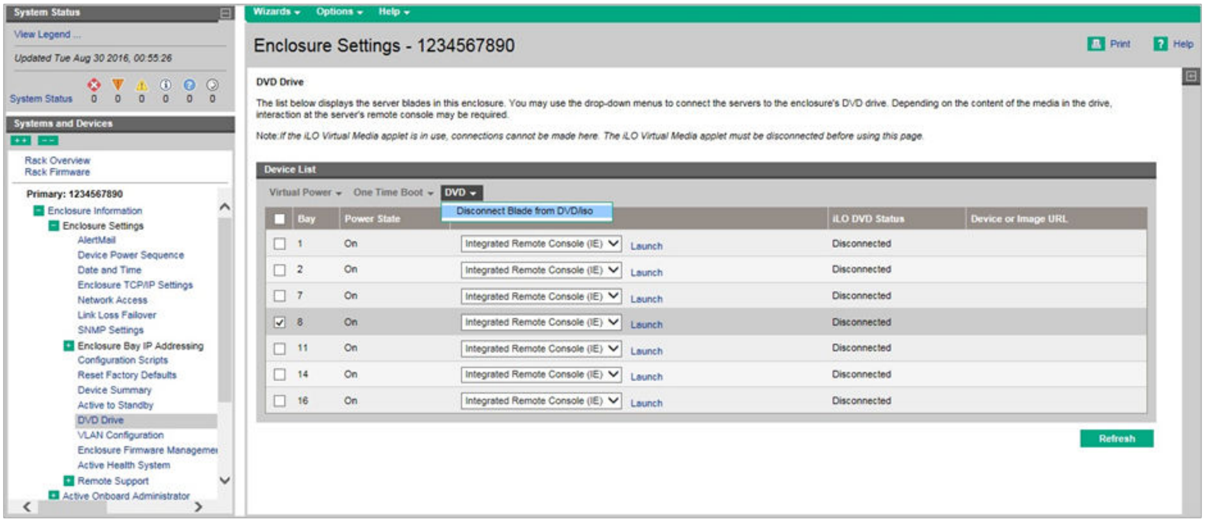
You can insert and eject media as needed per your operating system, application, and data requirements guidelines.

Unattended OS deployment

The Onboard Administrator can silently provision from one to eight blades by leveraging the shared DVD/CD-ROM drive. The build disc that is used in the DVD/CD-ROM drive must be capable of booting the blade, detecting blade hardware, creating local disk partitions, and deploying an operating system on the blade. This type of provisioning requires only one disc and does not require ejecting media. Subsequent applications can also be installed in the same manner, provided the application fits on a single disc.

To access media in a blade DVD drive:

1. Connect the blade to the drive by browsing to the DVD/CD-ROM drive page.
2. Browse to then Device List Mapping page.
3. Select the DVD menu, and then select **Connect to Enclosure DVD**.
4. Insert the media into the DVD/CD-ROM drive before connecting to it.



Enclosure Settings - 1234567890

DVD Drive

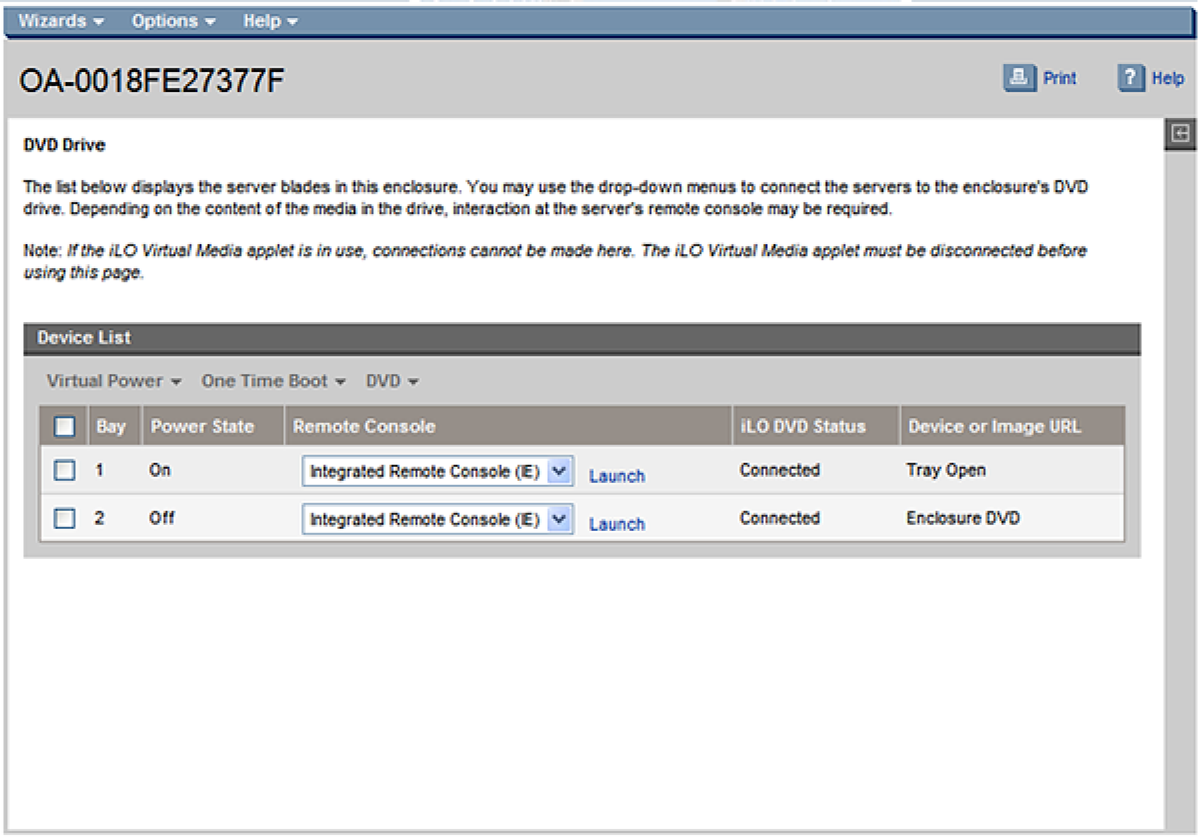
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.

Note: *If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.*

Device List

■	Bay	Power State			iLO DVD Status	Device or Image URL
□	1	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	2	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	7	On	Integrated Remote Console (IE)	Launch	Disconnected	
☑	8	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	11	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	14	On	Integrated Remote Console (IE)	Launch	Disconnected	
□	16	On	Integrated Remote Console (IE)	Launch	Disconnected	

After the media is inserted in the DVD drive, you can power on or reboot the blade using the corresponding menu items on the DVD Drive to Device List mapping page.



OA-0018FE27377F

DVD Drive

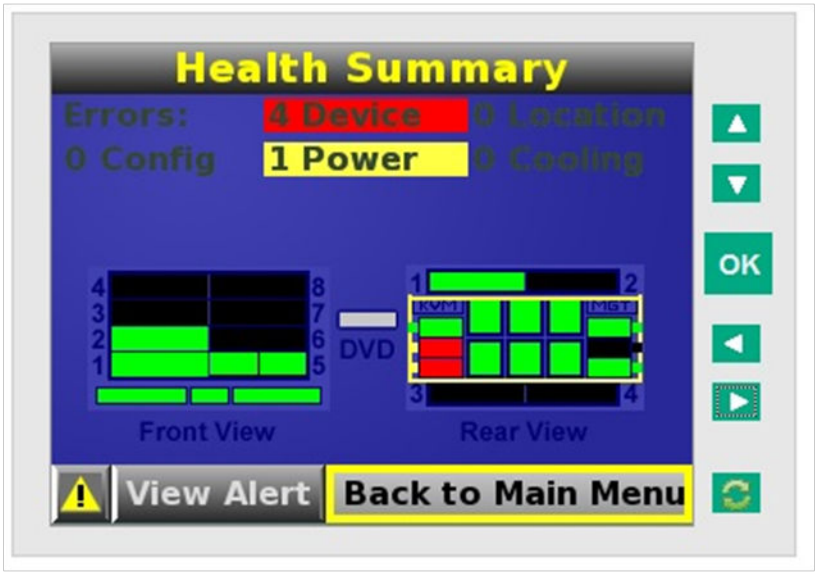
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.

Note: *If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.*

Device List

□	Bay	Power State	Remote Console		iLO DVD Status	Device or Image URL
□	1	On	Integrated Remote Console (IE)	Launch	Connected	Tray Open
□	2	Off	Integrated Remote Console (IE)	Launch	Connected	Enclosure DVD

You can initiate an unattended operating system deployment on the Insight Display. To begin the installation process, connect the DVD/CD-ROM drive, and then reboot the server. Insert the DVD or CD into the DVD/CD-ROM drive. The Insight Display Health Summary displays a status of green, indicating that media is inserted in the drive. You can only connect blades to the DVD drive after media is inserted. Performance might vary as the number of blades is increased.

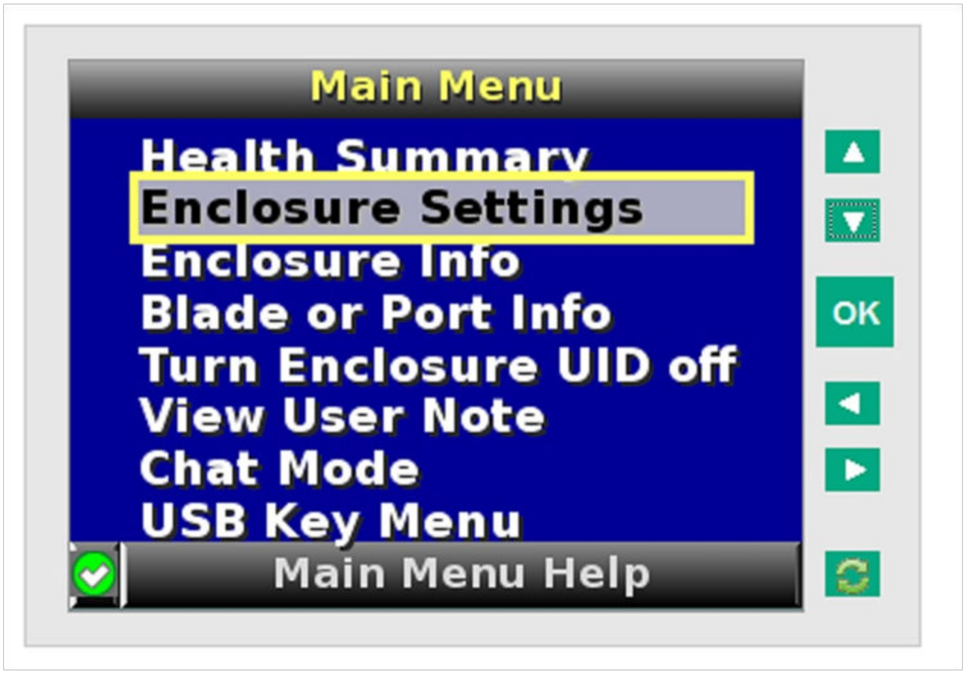


The Insight Display displays the DVD/CD-ROM drive status on the Health Summary screen as a DVD icon with one of the following colors:

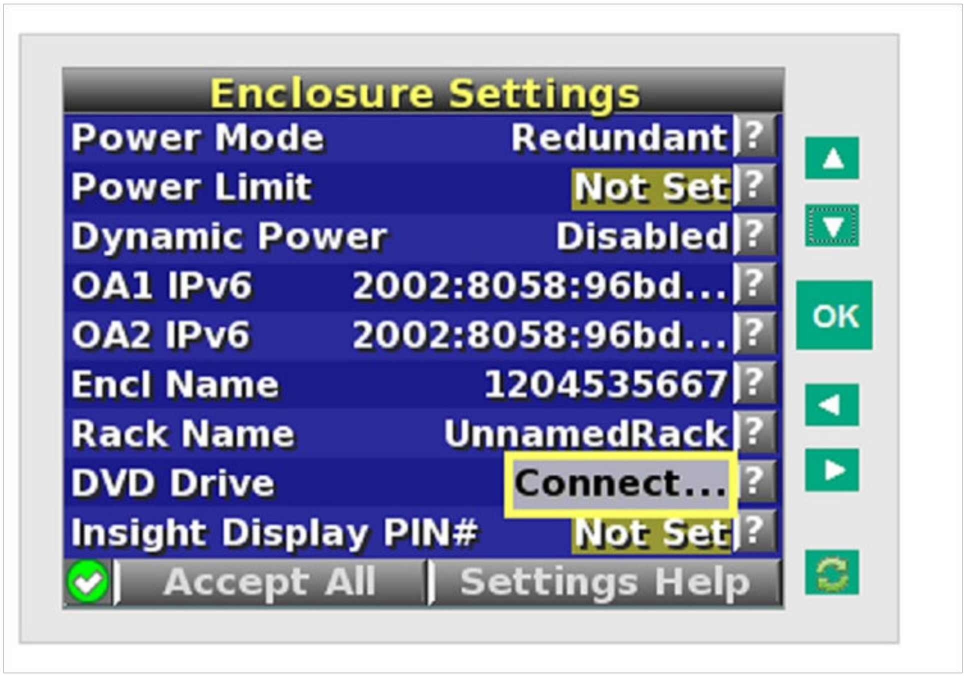
- Black—No drive present
- Light gray—Drive present, but no media present
- Dark green—Disconnected media present
- Light green—Connected media present

The Insight Display Main Menu enables you to connect blades to the DVD/CD-ROM drive and then reboot the blades.

From the Main Menu, select **Enclosure Settings**.



From the DVD Drive Enclosure Settings screen, select **Connect…**.



Enclosure Settings

Power Mode Redundant

Power Limit Not Set

Dynamic Power Disabled

OA1 IPv6 2002:8058:96bd...

OA2 IPv6 2002:8058:96bd...

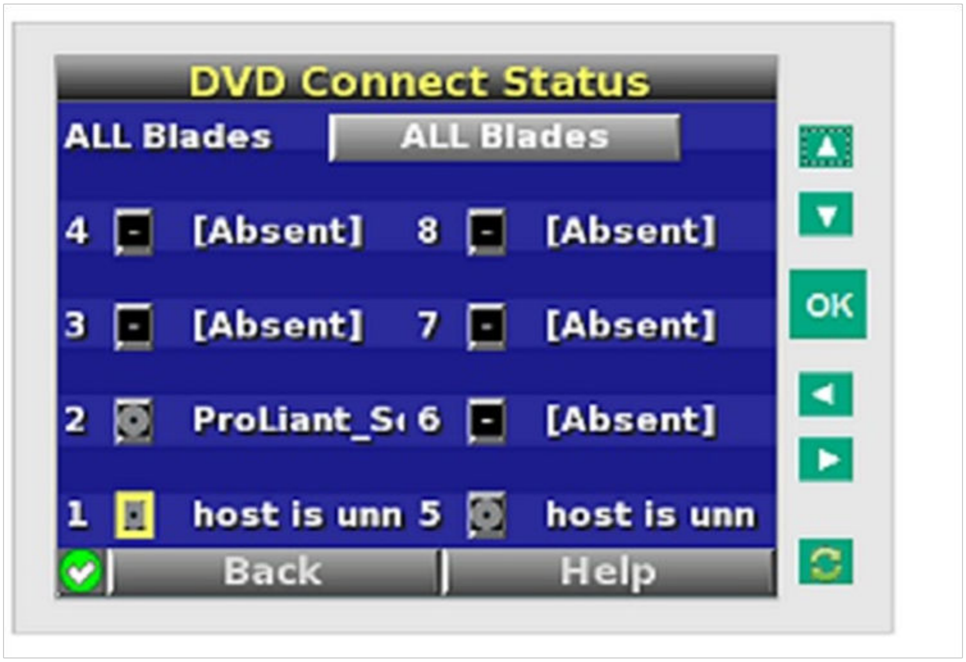
Encl Name 1204535667

Rack Name UnnamedRack

DVD Drive Connect...

Insight Display PIN# Not Set

From the DVD Connection Status screen, select **All Blades**.

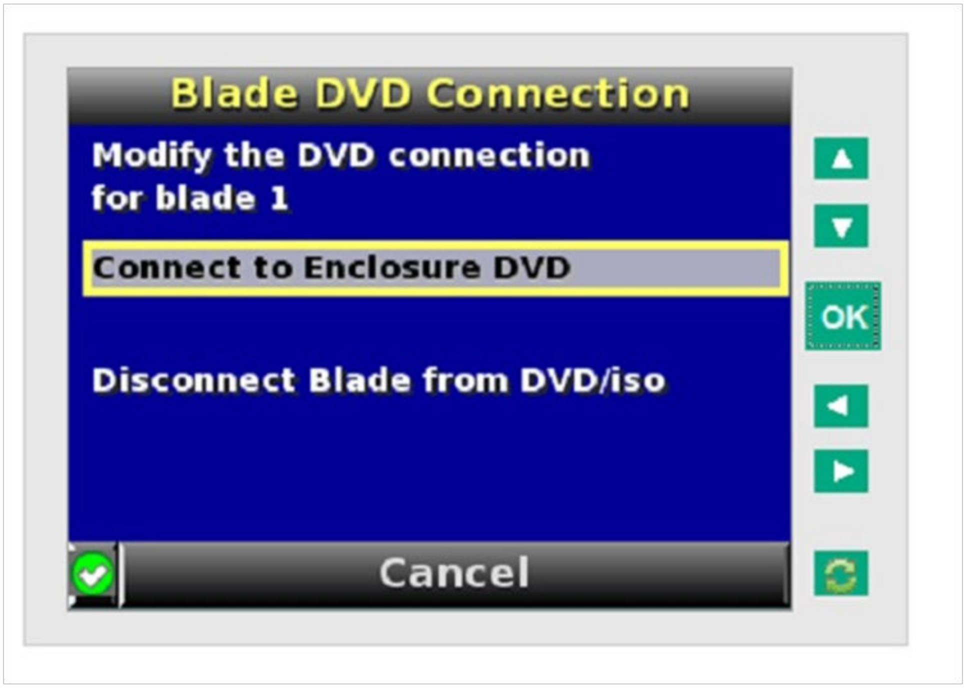


DVD Connect Status

ALL Blades ALL Blades

4	▪	[Absent]	8	▪	[Absent]
3	▪	[Absent]	7	▪	[Absent]
2	●	ProLiant_S	6	▪	[Absent]
1	▪	host is unn	5	●	host is unn

Select **Connect to Enclosure DVD** from the Blade DVD Connection screen.



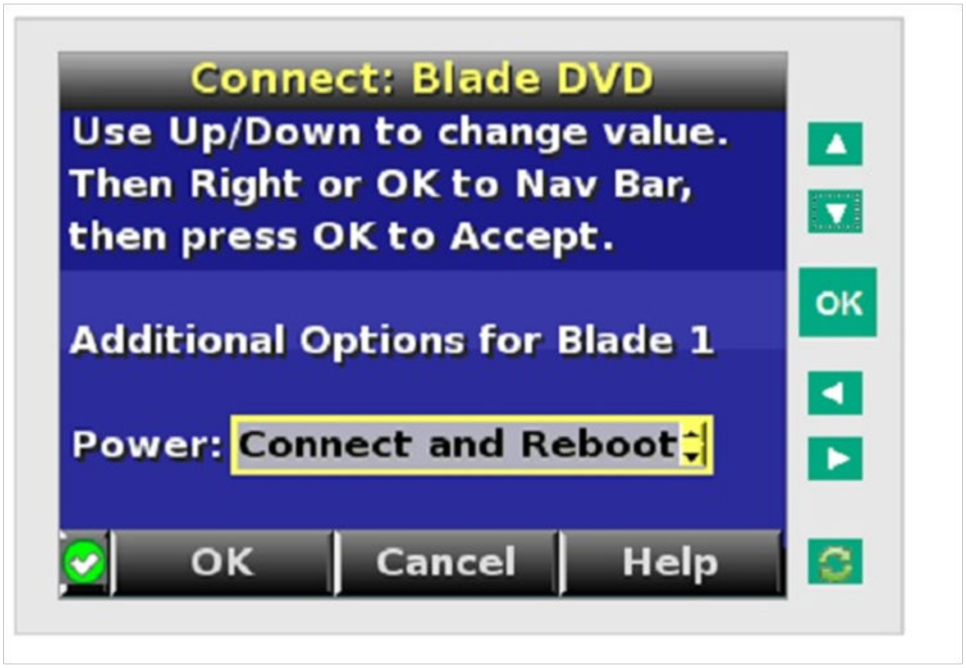
Blade DVD Connection

Modify the DVD connection
for blade 1

Connect to Enclosure DVD

Disconnect Blade from DVD/iso

From the Connect: Blade DVD screen, select **Connect and Reboot**.



Connect: Blade DVD

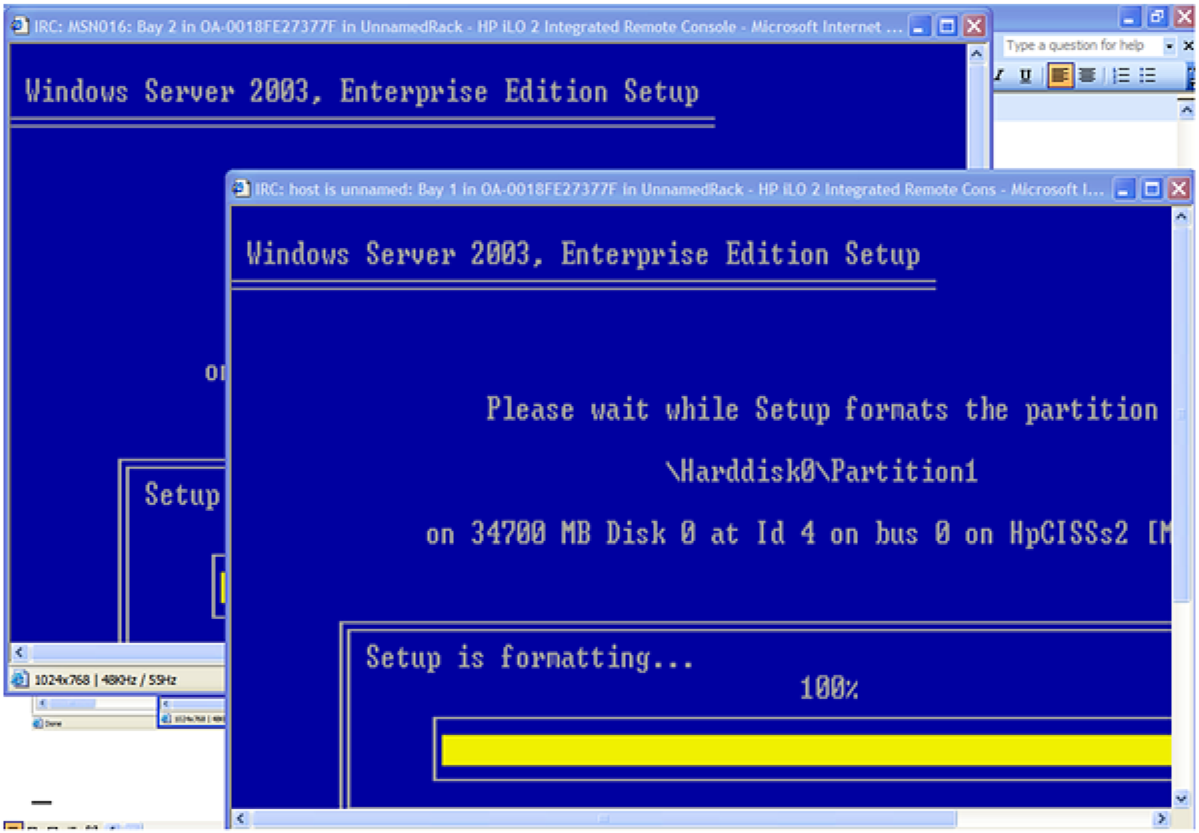
Use Up/Down to change value. Then Right or OK to Nav Bar, then press OK to Accept.

Additional Options for Blade 1

Power: Connect and Reboot

All blades reboot with the DVD/CD-ROM drive connected. If the media in the DVD/CD-ROM drive is bootable, the blades boot from this media. If a partition exists, the server might attempt to boot from the local hard drive. If the blades are older or have been erased, then delete and re-create all local drive partitions.

To view the progress of the unattended installation, use the Integrated Console.



IRC: MSN016: Bay 2 in OA-0018FE27377F in UnnamedRack - HP iLO 2 Integrated Remote Console - Microsoft Internet ...

Windows Server 2003, Enterprise Edition Setup

IRC: host is unnamed: Bay 1 in OA-0018FE27377F in UnnamedRack - HP iLO 2 Integrated Remote Cons - Microsoft I...

Windows Server 2003, Enterprise Edition Setup

Please wait while Setup formats the partition

\Harddisk0\Partition1

on 34700 MB Disk 0 at Id 4 on bus 0 on HpCISSs2 [M

Setup is formatting...

100%

Ad-hoc access to DVD-based media for application installation or data import

Use the enclosure-based DVD/CD-ROM drive to insert CDs or DVDs to perform tasks such as installing an application or loading data from a CD. These tasks can be performed on an as-needed basis. Its primary function is for when the DVD Drive is not used as a boot device.

Updating blade firmware with the HP Smart Update Manager

Use the BladeSystem Enclosure DVD drive and the Firmware Maintenance media to update ROMs on all server blades. Create the Firmware Maintenance DVD media to build a bootable DVD. Insert the DVD in the shared DVD drive, connect all server blades to the drive, and then reboot. The Firmware Maintenance DVD runs on all server blades connected to the DVD drive.

For more information about the HP Smart Update Manager, see the HP Smart Update Manager User Guide. For more information about updating firmware on server blades, see the HPE BladeSystem ProLiant Firmware Management Best Practices document.

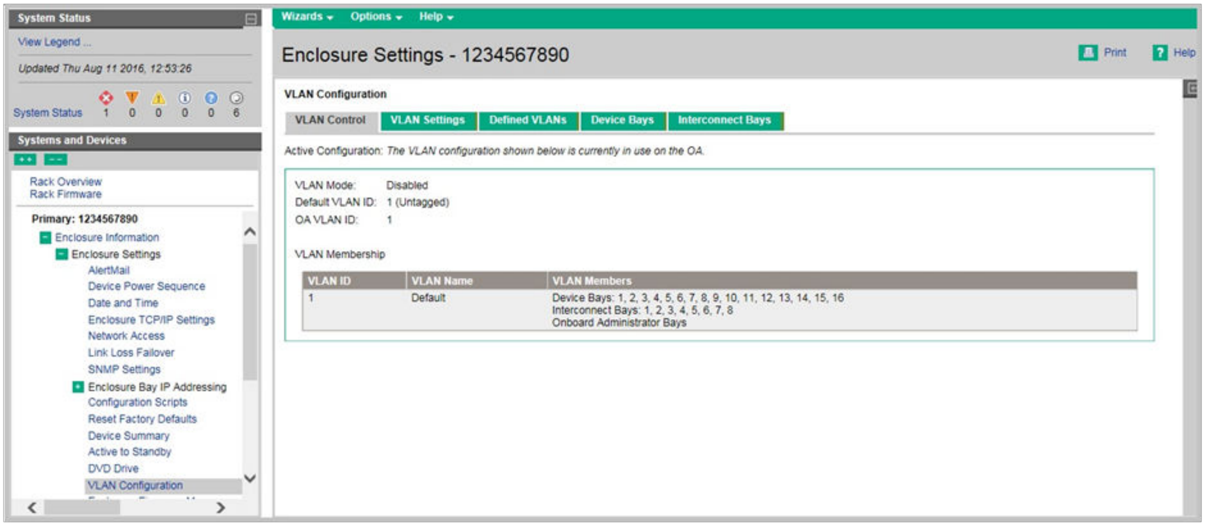
VLAN Configuration

Onboard Administrator 3.00 and higher provides a user-configurable IEEE 802.1Q tagged VLAN. This feature enables you to completely isolate traffic from the server or the interconnect module by creating a VLAN on the enclosure management network.

VLAN places no requirements or restrictions on the IP address. However, the external router or switch, which the Onboard Administrator is connected to, must be configured for VLAN trunk mode to route and pass Ethernet frames with VLAN tags for multiple VLANs through the Onboard Administrator's external Ethernet interface.

Hewlett Packard Enterprise recommends using a console terminal to configure your network to prevent loss of communication when changing the VLAN configuration. The corresponding changes should then also be made to the external switch that Onboard Administrator is connected to.

The VLAN Control tab displays the active configuration that is currently in use on the Onboard Administrator.



Enclosure Settings - 1234567890

VLAN Configuration

Active Configuration: *The VLAN configuration shown below is currently in use on the OA.*

VLAN Mode: Disabled
Default VLAN ID: 1 (Untagged)
OA VLAN ID: 1

VLAN Membership

VLAN ID	VLAN Name	VLAN Members
1	Default	Device Bays: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 Interconnect Bays: 1, 2, 3, 4, 5, 6, 7, 8 Onboard Administrator Bays

VLAN features

- The VLAN ID is a unique number, which identifies each VLAN. The allowable range of VLAN ID numbers is 1 to 4094. By default, VLAN is disabled, and all devices are set to VLAN ID 1. After a VLAN is configured, devices that do not have the same VLAN ID cannot communicate with each other.
- All untagged frames received by Onboard Administrator are assigned to the default VLAN ID. Onboard Administrator responds with untagged frames. All tagged frames have a VLAN ID or tag in the frame, and Onboard Administrator responds with tagged frames.

- If a tagged frame is sent using the default VLAN ID, it is dropped by Onboard Administrator because Onboard Administrator expects default VLAN ID frames to be untagged. If the destination is the server or interconnect, then the Onboard Administrator responds with untagged frames.
- Traffic between the iLO/IOM and the Broadcom switch is untagged, making VLAN transparent to them. Incoming traffic destined to the device is tagged by Onboard Administrator going into the Broadcom switch which then removes the tag before sending the traffic to the device. The Broadcom switch adds the default VLAN ID to the port the device is attached to the outgoing traffic of the device before sending it out.
- The VLAN ID of the server, interconnect module, and Onboard Administrator is configurable to allow Onboard Administrator to be part of any network by configuring the VLAN ID to match the default VLAN setting of the external switch that the Onboard Administrator is connected to.
- The Onboard Administrator firmware assigns the default VLAN ID to all non-configured bays. The default VLAN ID can be changed by the user. You can associate a name, limited to 31 alphanumeric characters, to a VLAN ID. You can save up to 25 VLAN entries with a VLAN ID and name at one time.
- VLAN supports SAS interconnect peer-to-peer communication. There is also full interface support for CLI and GUI along with limited support for LCD. You can enable and disable VLAN and view or change VLAN IDs though the Insight Display. There is no VLAN support on the enclosure link and service port.
- Both active and standby Onboard Administrator are set to the same VLAN configuration settings, causing any changes to the active Onboard Administrator to be made to the standby Onboard Administrator as well. No changes can be made to the standby Onboard Administrator, but you can view the settings.
- You can configure or change VLAN settings with VLAN disabled. Run-time user changes are saved in RAM only and are lost when Onboard Administrator is restarted. Use the `Save Config` command to save configuration changes permanently.
- You can configure VLAN remotely. VLAN configuration changes are saved in RAM only, and these changes are discarded upon reboot unless you save the changes to FLASH.
- Devices on different VLAN domain networks cannot communicate. All servers and interconnects, regardless of their VLAN ID, can still be managed using the Onboard Administrator. The client machine and the Onboard Administrator must be on the same VLAN ID to access the Onboard Administrator.

VLAN settings

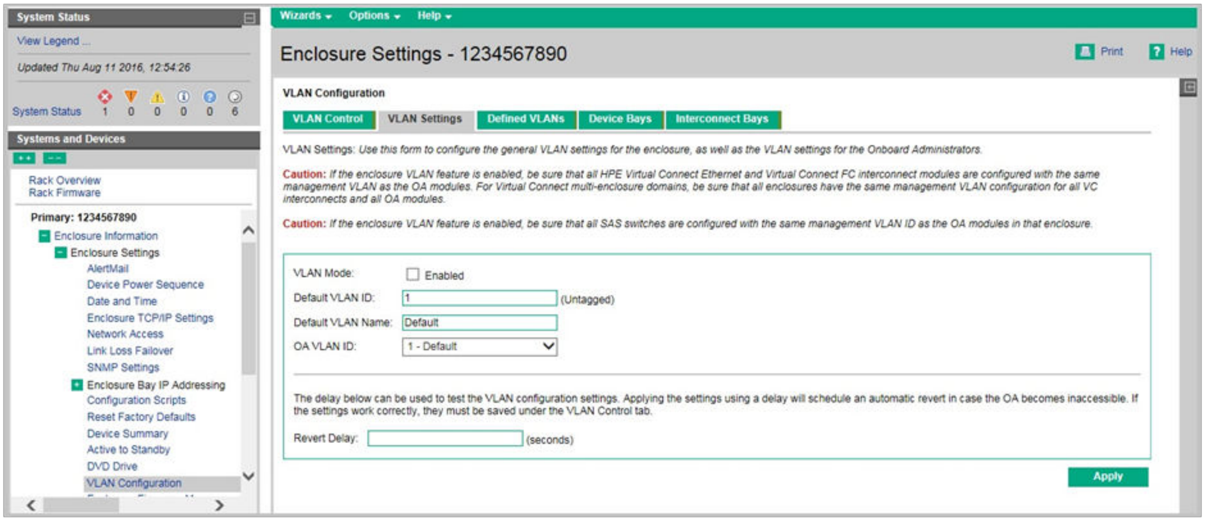
The general VLAN settings and the VLAN settings for the Onboard Administrator are configured from the VLAN Settings tab. Settings for the Device and Interconnect bays are configured from the Device Bays and Interconnect Bays tabs. After changes are made on any of these three tabs, the VLAN Control tab displays. After the VLAN Control tab displays, you can save the settings or revert to the previous settings.

The revert delay on the VLAN Settings tab is used to schedule a reversion of the settings to what has currently been saved on the Onboard Administrator. This can be used if you are administering the settings remotely and become disconnected. If you incorrectly configure the VLAN settings and become disconnected, the Onboard Administrator VLAN settings revert back to the previous state before you connected.

NOTE:

If the enclosure VLAN feature is enabled, be sure that all HPE Virtual Connect Ethernet and Virtual Connect FC interconnect modules are configured with the same management VLAN as the OA modules. For Virtual Connect multi-enclosure domains, be sure that all enclosures have the same management VLAN configuration for all VC interconnects and all OA modules.

Additionally, be sure that all HPE SAS switches are configured with the same management VLAN ID as the OA modules in that enclosure.



Updated Thu Aug 11 2016, 12:54:26

Enclosure Settings - 1234567890

VLAN Configuration

VLAN Settings: *Use this form to configure the general VLAN settings for the enclosure, as well as the VLAN settings for the Onboard Administrators.*

Caution: *If the enclosure VLAN feature is enabled, be sure that all HPE Virtual Connect Ethernet and Virtual Connect FC interconnect modules are configured with the same management VLAN as the OA modules. For Virtual Connect multi-enclosure domains, be sure that all enclosures have the same management VLAN configuration for all VC interconnects and all OA modules.*

Caution: *If the enclosure VLAN feature is enabled, be sure that all SAS switches are configured with the same management VLAN ID as the OA modules in that enclosure.*

VLAN Mode: □ Enabled

Default VLAN ID: 1 (Untagged)

Default VLAN Name: Default

OA VLAN ID: 1 - Default

The delay below can be used to test the VLAN configuration settings. Applying the settings using a delay will schedule an automatic revert in case the OA becomes inaccessible. If the settings work correctly, they must be saved under the VLAN Control tab.

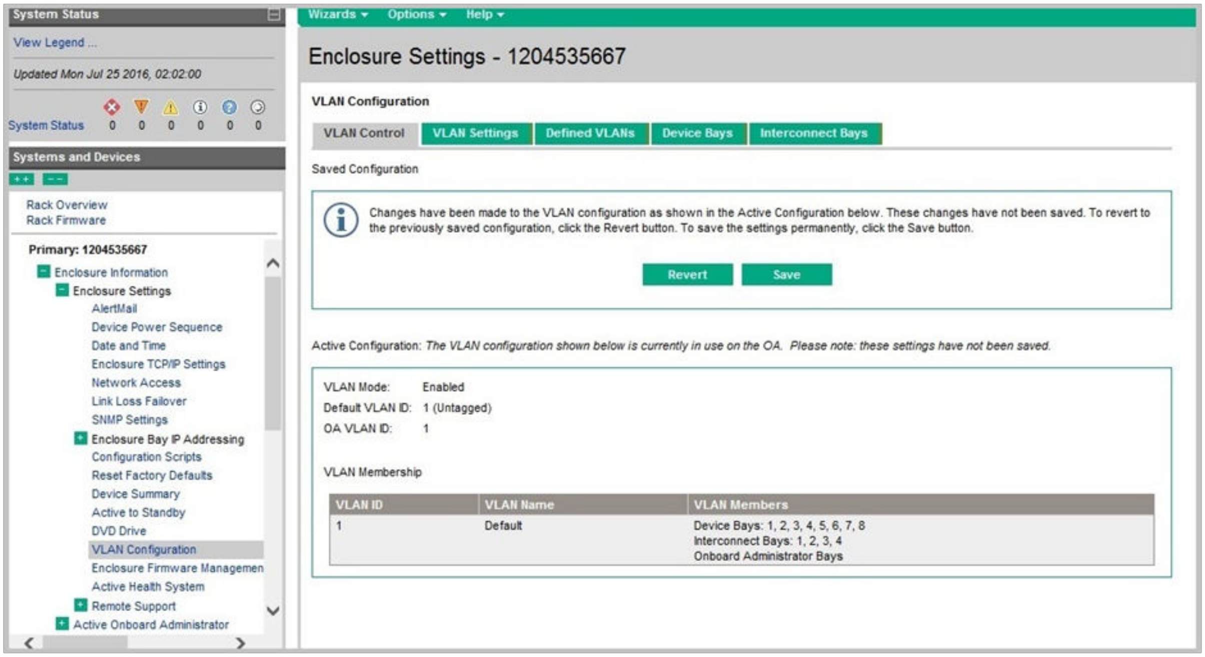
Revert Delay: (seconds)

VLAN Mode—The default setting for VLAN is disabled. To enable VLAN settings, select this check box.

Setting	Description
Default VLAN ID	The current Default VLAN ID number. The possible values for the VLAN ID are 1 to 4094.
Default VLAN Name	The current Default VLAN ID name. This field is optional and limited to a maximum of 31 characters, including alphanumeric characters, dashes (-), underscores (_), and spaces.
OA VLAN ID	The current OA VLAN ID. To change the membership of the Onboard Administrator, select a defined VLAN from the menu. The membership change will apply to the Active and the Standby Onboard Administrator.
Revert Delay	This setting enables you to automatically revert back to the currently saved VLAN configuration if you become disconnected after making the VLAN configuration changes.

To save changes to the VLAN configuration temporarily, click **Apply**.

The VLAN Control tab displays so you can choose to permanently save the configuration changes or revert back to the previously saved configuration.



Enclosure Settings - 1204535667

VLAN Configuration

Saved Configuration

Changes have been made to the VLAN configuration as shown in the Active Configuration below. These changes have not been saved. To revert to the previously saved configuration, click the Revert button. To save the settings permanently, click the Save button.

Active Configuration: *The VLAN configuration shown below is currently in use on the OA. Please note: these settings have not been saved.*

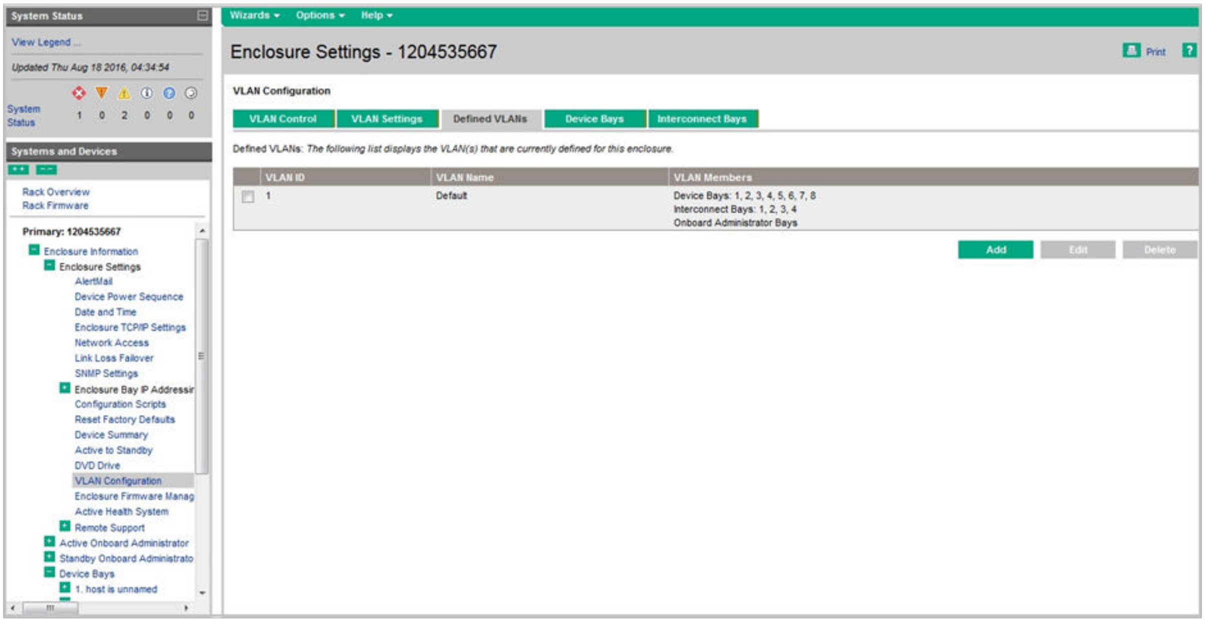
VLAN Mode: Enabled
Default VLAN ID: 1 (Untagged)
OA VLAN ID: 1

VLAN Membership

VLAN ID	VLAN Name	VLAN Members
1	Default	Device Bays: 1, 2, 3, 4, 5, 6, 7, 8 Interconnect Bays: 1, 2, 3, 4 Onboard Administrator Bays

Adding, editing, and removing VLANs

To add a new VLAN, click the **Defined VLANs** tab, and then click **Add**.



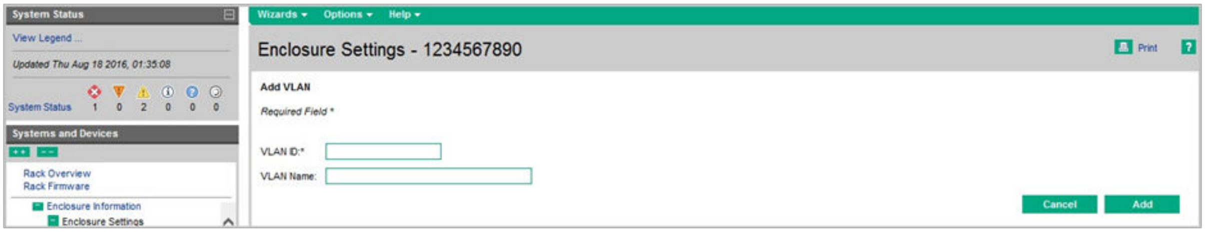
Enclosure Settings - 1204535667

VLAN Configuration

Defined VLANs: *The following list displays the VLAN(s) that are currently defined for this enclosure.*

	VLAN ID	VLAN Name	VLAN Members
□	1	Default	Device Bays: 1, 2, 3, 4, 5, 6, 7, 8 Interconnect Bays: 1, 2, 3, 4 Onboard Administrator Bays

The Add VLAN page displays with two fields: **VLAN ID** and **VLAN Name**. The **VLAN Name** field is optional, and the **VLAN ID** must be an integer between 1 and 4094. If you try to add a new VLAN where either the name or ID matches that of an existing VLAN, an error message appears.



Enclosure Settings - 1234567890

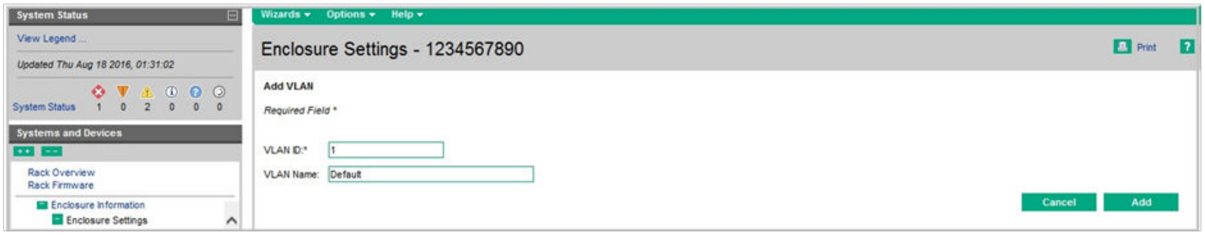
Add VLAN

*Required Field **

VLAN ID:*

VLAN Name:

An existing VLAN name can be edited by navigating to the **Defined VLANs** tab. Select one VLAN, and then click **Edit**. The Edit VLAN page appears with a field that enables you to edit the VLAN name. The VLAN name is not a required field.



Enclosure Settings - 1234567890

Add VLAN

*Required Field **

VLAN ID:* 1

VLAN Name: Default

Existing VLANs can be removed from the Defined VLANs page by selecting VLANs and then clicking **Delete.** Deleting a VLAN moves all of the members into the default VLAN. The default VLAN cannot be deleted.

NOTE:

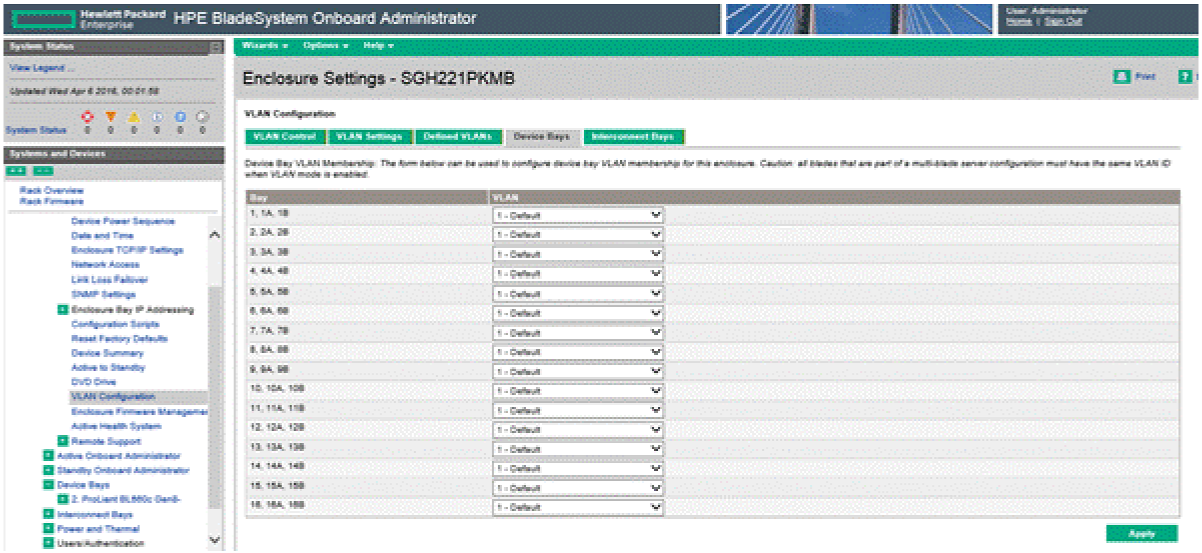
Accessing the Active OA through a link-local IPv6 address might not work on all client system setups containing multiple network interfaces.

Configuring devices

After VLANs are defined under the Defined VLANs tab, devices can be assigned to use them. The Onboard Administrator is assigned to a VLAN under the VLAN Settings tab. Device bays and Interconnect bays are assigned under the Device Bays tab and the Interconnect Bays tab.

Device bays

To change the membership of a device bay, select a defined VLAN from the menu under the VLAN column, and click **Apply**.



Enclosure Settings - SGH221PKMB

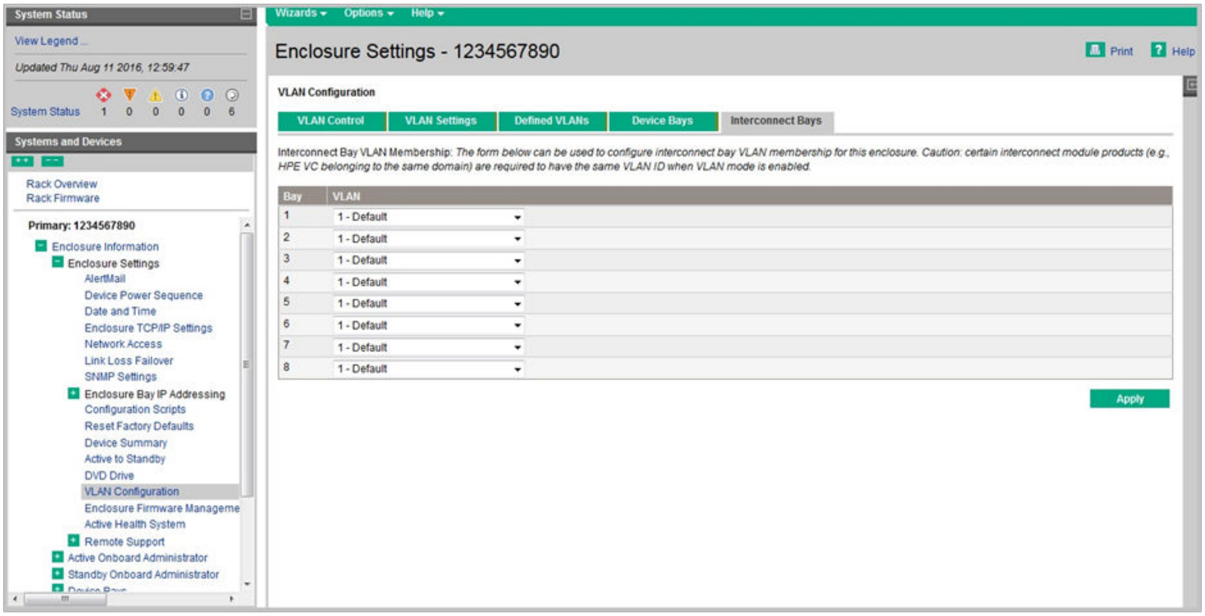
VLAN Configuration

Device Bay VLAN Membership: The form below can be used to configure device bay VLAN membership for this enclosure. Caution: all blades that are part of a multi-blade server configuration must have the same VLAN ID when VLAN mode is enabled.

Bay	VLAN
1, 1A, 1B	1 - Default
2, 2A, 2B	1 - Default
3, 3A, 3B	1 - Default
4, 4A, 4B	1 - Default
5, 5A, 5B	1 - Default
6, 6A, 6B	1 - Default
7, 7A, 7B	1 - Default
8, 8A, 8B	1 - Default
9, 9A, 9B	1 - Default
10, 10A, 10B	1 - Default
11, 11A, 11B	1 - Default
12, 12A, 12B	1 - Default
13, 13A, 13B	1 - Default
14, 14A, 14B	1 - Default
15, 15A, 15B	1 - Default
16, 16A, 16B	1 - Default

Interconnect bays

To change the membership of an interconnect bay, select a defined VLAN from the menu under the VLAN column, and click **Apply**.



Enclosure Settings - 1234567890

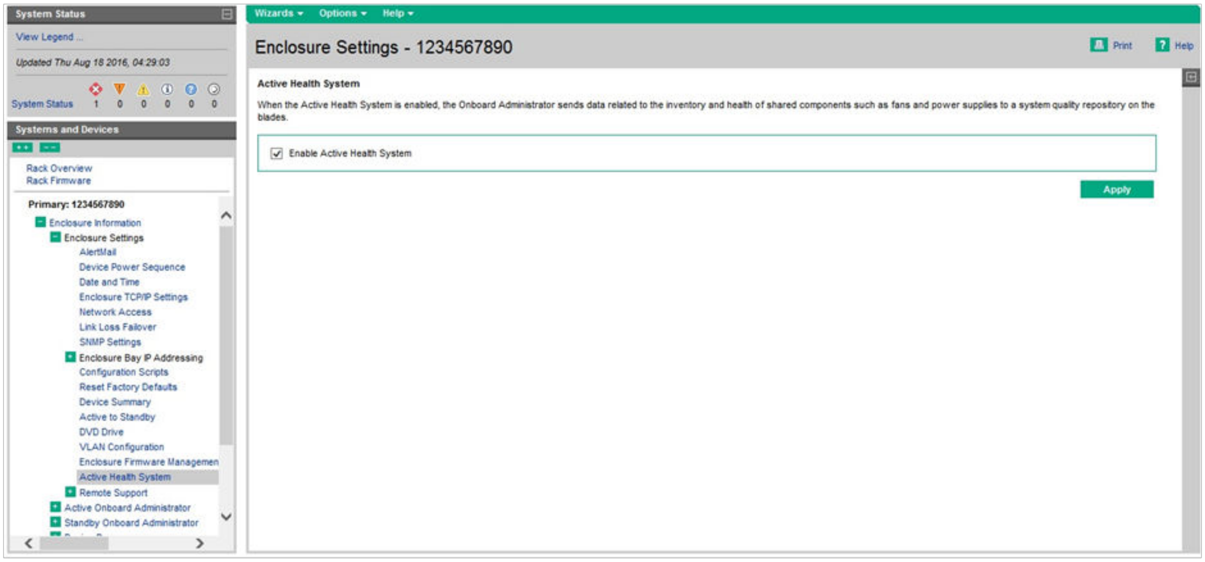
VLAN Configuration

Interconnect Bay VLAN Membership: *The form below can be used to configure interconnect bay VLAN membership for this enclosure. Caution: certain interconnect module products (e.g., HPE VC belonging to the same domain) are required to have the same VLAN ID when VLAN mode is enabled.*

Bay	VLAN
1	1 - Default
2	1 - Default
3	1 - Default
4	1 - Default
5	1 - Default
6	1 - Default
7	1 - Default
8	1 - Default

Active Health System

The HPE Active Health System monitors and records changes in the server hardware and system configuration. The Active Health System assists in diagnosing problems and delivering rapid resolution when system failures occur. In a BladeSystem Enclosure, the Onboard Administrator provides data related to shared infrastructure components and system settings to the Active Health System located on HPE ProLiant Server Blades. The Active Health System does not collect information about Active Health System user operations, finances, customers, employees, partners, or datacenter (for example, IP addresses, host names, user names, and passwords).



Enclosure Settings - 1234567890

Active Health System

When the Active Health System is enabled, the Onboard Administrator sends data related to the inventory and health of shared components such as fans and power supplies to a system quality repository on the blades.

☑ Enable Active Health System

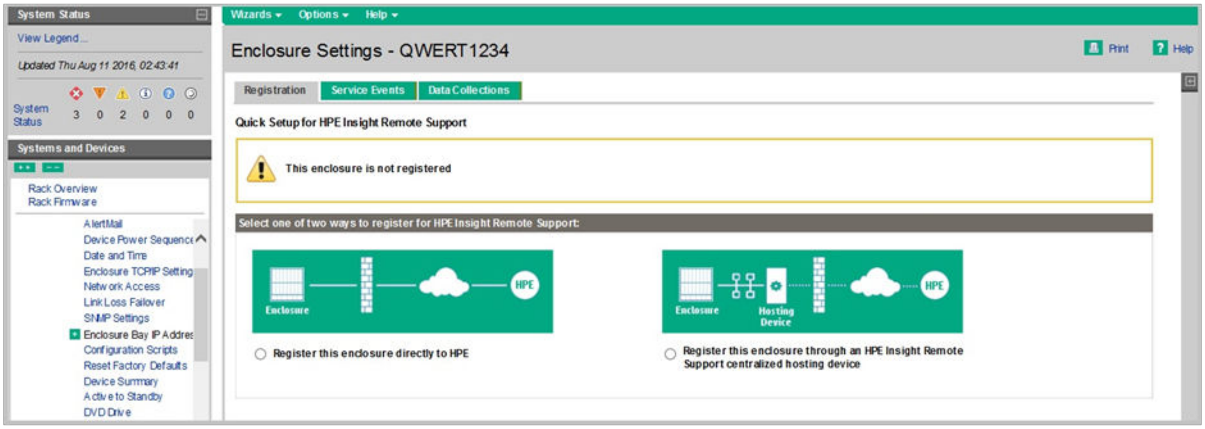
Examples of data collected by Onboard Administrator include inventory and status information for the following components and settings:

- Enclosure fans
- Enclosure power supplies
- Interconnect modules
- Enclosure midplane

- Onboard Administrators
- Enclosure power measurements

Insight Remote Support Registration

The following screen displays the Remote Support Registration tab, as seen with the enclosure not yet registered.



Enclosure Settings - QWERT1234

Quick Setup for HPE Insight Remote Support

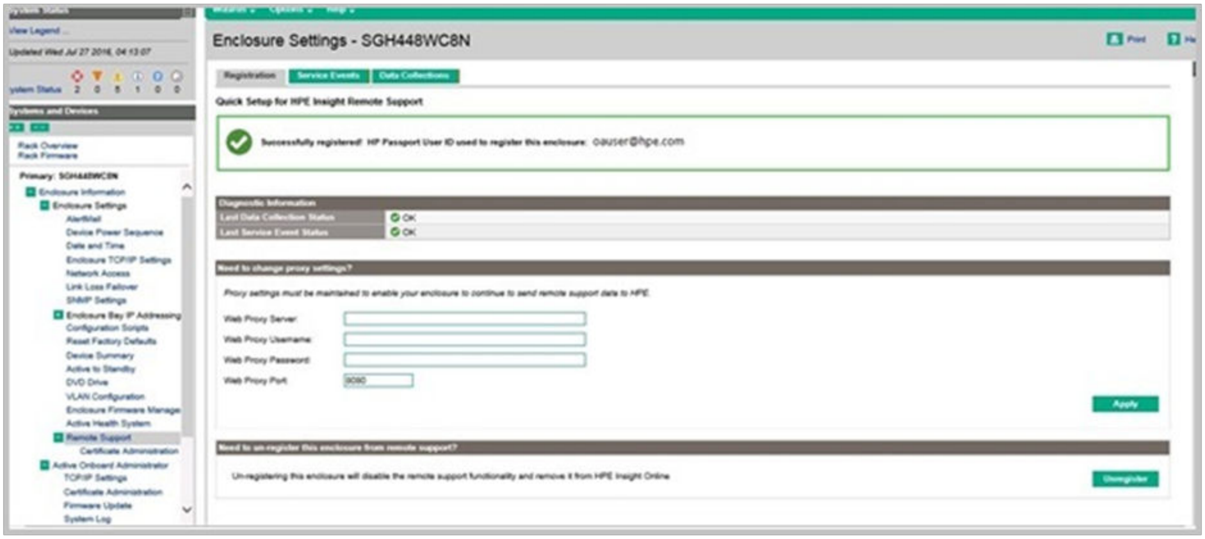
This enclosure is not registered

Select one of two ways to register for HPE Insight Remote Support:

○ Register this enclosure directly to HPE

○ Register this enclosure through an HPE Insight Remote Support centralized hosting device

The following screen displays the Remote Support Registration tab, as seen with the enclosure registered.



Enclosure Settings - SGH448WC8N

Quick Setup for HPE Insight Remote Support

Successfully registered! HP Passport User ID used to register this enclosure: oauser@hpe.com

Diagnostic Information	
Last Data Collection Status	OK
Last Service Event Status	OK

Need to change proxy settings?

Proxy settings must be maintained to enable your enclosure to continue to send remote support data to HPE.

Web Proxy Server:

Web Proxy Username:

Web Proxy Password:

Web Proxy Port: 8080

Need to un-register this enclosure from remote support?

Un-registering this enclosure will disable the remote support functionality and remove it from HPE Insight Online

Hewlett Packard Enterprise has developed a service and support experience that automates many day-to-day tasks and helps you reduce risk. Hewlett Packard Enterprise integrates an online, personalized dashboard (HPE Insight Online), a support portal and mobile application (Hewlett Packard Enterprise Support Center Mobile), and 24x7 remote support (HPE Insight Remote Support) for the consolidated infrastructure.

When you use the embedded Remote Support functionality with a BladeSystem c-Class enclosure, you can choose from the following configuration options:

- **Insight Online direct connect**

  Register an enclosure to communicate directly to Insight Online without the need to set up an Insight Remote Support centralized Hosting Device in your local environment. The Insight Online will be your primary interface for remote support information. The direct connect configuration is available in Onboard Administrator 4.11 and later.
- **Insight Remote Support central connect**

Register an enclosure to communicate to Hewlett Packard Enterprise through an Insight Remote Support centralized Hosting Device in your local environment. All configuration and service event information is routed through the Hosting Device. This information can be viewed by using the local Insight RS Console or the web-based view in Insight Online. The central connect configuration is available on Onboard Administrator 3.60 and later.

Data collected by Insight Remote Support

When the BladeSystem Enclosure is registered with Insight Remote Support, the following information about the BladeSystem Enclosure shared infrastructure components within the enclosure is sent to Hewlett Packard Enterprise:

- Registration

  As part of the enclosure registration process, for central connect, the Onboard Administrator sends to the Insight Remote Support hosting server the data that uniquely identifies the enclosure hardware. For direct connect, the Onboard Administrator sends that data directly to a web service in the Remote Support Data Center.

  Examples of data that is collected include:

  - Enclosure name
  - Enclosure product name
  - Enclosure part number
  - Enclosure serial number
  - Enclosure manufacturer name
  - Onboard Administrator firmware version
  - Onboard Administrator IP and MAC addresses
- Service events

  As part of the service event process, Onboard Administrator sends data to uniquely identify the relevant hardware component to the Insight Remote Support hosting device.

  Examples of data that is collected include:

  - Enclosure model
  - Enclosure serial number
  - Part number of the relevant hardware component
  - Description, location, and other identifying characteristics of the relevant hardware component

  For more information, see **Insight Remote Support Service Events**.
- Data collections

  As part of the data collection process, the Onboard Administrator sends data to Insight Remote Support to enable proactive advice and consulting. Information is sent for the enclosure hardware as well as populated system components including the LCD module, Onboard Administrator modules, enclosure fan modules, enclosure power supply modules, interconnect modules and server blades.

  Examples of data that is collected for these system components include:

  - Hardware module descriptors such as manufacturer, product name, serial number, UUID, part number, and location within the enclosure
  - Firmware revision
  - Diagnostic and status information
  - Power and thermal configuration and status information
  - Network and port mapping information

  For more information, see **Insight Remote Support Data Collections**.

Prerequisites for registering for Insight Remote Support

Before registering, verify that the following prerequisites are met:

- A supported version of the OA firmware is installed on all OA modules in the enclosure.
  - ◦ Version 3.60 or later is required for Insight Remote Support central connect registration.
  - ◦ Version 4.11 or later is required for Insight Online direct connect registration.

  You can download the latest firmware from the **Hewlett Packard Enterprise website**.
- For Insight Online direct connect only: A DNS server is configured in the Onboard Administrator . This is required for communication between iLO and Insight Online.
- For Insight Remote Support central connect only: Insight RS version 7.0.5 or later is installed and configured on the Insight RS hosting device.

NOTE:

A valid certificate is required if connecting to an Insight Remote Support Hosting Device and the Onboard Administrator is operating in FIPS Mode.

When the Onboard Administrator is operating in FIPS Mode ON, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. In FIPS Top-Secret Mode - certificates must have a minimum RSA key length of 3072 bits or ECDSA 384 bits, and the signature hash algorithm must be SHA-384.

Registering for Insight Remote Support using the OA web interface

The Insight Remote Support provides automatic submission of hardware events to Hewlett Packard Enterprise to prevent downtime and enable faster issue resolution. You can register directly to Hewlett Packard Enterprise or through an Insight RS Hosting Device.

Registering for Insight Remote Support using direct connect

To register a BladeSystem c-Class enclosure for Insight Online direct connect, use the following procedure. When you register for Insight Online direct connect, you must complete steps in both the OA interface and the Insight Online portal.

Procedure

1. Verify that the system meets the prerequisites for using the Insight Remote Support solution.

   For more information, see Prerequisites for registering for Insight Remote Support.
2. Navigate to the **Remote Support** page.

   Select **Enclosure Information** > **Enclosure Settings** > **Remote Support**.
3. Under the **Registration** tab, select **Register this enclosure directly to HP**.

   The page updates to show the direct connect registration options.
4. Enter your HP Passport credentials in the **HP Passport User ID** and **HP Passport Password** boxes.

   IMPORTANT:

   Enter your HP Passport User ID in the **HP Passport User ID** box. In most cases, your HP Passport User ID is the email address you used during the HP Passport registration process. If you changed your User ID in Hewlett Packard Enterprise Support Center, ensure that you enter your User ID and not your email address.
5. (Optional) If your BladeSystem c-Class enclosure uses a web proxy server to access the Internet, enter the following information:

- **Web Proxy Server**
- **Web Proxy Username**
- **Web Proxy Password**
- **Web Proxy Port**

6. Select the **I accept the terms and conditions of the HP Software License Agreement and the HP Insight Management Additional License Authorization** check box.

   These documents can be viewed at the **Hewlett Packard Enterprise Software License Documents website**.

7. Click **Register**.

   Clicking **Register** is Step 1 of a two-step registration process. Step 2 is completed in Insight Online.

   By registering, you agree to send registration, service events, and configuration data to Hewlett Packard Enterprise. All data collected and sent to Hewlett Packard Enterprise will be managed according to the Hewlett Packard Enterprise Data Privacy Policy. You can view the Data Privacy Policy at the **Hewlett Packard Enterprise website**.

   When Step 1 of the registration process begins, the following message appears:

   ```
   Step 1 of registration in progress, please wait...
   ```

   When Step 1 is finished, the following message appears:

   ```
   Step 1 of remote support registration has been completed. Please proceed to
   step 2 to complete the registration process.
   ```

   Allow up to 5 minutes for your registration request to be fully processed.

8. Navigate to the **Insight Online website**, and then log in with your HP Passport account credentials.

9. Follow the onscreen instructions in Insight Online, and provide your site, contact, and partner information so Hewlett Packard Enterprise can deliver service for your enclosure.

   For detailed instructions, see the Insight Remote Support and Insight Online Setup Guide for HPE ProLiant Servers and BladeSystem c-Class Enclosures.

10. Return to the **Remote Support** page in the OA web interface, and select the **Please confirm that you have completed the registration process in HP Insight Online** check box, and then click **Apply.**

    The following message appears:

    ```
    Are you sure you have completed registration in HP Insight Online? Click OK
    to confirm or Cancel to cancel.
    ```

11. Click **OK**.

    A message similar to the following appears:

    ```
    Successfully registered!
    ```

    ```
    HP Passport User ID used to register this enclosure: <HP passport User ID>.
    ```

12. (Optional) Send a test event to confirm the connection between OA and Insight Remote Support.

    a. Go to **Enclosure Settings** > **Remote Support**.

    b. Click the **Service Events** tab.

    c. Click **Send Test Event**.

13. (Optional) To receive email alerts about system events, configure AlertMail on the **Enclosure Information** > **Enclosure Settings** > **AlertMail** page.

Unregistering from Insight Online direct connect

Use the following procedure to unregister a BladeSystem c-Class enclosure from Insight Online direct connect.

Procedure

1. Go to **Enclosure Information** > **Enclosure Settings** > **Remote Support**.
2. Click **Unregister**.

   The following message appears:

   ```
   Are you sure you want to un-register and disable HP Insight Remote Support?
   ```
3. Click **OK**.

   The following message appears:

   ```
   Un-registration in progress. Please wait…
   ```

   When the un-registration is finished, the Remote Support page displays the following message:

   ```
   The enclosure is not registered.
   ```

Connection error during OA direct connect registration

Symptom

The following error occurs when attempting to register a BladeSystem c-Class enclosure for Insight Online direct connect:

```
Failed to resolve HP Insight Remote Support direct connect web service. Please
verify DNS settings, proxy settings and connectivity.
```

Action

- Verify that the DNS settings are configured correctly in OA. You can use the OA web interface or CLI to perform this task.
  - Log in to the OA web interface and navigate to **Active Onboard Administrator TCP/IP Settings screen**. Verify that the DNS configuration is correct. To edit the configuration, click the **Click here to modify the TCP/IP** settings link at the bottom of the screen.
  - Log in to the OA CLI interface and run the `SHOW NETWORK` command. Verify that the DNS configuration is correct. To edit the configuration, use the `ADD OA DNS` command.
- Verify that the web proxy settings are configured correctly in OA.
- Verify that your configuration meets the network requirements for Insight Online direct connect.

Editing the web proxy settings

Proxy settings must be maintained to enable your enclosure to continue to send Remote Support data to Hewlett Packard Enterprise. If the proxy settings change, use the following procedure to edit them.

Procedure

1. Go to **Enclosure Information** > **Enclosure Settings** > **Remote Support**.
2. Update the following settings, as needed:
   - **Web Proxy Server**

     Enter the web proxy server in the format http://<hostname or IP address>.
   - **Web Proxy Port**
   - **Web Proxy Username**
   - **Web Proxy Password**
3. Click **Apply**.

Registering for Insight Remote Support using central connect

To register a BladeSystem c-Class enclosure for Insight Remote Support central connect, use the following procedure.

Procedure

1. Verify that the system meets the prerequisites for using Insight Remote Support.

   For more information, see **Prerequisites for registering for Insight Remote Support**.
2. Go to **Enclosure Information** > **Enclosure Settings** > **Network Access** and click the **Protocol** tab.
3. Verify that the **Enable XML Reply** check box is selected.

   If this check box is not selected, the Insight RS hosting device cannot collect data from the Onboard Administrator.
4. Go to **Enclosure Information** > **Enclosure Settings** > **Remote Support**.
5. Select **Register this enclosure through an HP Insight Remote Support centralized hosting device**.

   The page updates to show the central connect registration options.
6. Enter the Insight RS hosting device host name or IP address and port number. The default port is 7906.
7. Click **Register.**

   By registering, you agree to send registration, service events, and configuration data to Hewlett Packard Enterprise. All data collected and sent to Hewlett Packard Enterprise will be managed according to the Data Privacy Policy. You can view the Data Privacy Policy at the **Hewlett Packard Enterprise website**.

   The following message appears:

   ```
   Device successfully registered.
   ```
8. (Optional) Send a test event to confirm the connection between OA and Insight Remote Support.
   a. Go to **Enclosure Settings** > **Remote Support**.
   b. Click the **Service Events** tab.
   c. Click **Send Test Event**.

Unregistering from Insight Remote Support central connect

Use the following procedure to unregister a BladeSystem c-Class enclosure from Insight Remote Support central connect.

Procedure

1. Log in to the Insight RS Console.
2. Do one of the following:
   - To stop monitoring a BladeSystem c-Class enclosure temporarily, select the enclosure on the **Devices** > **Device Summary** tab in the Insight RS Console, and then select **ACTIONS** > **DISABLE SELECTED**.
   - To stop monitoring a BladeSystem c-Class enclosure permanently, delete the enclosure from the Insight RS Console. To delete the enclosure, select it on the **Device Summary** tab, and then select **ACTIONS** > **DELETE SELECTED**.

   Disabling or deleting the enclosure in the Insight RS Console does not unregister the enclosure in OA. For OA to be aware that an enclosure is disabled, you must use OA to unregister from Insight Remote Support.
3. Go to **Enclosure Information** > **Enclosure Settings** > **Remote Support** in the OA web interface.
4. Click **Unregister**.

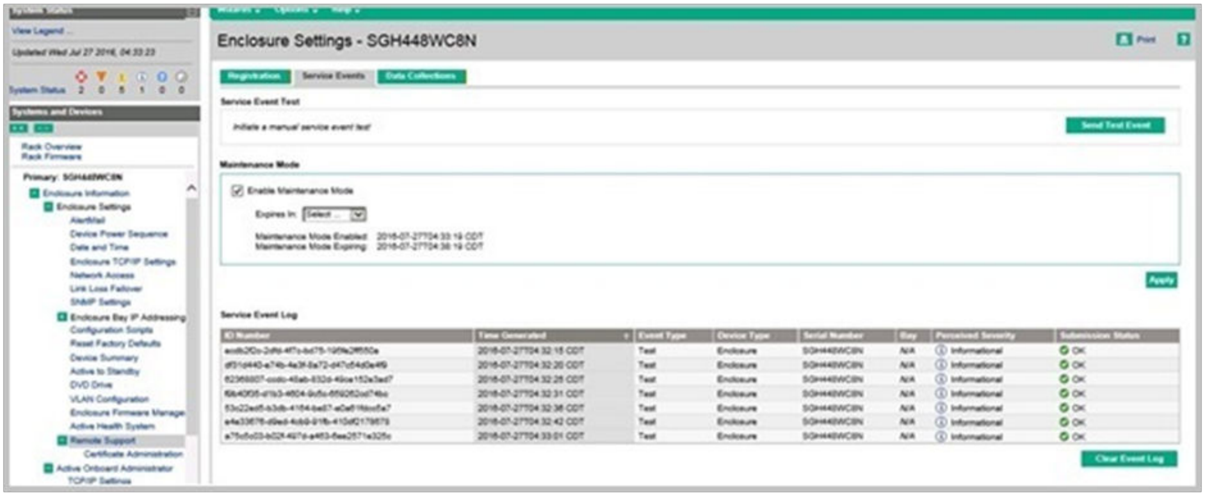
   The following message appears:

   ```
   Are you sure you want to un-register and disable HP Insight Remote Support?
   ```
5. Click **OK**.

The following message appears:

```
The enclosure is not registered.
```

Insight Remote Support Service Events



Enclosure Settings - SGH448WC8N

Service Event Test

Initiate a manual service event test

Maintenance Mode

☑ Enable Maintenance Mode

Expires In: Select ...

Maintenance Mode Enabled: 2016-07-27T04:33:19 CDT
Maintenance Mode Expiring: 2016-07-27T04:38:19 CDT

Service Event Log

ID Number	Time Generated	Event Type	Device Type	Serial Number	Bay	Perceived Severity	Submission Status
ecdb2f0c-2dfd-4f7c-bd75-19f9e2ff550a	2016-07-27T04:32:15 CDT	Test	Enclosure	SGH448WC8N	N/A	ⓘ Informational	✓ OK
df31d440-a74b-4a3f-8a72-d47c54d0e4f9	2016-07-27T04:32:20 CDT	Test	Enclosure	SGH448WC8N	N/A	ⓘ Informational	✓ OK
62368807-ccdc-46ab-832d-49ce152e3ad7	2016-07-27T04:32:26 CDT	Test	Enclosure	SGH448WC8N	N/A	ⓘ Informational	✓ OK
f6b40f35-d1b3-4604-9d5c-6f9262cd74bc	2016-07-27T04:32:31 CDT	Test	Enclosure	SGH448WC8N	N/A	ⓘ Informational	✓ OK
53c22ed5-b3db-4164-ba07-a0af1fdcc5a7	2016-07-27T04:32:36 CDT	Test	Enclosure	SGH448WC8N	N/A	ⓘ Informational	✓ OK
e4e33676-d9ed-4cb0-91fb-410df2179879	2016-07-27T04:32:42 CDT	Test	Enclosure	SGH448WC8N	N/A	ⓘ Informational	✓ OK
a75c5c03-b02f-497d-a463-6ee2571e325c	2016-07-27T04:33:01 CDT	Test	Enclosure	SGH448WC8N	N/A	ⓘ Informational	✓ OK

Use the Remote Support Service Events page to monitor service events, send test events, or set maintenance mode.

A service event is a hardware failure, for example, a problem with an enclosure power supply module or enclosure fan module. When the BladeSystem Enclosure is registered with Insight Remote Support, service events are logged and sent to Hewlett Packard Enterprise. When Hewlett Packard Enterprise receives a service event, a support case is opened and details are displayed in the Service Event Log.

NOTE:

To receive email alerts about system events, configure AlertMail on the **AlertMail** page.

Go to **Enclosure Information** > **Enclosure Settings** > **AlertMail**.

Using Maintenance Mode

Use Maintenance Mode when performing maintenance on a system. During this time, if a service event is generated, the event will indicate that the system is in maintenance mode. This service event helps Hewlett Packard Enterprise to determine whether to open a service case. If maintenance mode is not turned off by the user explicitly during this time, it is turned off automatically by Onboard Administrator after the selected amount of time has passed.

To use Maintenance Mode:

1. Select the **Enable Maintenance Mode** check box.
2. Select a time in the **Expires in** menu.
3. Click **Apply**.

Maintenance mode ends automatically when the selected amount of time has passed.

Sending a test service event

To verify that your Insight Remote Support configuration is correct, click **Send Test Event** to send a test event.

When the transmission is finished, the test event is listed in the Service Event Log.

Viewing the Service Event Log

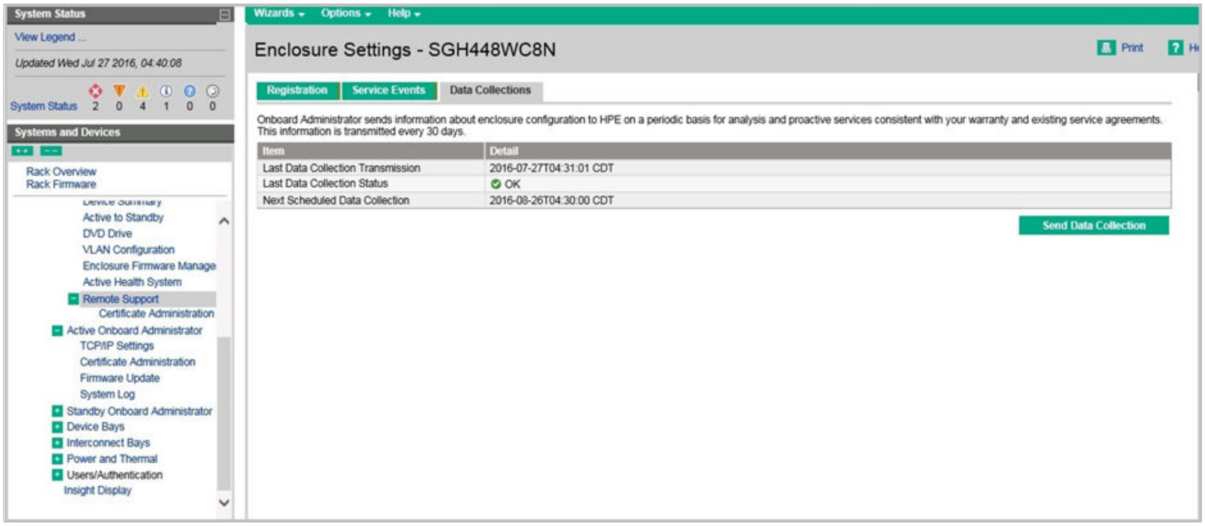
The Service Event Log displays the following details for each service event.

Row	Description
ID Number	A unique string that identifies the service event
Time Generated	The time the service event was generated
Event Type	Each event is classified with a type of either System or Test
Device Type	A string that identifies the source of the event. Possible values are Fan, Power Supply, Onboard Administrator, Interconnect, or Enclosure.
Serial Number	A string that provides the serial number of the device that generated the event.
Bay	The bay number of the device that generated the event.
Perceived Severity	A string that indicates the severity of the event. The possible values are Critical Error, Degraded, or Informational.
Submission Status	The status of the event submission. Possible values are OK or ERROR.

Clearing the Service Event Log

To clear the Service Event Log, click **Clear Event Log**.

Insight Remote Support Data Collections



Enclosure Settings - SGH448WC8N

Onboard Administrator sends information about enclosure configuration to HPE on a periodic basis for analysis and proactive services consistent with your warranty and existing service agreements. This information is transmitted every 30 days.

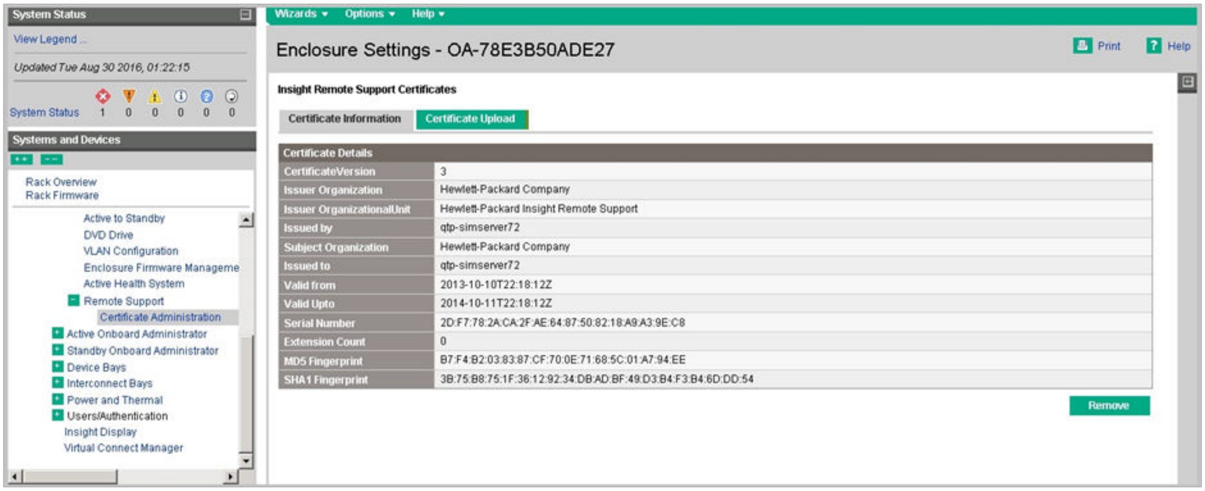
Item	Detail
Last Data Collection Transmission	2016-07-27T04:31:01 CDT
Last Data Collection Status	✓ OK
Next Scheduled Data Collection	2016-08-26T04:30:00 CDT

Data collection information

Insight Online direct connect

Row	Description
Last Data Collection Transmission	The date and time of the last successful data collection
Last Data Collection Status	The transmission status; possible values are OK or Error
Next Scheduled Data Collection	The date and time of the next scheduled data collection; data collection is scheduled automatically at 30-day intervals

Remote Support Certificate Administration



Enclosure Settings - OA-78E3B50ADE27

Insight Remote Support Certificates

Certificate Details	
CertificateVersion	3
Issuer Organization	Hewlett-Packard Company
Issuer OrganizationalUnit	Hewlett-Packard Insight Remote Support
Issued by	qtp-simserver72
Subject Organization	Hewlett-Packard Company
Issued to	qtp-simserver72
Valid from	2013-10-10T22:18:12Z
Valid Upto	2014-10-11T22:18:12Z
Serial Number	2D:F7:78:2A:CA:2F:AE:64:87:50:82:18:A9:A3:9E:C8
Extension Count	0
MD5 Fingerprint	B7:F4:B2:03:83:87:CF:70:0E:71:68:5C:01:A7:94:EE
SHA1 Fingerprint	3B:75:B8:75:1F:36:12:92:34:DB:AD:BF:49:D3:B4:F3:B4:6D:DD:54

Figure 4: Certificate Information tab

This screen displays all Insight Remote Support server certificates trusted by the Onboard Administrator. A maximum of eight certificates can be uploaded to the Onboard Administrator. Certificates ensure that the Onboard Administrator sends information securely to the Insight Remote Control server. If no certificates are used, then the communication is vulnerable to a "man-in-the-middle" attack. To ensure the certificate is valid and has not been modified, verify the SHA1 fingerprint of the certificate through a separate method, such as email from the server administrator, a webpage, or some other trusted source.

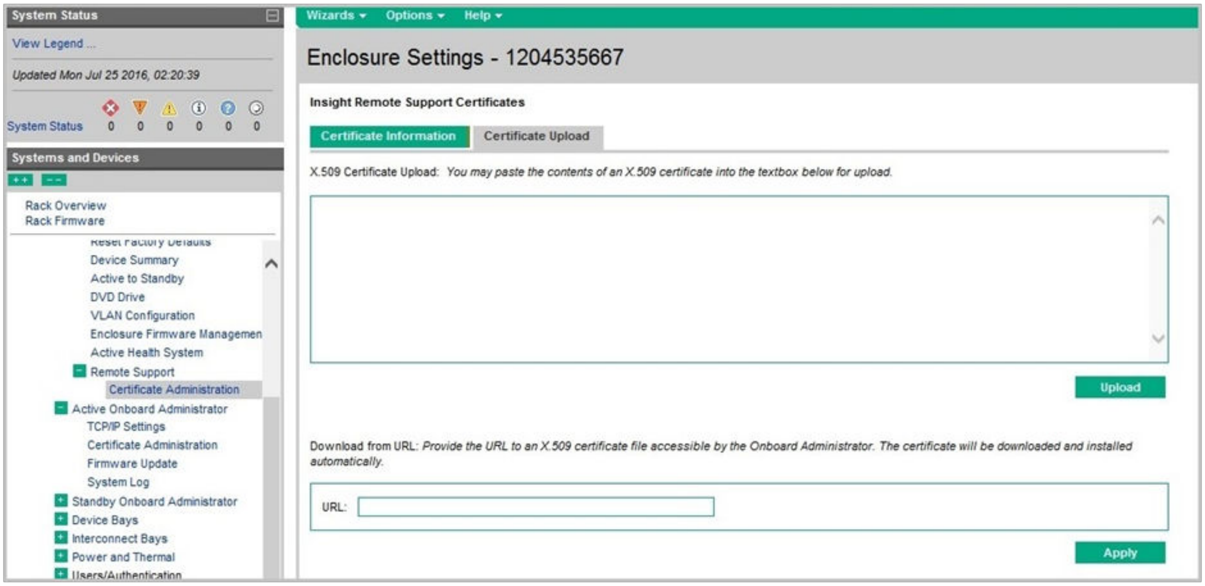
NOTE:

A valid certificate is required if connecting to an Insight Remote Support Hosting Device and the Onboard Administrator is operating in FIPS Mode.

When the Onboard Administrator is operating in FIPS Mode ON, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. In FIPS Top-Secret Mode - certificates must have a minimum RSA key length of 3072 bits or ECDSA 384 bits, and the signature hash algorithm must be SHA-384.

Row	Description
Certificate Version	Version number of current certificate
Issuer Organization	Name of the organization that issued the certificate
Issuer Organization Unit	Name of the organizational unit that issued the certificate
Issued By	The certificate authority that issued the certificate
Subject Organization	Subject name
Issued To	Organization to whom the certificate was issued
Valid From	The date from which the certificate is valid
Valid Upto	The date the certificate expires
Serial Number	The serial number assigned to the certificate by the certificate authority
Extension Count	Number of extensions in the certificate
MD5 Fingerprint	This field can be used to validate the authenticity of the certificate
SHA1 Fingerprint	This field can be used to validate the authenticity of the certificate.

Remote Support Certificate Administration Upload tab



Enclosure Settings - 1204535667

Insight Remote Support Certificates

X.509 Certificate Upload: *You may paste the contents of an X.509 certificate into the textbox below for upload.*

Download from URL: *Provide the URL to an X.509 certificate file accessible by the Onboard Administrator. The certificate will be downloaded and installed automatically.*

URL:

Figure 5: Certificate Upload tab

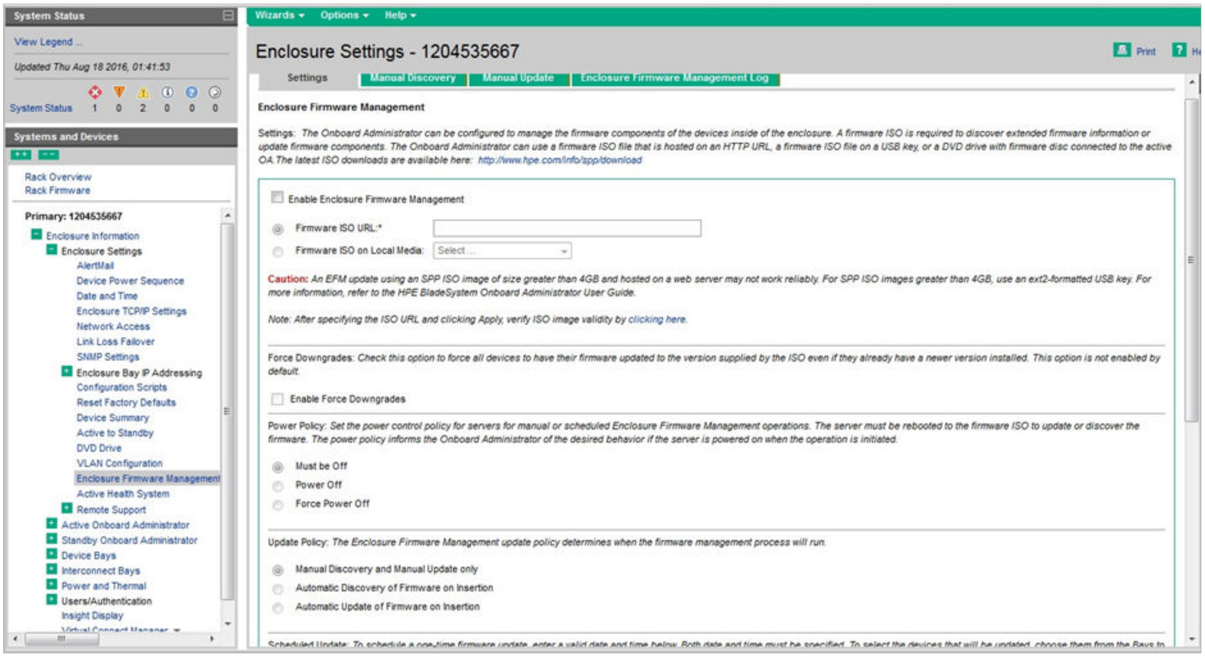
Upload the certificate of the Insight Remote Support server to the Onboard Administrator.

There are two methods for uploading certificates for use in HPE BladeSystem Onboard Administrator:

- Paste certificate contents into the text field and click **Upload**.
- Paste the URL of the certificate into the URL field and click **Apply**.

Enclosure Firmware Management

The Enclosure Firmware Management feature provides a single point from which to manage firmware on supported Hewlett Packard Enterprise servers and interconnect modules in the enclosure. As a result, EFM allows administrators to define a single firmware baseline (SPP version) for the server blades in an enclosure. The firmware can be updated to the baseline on server insertion or during a pre-defined maintenance window, or the firmware can be updated manually. The Onboard Administrator maintains logs of the EFM firmware updates, and reports on compliance with the established baseline.



Enclosure Settings - 1204535667

Enclosure Firmware Management

Settings: *The Onboard Administrator can be configured to manage the firmware components of the devices inside of the enclosure. A firmware ISO is required to discover extended firmware information or update firmware components. The Onboard Administrator can use a firmware ISO file that is hosted on an HTTP URL, a firmware ISO file on a USB key, or a DVD drive with firmware disc connected to the active OA.The latest ISO downloads are available here:* http://www.hpe.com/info/spp/download

□ Enable Enclosure Firmware Management

● Firmware ISO URL:*

○ Firmware ISO on Local Media: Select ...

Caution: *An EFM update using an SPP ISO image of size greater than 4GB and hosted on a web server may not work reliably. For SPP ISO images greater than 4GB, use an ext2-formatted USB key. For more information, refer to the HPE BladeSystem Onboard Administrator User Guide.*

Note: After specifying the ISO URL and clicking Apply, verify ISO image validity by clicking here.

Force Downgrades: *Check this option to force all devices to have their firmware updated to the version supplied by the ISO even if they already have a newer version installed. This option is not enabled by default.*

□ Enable Force Downgrades

Power Policy: *Set the power control policy for servers for manual or scheduled Enclosure Firmware Management operations. The server must be rebooted to the firmware ISO to update or discover the firmware. The power policy informs the Onboard Administrator of the desired behavior if the server is powered on when the operation is initiated.*

● Must be Off
○ Power Off
○ Force Power Off

Update Policy: *The Enclosure Firmware Management update policy determines when the firmware management process will run.*

● Manual Discovery and Manual Update only
○ Automatic Discovery of Firmware on Insertion
○ Automatic Update of Firmware on Insertion

Scheduled Update: *To schedule a one-time firmware update, enter a valid date and time below. Both date and time must be specified. To select the devices that will be updated, choose them from the Bays to*

Enclosure Firmware Management execution and reporting

During an EFM firmware update of devices within the enclosure, different phases of the update process and the associated processing that execute on the OA module consume a significant amount of OA resources (CPU, memory, and network throughput). This is especially true when attempting to perform the firmware update of multiple blades in the enclosure simultaneously. Resources within the OA module might not be sufficient to support the simultaneous firmware update of all devices within an enclosure. Therefore, it is necessary to control the instantaneous load demands that the EFM processing places on the OA module. To accomplish this, the OA firmware implements a form of job control based on a dynamic resource management heuristic that attempts to limit the resource utilization of EFM-related processing to a level that does not interfere with the OA module’s ability to perform its other enclosure management tasks. As part of this dynamic resource management heuristic, the OA firmware specifically monitors the following factors:

- Processor utilization (specifically, the process load average on the OA module’s embedded CPU)
- Memory utilization
- Number of outstanding transfers of the firmware ISO to the blades via iLO Virtual Media.

Based on these factors, the EFM job control logic updates the servers in batches when necessary by (1) allowing the simultaneous update of as many devices within the enclosure as can fit within the established resource limits enforced by the dynamic resource management heuristic and (2) delaying the update of other devices until resources become available. Thus, when the simultaneous update of multiple enclosure devices is attempted, some of the updates might not be performed all at once. The point at which the batching occurs is variable and depends on such factors as the number of devices selected for update, management network considerations such as amount and type of traffic, the specific OA configuration, other outstanding management activities being performed by the OA, and any other factor that impacts the resource utilization on the OA module when the EFM update is initiated. Evidence of such batching might be certain delays reported in the Firmware log.

For more information about the Firmware log and other firmware management logs, see **Firmware management logs**.

EFM and integration with HP SUM

EFM discovers and updates firmware by booting a server from a supported HPE SPP ISO image. EFM orchestrates the HP SUM engine integrated into the SPP ISO, providing results similar to running HP SUM manually but saving time by centralizing control and discovering and updating firmware on multiple servers.

During execution of an EFM task, if an associated HP SUM or EFM operation fails, EFM automatically initiates a retry of the entire EFM task. EFM will attempt executing the task a total of three times. Attempted retries potentially repeat steps previously completed in the EFM task, depending on the point where the failure occurs. If the task cannot be completed successfully on the last attempt, the EFM task terminates with a failed status.

NOTE:

In rare circumstances, although the HP SUM processes have terminated due to a failure, EFM logs might still indicate successful completion of the overall EFM task. Firmware levels will not be updated as expected, and this can be observed as a discrepancy between the installed firmware versions reported and the firmware versions available on the firmware ISO being used. When such a discrepancy occurs, Hewlett Packard Enterprise recommends checking the Firmware and Session logs for evidence of an HP SUM failure. If one is indicated, the EFM task could have failed as well. For more information about EFM logs, see **Firmware management logs**. For more information about EFM failures, see **Enclosure Firmware Management log**. For more information about viewing firmware versions, see **Viewing firmware versions**.

HP SUM does not support TPM firmware update. Therefore, OA EFM does not support TPM firmware update.

Other processing performance precautions

Enclosure Firmware Management will not work reliably and should not be used on slow network links (less than 1GB).

While running Enclosure Firmware Management operations, the Onboard Administrator response time might be slower than usual, and during brief intervals, enclosure status might be reported as degraded. You can safely ignore messages or alert conditions of this nature while the operations are in progress.

NOTE:

The c-Class BladeSystem ProLiant and Integrity iLO virtual media performance will be limited based on the activity and number of simultaneous iLO virtual media sessions and the Onboard Administrator workload. The Onboard Administrator Enclosure DVD and Enclosure Firmware Management features also use the iLO virtual media feature and will have similar performance limitations. To prevent media timeout issues, Hewlett Packard Enterprise recommends that you limit the number of simultaneous sessions. If timeout issues are experienced during OS install or firmware updates, reduce the number of virtual media sessions in progress, and restart the operation.

In rare circumstances during an EFM task, certain server-side failures (such as the iLO firmware update process hanging or taking an excessively long time to complete) can occur without providing failure indications to the associated EFM process. When such errors occur, the OA EFM task does not complete and appears to be hung with no progress or status reported. To recover from this condition, reboot the active OA module or perform a manual failover to the redundant OA module.

Enclosure Firmware Management settings

Enclosure Firmware Management settings are restricted to users with administrator privileges in Onboard Administrator and are available on the Onboard Administrator GUI in **Enclosure Settings** > **Enclosure Firmware Management** or from the Onboard Administrator CLI.

Required user permissions

All Enclosure Firmware Management features are available through both the Onboard Administrator GUI and CLI, unless Secure Boot is in effect for the blade in the enclosure. Secure Boot restricts users from modifying boot options or performing boot operations from the Onboard Administrator GUI or CLI. These tasks must be performed from the device configured in BIOS by the Administrator.

The Onboard Administrator user role and bay permissions control the Enclosure Firmware Management settings and ability to view the firmware information.

User role	Modify settings or scheduled update	Initiate manual discovery or update	View firmware versions
Onboard Administrator administrator or operator	Yes	Yes, OA Administrator only [1]	Yes
Server administrator or operator	No	Yes, OA Administrator only [1]	Yes, for permitted server bays
Onboard Administrator user	No	No	Yes, for permitted bays

[1] *If Secure Boot mode is in effect for the blade in the enclosure, this operation cannot be performed from the GUI or CLI.*

Enabling Enclosure Firmware Management

The **Enable Enclosure Firmware Management** check box globally enables or disables (default setting) Enclosure Firmware Management. When disabled, you cannot start any manual Enclosure Firmware Management operations. Any previously configured automatic or scheduled operation does not occur. If the setting is changed from enabled to disabled, any in-progress Enclosure Firmware Management discoveries or updates continue until they are finished.

IMPORTANT:

After Enclosure Firmware Management operations (updates and discoveries) have begun on a server, you cannot stop these operations. Ensure that your enclosure is IPv6-enabled before using an IPv6 address for the Firmware Management ISO.

Enclosure Firmware Management is not supported on the following Onboard Administrator hardware modules:

- HPE BladeSystem c3000 Onboard Administrator (part number 448589-B21, 461514-B21)
- HPE BladeSystem c7000 Onboard Administrator (part number 412142-B21)

Enclosure Firmware Management cannot be enabled unless the Active Onboard Administrator hardware module is supported. If you attempt to enable Enclosure Firmware Management when the Active Onboard Administrator is not supported, an error message appears:

```
Enclosure Firmware Management is not supported on the active OA hardware
present.
```

If the Standby Onboard Administrator module is not supported, a warning message appears:

```
Enclosure Firmware Management is not supported on the standby OA hardware
present. The feature will be disabled if the standby OA becomes Active.
```

Enclosure Firmware Management fails on any blade if SSH is disabled in the blade's iLO configuration settings. By default, SSH is enabled in iLO.

Configuring the location of the firmware image

To perform firmware discovery or firmware updates, Enclosure Firmware Management requires a firmware ISO image. The latest ISO downloads are available at the **Hewlett Packard Enterprise website**.

You can provide one the following locations for the ISO firmware image:

- An HTTP URL-based ISO image hosted on a web server.

  Provide an IPv4 address in the following format: `protocol://[<IPv4 Address>]/path/filename`.

To provide an IPv6 URL address, specify the address between brackets in the following format: `protocol://[<IPv6 Address>]/path/filename`.

The maximum length of the URL is 511 characters.

The maximum supported size of the SPP ISO image is 4GB. With SPP ISO images greater than 4GB, create a custom ISO image that excludes components unnecessary to the OA EFM blade firmware update process. At minimum, the custom ISO must contain only the firmware components for HPE ProLiant BL Series server blades. For information about creating a custom ISO image, see the HPE BladeSystem Onboard Administrator User Guide.

To use the complete ISO image with a file size greater than 4GB, you must use an ext2-formatted USB key.

- A USB key with ISO image connected to the USB port of the Onboard Administrator.

  A USB key converted to bootable media from the SPP ISO image is not supported with Enclosure Firmware Management. The USB key must contain the ISO image in the root directory.

  The maximum supported file size for USB keys formatted with FAT32 is 4GB. For SPP images greater than 4GB, use an ext2-formatted USB key. For information about formatting a USB key with an ext2 file system, see **USB Menu screen**.
- A physical DVD inserted into the enclosure DVD drive.

  If a physical DVD is used, the DVD must not contain the ISO image. The DVD must be a bootable disk created from the ISO image.

NOTE:

After disabling IPv6 to convert to an IPv4-only environment, if the Enclosure Firmware Management Firmware ISO URL specifies a USB key or an IPv6-based URL for a web server, you must reenter the location of the USB key or provide an IPv4-based URL for the web server. If this is not done, EFM cannot access the ISO image.

After specifying the ISO URL and clicking **Apply**, verify ISO image validity by clicking the provided **clicking here** link.

Creating a custom SPP ISO image

The following instructions provide the basic steps for creating a custom SPP ISO image compatible for Onboard Administrator EFM functionality. It is assumed that you have experience using HP SUM to create custom ISO images. For more information, see the HP SUM online help, or see the *Building and deploying a customized SPP firmware ISO image* white paper and other documentation in the **Hewlett Packard Enterprise Information Library**.

Procedure

1. Download the SPP ISO image containing HP SUM 7.2 (or later) to a folder on your local drive.
2. Launch the HP SUM batch file.
3. From the **Options** menu, select **Baseline Library**.

   The SPP is automatically added as a baseline. Wait until HP SUM displays and finishes inventory on the baseline before proceeding to the next step,.
4. From the Baseline Library **Actions** tab, select **Create Custom**.
5. From the Create Custom Baseline window, specify the necessary information in the Overview section.

- **Output Location** - specify or browse to the location where you want the custom ISO image placed.
- **Extracted Source ISO Location** - click **Browse** to select the source SPP ISO image that will be customized.
- Select the **Make Bootable ISO file** check box.

6. In the **Step 2 - Filters** section:
   - Select **Firmware** in the **Component Type** field.
   - Select all check boxes (**Critical Updates**, **Recommended Updates**, and **Optional Updates**).
7. Click **Advanced Filters** and select the required filters.

   For **Server Model**, select **HP ProLiant BL Series**.
8. In the **Step 3 - Review** section, click **Apply Filters**.

   Wait until all filtered components are retrieved. The status of the retrieval process can be viewed at the bottom of the page. When the process completes, the message "`Completed retrieving components`" is displayed.
9. Click **Create ISO**.

   After a few minutes, the customized SPP ISO image is ready for use at the **Output Location** specified earlier.

Enabling force downgrades

This check box globally enables or disables (default setting) forced downgrades. When disabled, components that have higher firmware revisions than are present on the ISO image are excluded from update. This setting is for all the supported server blades in this enclosure. When enabled, Enclosure Firmware Management instructs the HP SUM engine to enable flashing of component firmware that is at a higher revision than in the image. Enabling this setting does not guarantee component firmware will be downgraded. If you are using the Enable Force Downgrades option, consult the ISO documentation in advance to correctly set expectation.

Setting the power policy

The server must be booted from the ISO image to update or discover the firmware. The power policy informs the Onboard Administrator of what action to take if the server is powered on when the operation is initiated. This setting applies to both scheduled and manual operations. The default power policy is **Must be Off**.

If power policy is set to Power Off, the Onboard Administrator waits five minutes for the server to respond to the request. If the server does not shutdown in this time the Firmware Management operation fails. If the server is running an operating system that initiated the shutdown but did not complete within five minutes, the server might shut down and remain powered off.

Setting	Description
Must be Off	The Onboard Administrator cancels the operation if the server is powered on.
Power Off	The Onboard Administrator mimics a physical momentary press of the power button on the server blade, powering the server blade off gracefully.
Force Power Off	The Onboard Administrator mimics a physical press and hold of the power button on the server blade, forcing the server blade to shut power off without regard for first shutting down the OS.

CAUTION:

You must be careful when using the Force Power Off policy on servers with an operating system installed, because data corruption might occur.

Setting the update policy

Update policies available for Firmware Management include:

- **Manual Discovery and Manual Update Only**

  The default policy. This policy prevents the Onboard Administrator from automatically performing server update or discovery upon insertion into the enclosure.

  Manual Discovery or Update and Scheduled Update is required before the Onboard Administrator can display extended server firmware versions.
- **Automatic Discovery on Insertion**

  Enables the Onboard Administrator to perform a boot for discovery on a server enabled using Bays to Include, collecting extended firmware information for that server, updating the firmware management log for that event, and then rebooting the server into normal operation. You can then view the detected firmware versions and update that firmware with either a manual or scheduled update.
- **Automatic Update on Insertion**

  Enables the Onboard Administrator to perform a boot for update on a server enabled using Bays to Include, collecting updated extended firmware information for that server, updating the firmware management log for that event, and then rebooting the server into normal operation. This policy updates the server firmware to the selected firmware image after a service event, such as replacing the server board or option card.

Automatic Discovery and Automatic Update are mutually exclusive policies and affect all Bays to Include in the enclosure.

Setting a scheduled firmware update

A scheduled firmware update policy provides a schedule for the Onboard Administrator to automatically update all the Bays to Include to the firmware versions on the ISO firmware image. At the scheduled date and time, the Onboard Administrator starts an update operation using the Power Policy on all Bays to Include, updates their firmware using the ISO firmware image, and then reboots all the included servers back into normal operation.

Specifying the bays to include in a firmware management process

All device bays are included for firmware management by default. The Onboard Administrator administrator can select specific device bays to include and not select other device bays that must be excluded from enclosure firmware management update policies, manual updates, or scheduled updates.

By default, the **Firmware Manage All Servers** check box is selected, enabling Enclosure Firmware Management policies and scheduled updates to be performed on all available servers.

Either select each of the base bays, side a bays, and side b bays individually, or select all device bays by selecting the **Firmware Manage All Servers** check box.

To manually select specific servers for Enclosure Firmware Management:

1. Clear the **Firmware Manage All Servers** check box.
2. Select the check box next to the individual bays, or select bays according to bay type.
3. Click **Apply**.

   The updated list of bays to include for Enclosure Firmware Management appears.

Bay selection is currently limited to device bays only. Switch and Onboard Administrator bays cannot be selected.

The Bays to Include selection only applies to ProLiant server blades. Integrity server blades do not support this feature. Partner blade support is through the associated server blade based on whether the firmware ISO supports the PCIe adapter card in the partner blade.

Manual discovery

IMPORTANT:

While any Enclosure Firmware Management task is in progress, do not reboot the Onboard Administrator. Avoid shutting down or pulling out the blade from the enclosure.

Manual discovery of one or more servers can be initiated to simplify the collection of the existing firmware versions.

After initiating a manual firmware discovery, the Manual Discovery Device Bay Selection screen appears. Select one or more device bays on which to perform the discovery, or select the **Discover All Servers** check box to select all servers for the discovery. By default, all device bays and the Discover All Servers check box are selected.

If Secure Boot is configured on a server blade, you cannot select the associated bay (a padlock icon is displayed). Secure Boot mode restricts users from performing manual discovery from the Onboard Administrator GUI or CLI. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

To start the discovery process on the selected servers, click **Start Manual Discovery**.

Manual update

CAUTION:

Enclosure Firmware Management updates using an SPP image greater than 4GB and hosted from a web server might not work reliably.

IMPORTANT:

While any Enclosure Firmware Management task is in progress, do not reboot the Onboard Administrator. Avoid shutting down or pulling out the blade from the enclosure.

A manual update of one or more servers to the designated firmware image versions can be initiated. To initiate a firmware update on one or more servers, click **Manual Update**.

After initiating a manual firmware update the Manual Update Device Bay Selection screen appears. Select one or more device bays on which to perform the update, or select the **Update All Servers** check box to select all servers for the update. By default, all device bays and the Discover All Servers check box are selected.

If Secure Boot is configured on a server blade, you cannot select the associated bay (a padlock icon is displayed). Secure Boot mode restricts users from performing a manual update from the Onboard Administrator GUI or CLI. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

To start the update process on the selected servers, click **Start Manual Update**.

Enclosure Firmware Management log

The Enclosure Firmware Management log provides a consolidated view of major Enclosure Firmware Management events, such as firmware image selections, policy and schedule changes, and firmware operations initiating and completing. This log does not contain the step-by-step details included in the firmware log for each server.

The Enclosure Firmware Management log persists across OA reboots and power losses. It is retained on the Standby OA, if present.

To view updated log information, click **Refresh**.

To clear information for the Enclosure Firmware Management log and the server-specific Firmware log and Session log, click **Clear All Logs**. For more information about the Firmware log and Session log, see **Firmware management logs**.

To clear information for the Enclosure Firmware Management log, click **Clear Log**.

> **CAUTION:**
>
> Once deleted, this data cannot be restored.

Event failures

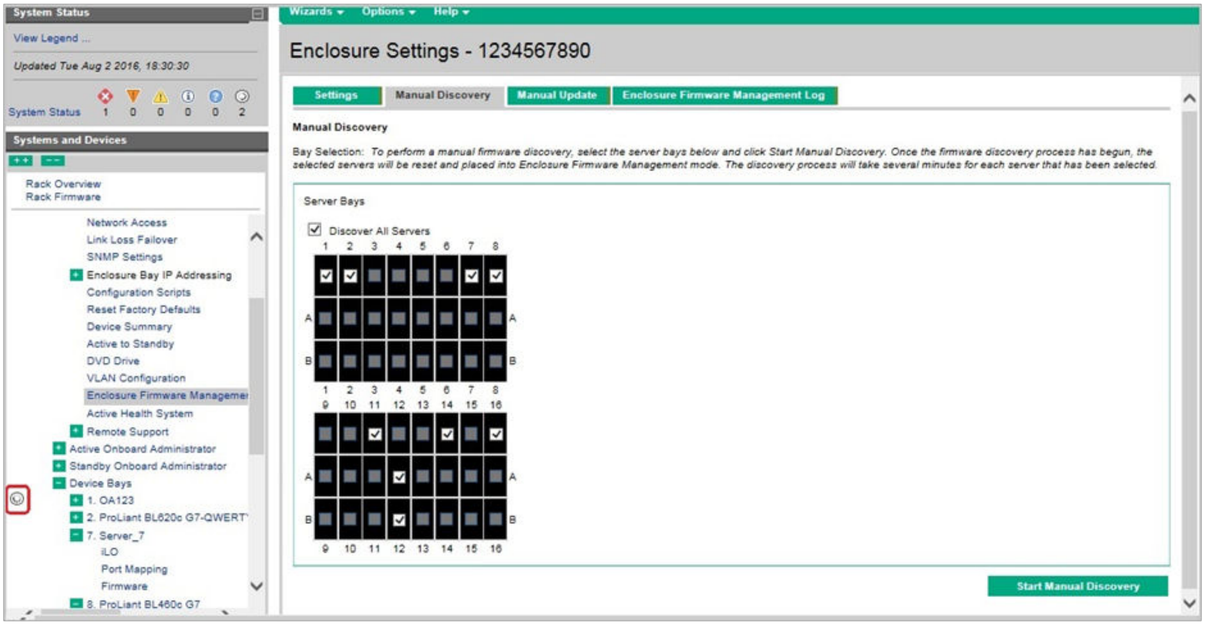
When an Enclosure Firmware Management task completes, the final event listed in the server firmware log is `Firmware Management successfully completed` or `Firmware Management is incomplete`.

If the last operation that appears in the Enclosure Firmware Management log does not indicate successful completion, the other firmware log entries might indicate the problem encountered by the Onboard Administrator. For example, the server must be powered off before a manual discovery, manual update, or scheduled update is performed. The log might indicate that the server was powered on, so the Enclosure Firmware Management operation was stopped.

If a failure occurs while performing an Enclosure Firmware Management task, the failed entry is logged as `Firmware Management failed on blade X`. The Onboard Administrator attempts the task again up to three times. If the task completes, the previous failed log entries can be disregarded. For detailed event information and current activity, see the firmware log for the server.

Status updates

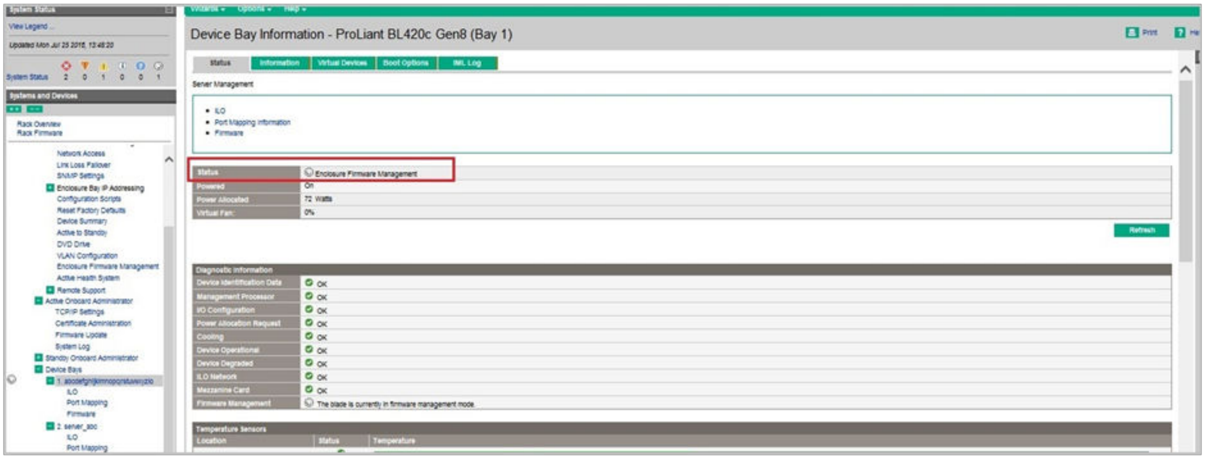
When an Enclosure Firmware Management task such as Manual Discovery or Manual Update is initiated on a server, an Enclosure Firmware Management status icon appears in the left navigation pane alongside each device being affected. In the following figure, one of several of these icons is encircled in red.



Bay Selection: *To perform a manual firmware discovery, select the server bays below and click Start Manual Discovery. Once the firmware discovery process has begun, the selected servers will be reset and placed into Enclosure Firmware Management mode. The discovery process will take several minutes for each server that has been selected.*

☑ Discover All Servers

While the Enclosure Firmware Management task is processing, the **Device Bay Status tab** displays server status as `Firmware Management`, as shown in the following figure.



Device Bay Information - ProLiant BL420c Gen8 (Bay 1)

Server Management

- iLO
- Port Mapping Information
- Firmware

Status	Enclosure Firmware Management
Powered	On
Power Allocated	72 Watts
Virtual Fan:	0%

Diagnostic Information	
Device Identification Data	OK
Management Processor	OK
I/O Configuration	OK
Power Allocation Request	OK
Cooling	OK
Device Operational	OK
Device Degraded	OK
iLO Network	OK
Mezzanine Card	OK
Firmware Management	The blade is currently in firmware management mode.

Temperature Sensors

Location	Status	Temperature

When the task is complete, the server status is returned to the appropriate indication. For meaning of status icons, click **View Legend...** near the top of the left navigation pane.

The server extended firmware information is time/date stamped when the discovery or update operation is complete. The information is written to a persistent location in the Onboard Administrator along with a log of the last firmware management event. This firmware information and log are also synchronized with the Standby Onboard Administrator, if present.

Managing enclosures

Powering off the enclosure

There are two methods for powering off an enclosure:

- Power off the PDU that powers the enclosure.
- Unplug the power cable(s) to the enclosure.

There is no virtual method in the Onboard Administrator to power down an enclosure.

Linking enclosures

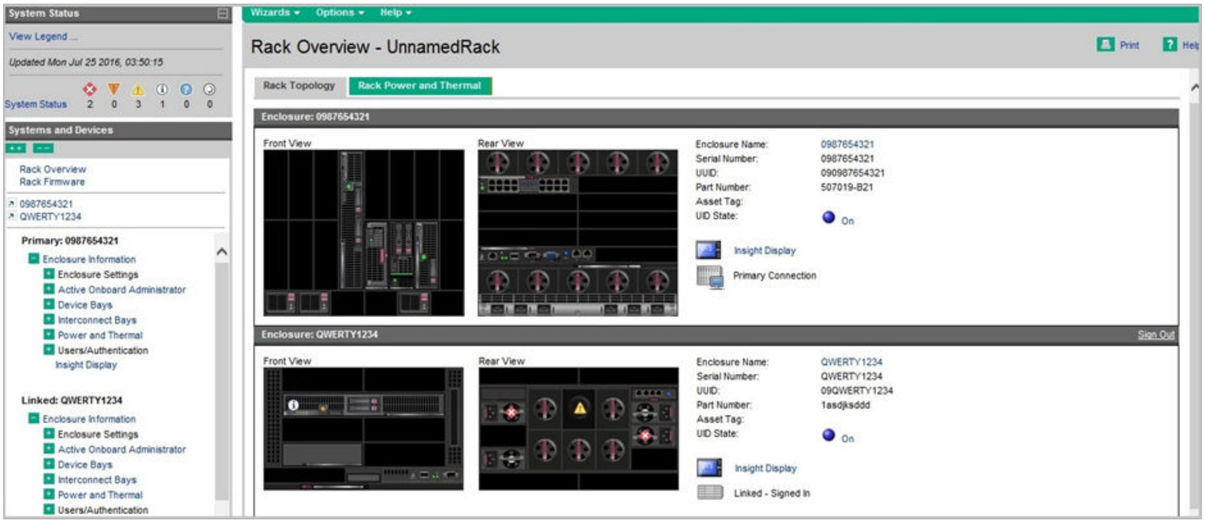
Linking enclosures can be done from the rear of the enclosure. For more information, see the appropriate BladeSystem c7000 Enclosure Setup and Installation guide.

Managing multiple enclosures

On the main menu within the Systems and Devices section of the screen, each enclosure is identified by its unique name (default enclosure name is the serial number of the enclosure). Clicking the green box containing a + expands the enclosure view, allowing access to the subcategories for the various blades, fans, power supplies, Onboard Administrators, and switches within the enclosure.

To physically determine which enclosure you are working on, press the Onboard Administrator UID button. Pressing the UID button illuminates a bright blue LED that is located on the tray. To turn off the UID, press the Onboard Administrator UID button a second time. When viewing the Enclosures screen, you can use one of two sections that can help you determine which enclosure is the enclosure you are attached to (highlighted in the image).

- Under Rack Overview, the name of the enclosure you are logged into is displayed.
- In the list of enclosures, the enclosure you are logged into displays Primary Connection.



Rack Overview - UnnamedRack

Enclosure: 0987654321

Enclosure Name:	0987654321
Serial Number:	0987654321
UUID:	090987654321
Part Number:	507019-B21
Asset Tag:	
UID State:	● On

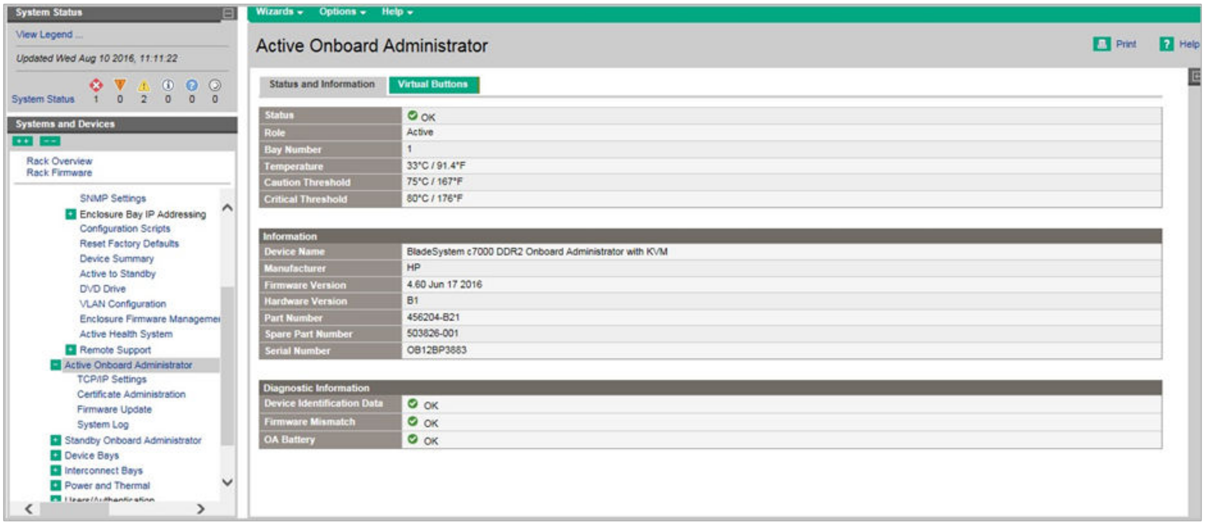
Enclosure: QWERTY1234

Enclosure Name:	QWERTY1234
Serial Number:	QWERTY1234
UUID:	09QWERTY1234
Part Number:	1asdjksddd
Asset Tag:	
UID State:	● On

Active Onboard Administrator Module

Active Onboard Administrator screen

The Active Onboard Administrator screen provides detailed information about Onboard Administrator.



Active Onboard Administrator

Status	✓ OK
Role	Active
Bay Number	1
Temperature	33°C / 91.4°F
Caution Threshold	75°C / 167°F
Critical Threshold	80°C / 176°F

Information	
Device Name	BladeSystem c7000 DDR2 Onboard Administrator with KVM
Manufacturer	HP
Firmware Version	4.60 Jun 17 2016
Hardware Version	B1
Part Number	456204-B21
Spare Part Number	503826-001
Serial Number	OB12BP3883

Diagnostic Information	
Device Identification Data	✓ OK
Firmware Mismatch	✓ OK
OA Battery	✓ OK

NOTE:

Accessing the Active OA through a link-local IPv6 address might not work on all client system setups containing multiple network interfaces.

Status and information tab

The Status and Information tab on the Active Onboard Administrator screen consists of three tables. These tables contain the status information, hardware information, and diagnostic information for the Onboard Administrator.

Status

Row	Description
Status	The overall status of the enclosure. Possible values are Unknown, OK, Degraded, and Failed.
Role	Possible values are Active or Standby.
Bay Number	The physical bay number where the Onboard Administrator is installed.
Temperature	The temperature of the Onboard Administrator measured in both degrees Celsius and Fahrenheit.
Caution Threshold	The temperature at which the enclosure will report a status of caution.
Critical Threshold	The temperature at which the enclosure will report a critical status.

General information

Row	Description
Device Name	The common descriptive name of the Onboard Administrator
Manufacturer	The name of the company that manufactured the Onboard Administrator
Firmware Version	The version of the firmware image in the Onboard Administrator
Hardware Version	The version of the enclosure hardware.
Part Number	The part number to be used when ordering an additional or replacement Onboard Administrator
Spare Part Number	The spare part number to be used when ordering an additional or replacement Onboard Administrator
Serial Number	The unique serial number of the Onboard Administrator

Diagnostic information

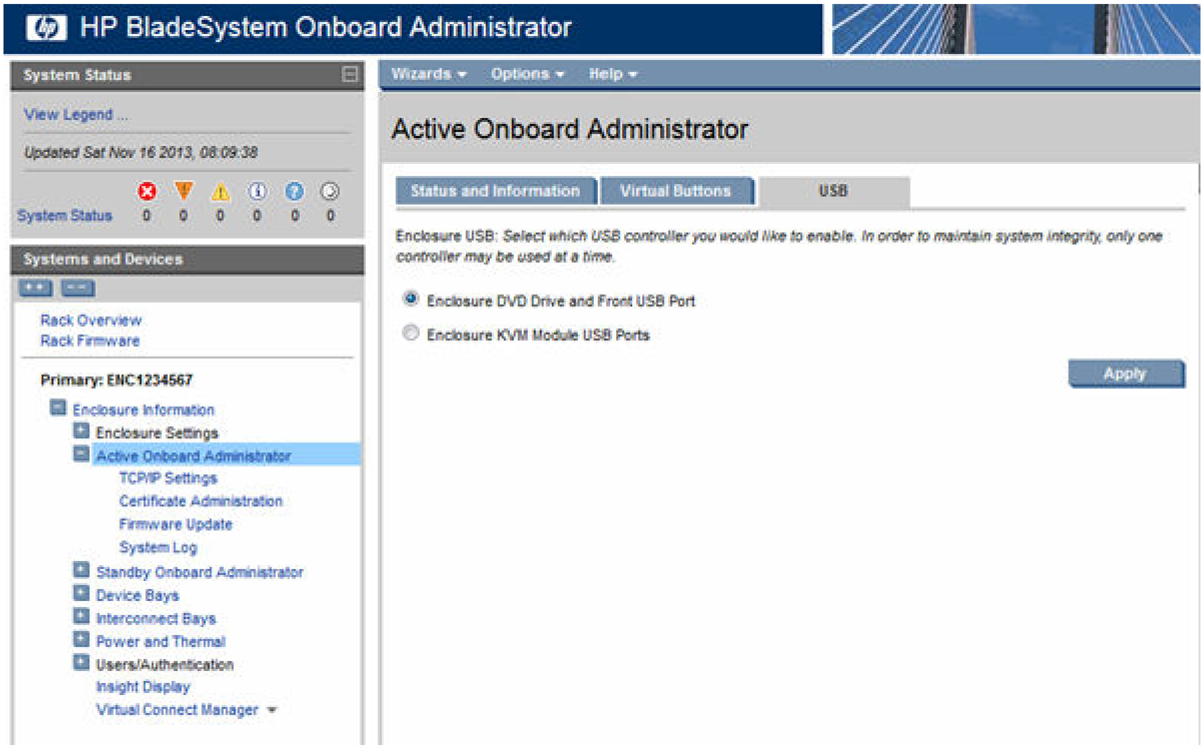
Row	Description
Device Identification Data	This row displays information such as model name, part number, serial number, and other information used to identify the device. This data is also referred to as FRU data. A device identification data error appears if the data is not present or not readable by the Onboard Administrator. Possible values are OK or Error.
Firmware Mismatch	The Onboard Administrator with the lowest firmware version displays this field when two Onboard Administrators are present.
OA Battery	Status of the Onboard Administrator battery. Possible values are OK or Error.

Active Onboard Administrator Virtual Buttons tab

Click **Reset** to reset the Onboard Administrator. A confirmation screen appears, asking if you are sure that you want to perform the action and that you will be signed out and disconnected from the Onboard Administrator. Click **OK** to proceed, or click **Cancel** to exit without a change.

Click **Toggle On/Off** to change the Onboard Administrator module UID light. This button is useful in identifying a particular Onboard Administrator when there are more than one.

Active Onboard Administrator USB tab



Enclosure USB: *Select which USB controller you would like to enable. In order to maintain system integrity, only one controller may be used at a time.*

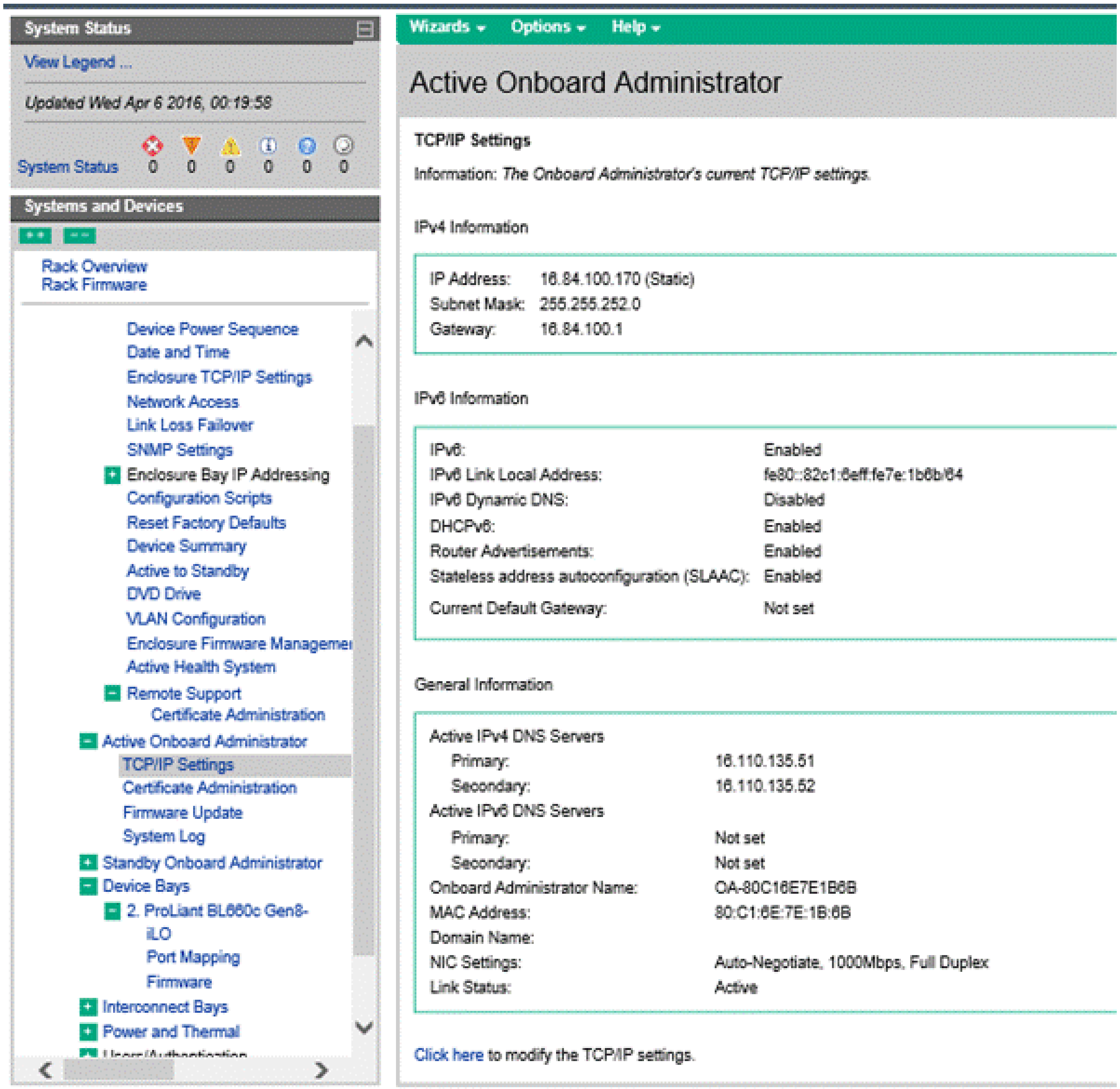
● Enclosure DVD Drive and Front USB Port

○ Enclosure KVM Module USB Ports

The **USB** tab only appears if an early version of the c3000 Onboard Administrator board (hardware revision level A0, B0, X1, or X3) is present.

With such boards, you can only use one USB controller at a time. This screen allows you to select which USB controller to enable: the one for the USB ports on the KVM module in the rear of the enclosure or the one for the DVD drive and USB port on the front of the enclosure. Changing the active USB controller resets the Active Onboard Administrator.

Active Onboard Administrator TCP/IP Settings screen



Active Onboard Administrator

TCP/IP Settings

Information: *The Onboard Administrator's current TCP/IP settings.*

IPv4 Information

IP Address:	16.84.100.170 (Static)
Subnet Mask:	255.255.252.0
Gateway:	16.84.100.1

IPv6 Information

IPv6:	Enabled
IPv6 Link Local Address:	fe80::82c1:6eff:fe7e:1b6b/64
IPv6 Dynamic DNS:	Disabled
DHCPv6:	Enabled
Router Advertisements:	Enabled
Stateless address autoconfiguration (SLAAC):	Enabled
Current Default Gateway:	Not set

General Information

Active IPv4 DNS Servers	
Primary:	16.110.135.51
Secondary:	16.110.135.52
Active IPv6 DNS Servers	
Primary:	Not set
Secondary:	Not set
Onboard Administrator Name:	OA-80C16E7E1B6B
MAC Address:	80:C1:6E:7E:1B:6B
Domain Name:	
NIC Settings:	Auto-Negotiate, 1000Mbps, Full Duplex
Link Status:	Active

Click here to modify the TCP/IP settings.

This screen displays the current enclosure TCP/IP settings for the Active Onboard Administrator:

- IPv4 Information
- IPv6 Information
- General Information

IPv4 Information

Parameter	Description
IP Address	The IPv4 address of the Active Onboard Administrator, with indication of the type of IP address assigned (static or dynamic).
Dynamic DNS	Indicates whether Dynamic DNS is enabled or disabled. Dynamic DNS updates the DNS server with new or changed records for IP addresses. This enables you to use the same host name over time, although the dynamically assigned IP address might change for the Active Onboard Administrator.

Table Continued

Parameter	Description
Subnet Mask	The subnet mask for the Active Onboard Administrator. The mask determines the subnet to which the Active Onboard Administrator IP address belongs.
Gateway	The gateway address for the Active Onboard Administrator.

IPv6 Information

Parameter	Description
IPv6	Indicates whether IPv6 is enabled or disabled on the Active Onboard Administrator.
IPv6 Link Local Address	The link local IPv6 address of the Active Onboard Administrator. When IPv6 is enabled, one link local IPv6 address is autoconfigured for the Active Onboard Administrator.
IPv6 Static Address 1	Onboard Administrator external NIC IPv6 address 1.
IPv6 Static Address 2	Onboard Administrator external NIC IPv6 address 2.
IPv6 Static Address 3	Onboard Administrator external NIC IPv6 address 3.
IPv6 Dynamic DNS	Indicates whether Dynamic DNS is enabled or disabled. Dynamic DNS updates the DNS server with new or changed records for IP addresses. This enables you to use the same host name over time, although the dynamically assigned IP address might change for the Active Onboard Administrator.
DHCPv6	Indicates whether DHCPv6 is enabled or disabled on the Active Onboard Administrator .
DHCPv6 Address	The DHCPv6 address of the Active Onboard Administrator.
Router Advertisements	Indicates whether router advertisements are enabled or disabled. Router advertisements are used for automatically configuring IPv6 addresses. When disabled, router advertisements are blocked, thereby preventing SLAAC address configuration of all devices within the enclosure.
Stateless address autoconfiguration (SLAAC)	Indicates whether SLAAC is enabled or disabled on the Active Onboard Administrator. Router advertisements must be enabled. See the description of Router Advertisements.
Stateless address autoconfiguration (SLAAC) Address	An autoconfigured SLAAC address. The Onboard Administrator can be assigned multiple SLAAC addresses based on its MAC address and the information received from router advertisements.
Current Default Gateway	Indicates the IPv6 address of the default gateway currently being used by the Active Onboard Administrator. The Current Default Gateway can be either the Static Default Gateway or a gateway configured via router advertisements. If router advertisements provide IPv6 gateway configuration, their gateway configuration overrides the static IPv6 gateway setting.
Static Default Gateway	Indicates the static IPv6 address of the IPv6 default gateway. This is displayed only if configured.
Static Route 1	The address of the external network or node that the Onboard Administrator can reach through an associated static route gateway.
Gateway (Static Route 1)	The address of the gateway used by the Onboard Administrator to reach the Static Route 1 destination.

Table Continued

Parameter	Description
Static Route 2	A second IPv6 static route.
Gateway (Static Route 2)	The address of the gateway used by the Onboard Administrator to reach the Static Route 2 destination.
Static Route 3	A third IPv6 static route.
Gateway (Static Route 3)	The address of the gateway used by the Onboard Administrator to reach the Static Route 3 destination.

General Information

Parameter	Description
Active IPv4 DNS Servers	Lists the configured IPv4 DNS servers that are active on the Active Onboard Administrator. [1]
Primary	IP address of the first IPv4 DNS server used by the Active Onboard Administrator. If not configured, `Not set` is displayed.
Secondary	IP address of the second IPv4 DNS server used by the Active Onboard Administrator. If not configured, `Not set` is displayed.
Active IPv6 DNS Servers	Lists the configured IPv6 DNS servers that are active on the Active Onboard Administrator. [1]
Primary	IP address of the first IPv6 DNS server used by the Active Onboard Administrator. If not configured, `Not set` is displayed.
Secondary	IP address of the second IPv6 DNS server used by the Active Onboard Administrator. If not configured, `Not set` is displayed.
Tertiary	IP address of the third IPv6 DNS server used by the Active Onboard Administrator. If not configured, this parameter and address are not displayed.
Quaternary	IP address of the fourth DNS server used by the Active Onboard Administrator. If not configured, this parameter and address are not displayed.
Onboard Administrator Name	The name (DNS host name) used for the Active Onboard Administrator.
VLAN ID (Name)	The unique number that identifies the VLAN. Displayed only if VLAN Mode is enabled.
MAC Address	The MAC address of the Active Onboard Administrator.
Domain Name	The name of the domain for the Active Onboard Administrator.
NIC Settings	The NIC settings for the Active Onboard Administrator, such as auto negotiation, duplex mode, and speed.
Link Status	Indicates whether the NIC is actively connected to the network.

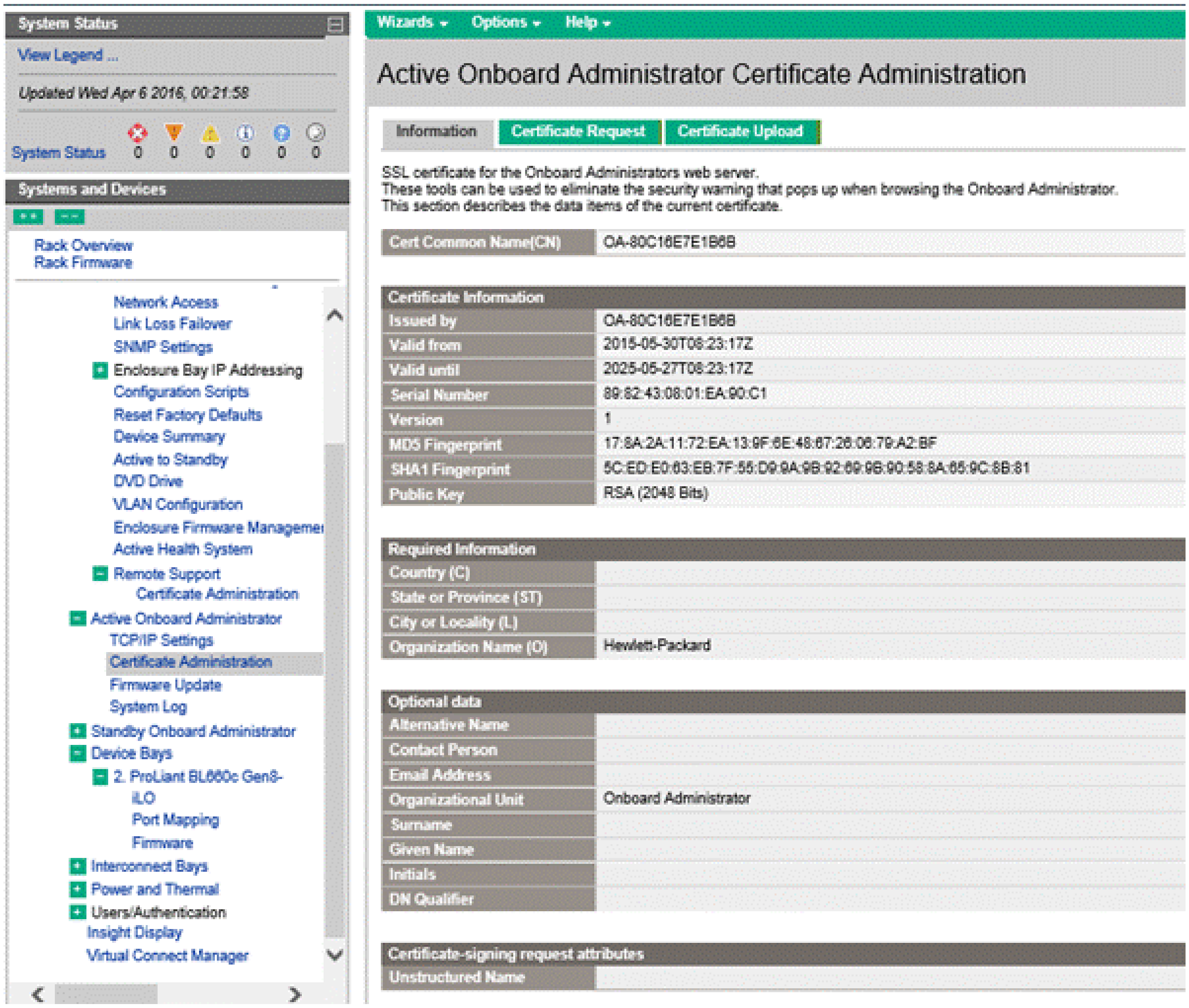
[1] *The order in which the Onboard Administrator uses DNS servers is described in* **IPv4 Settings tab** *and* **IPv6 Settings tab**.

To modify the TCP/IP settings, select **Click here**.

For information about the TCP/IP settings that you can modify, see the Enclosure TCP/IP **IPv4 Settings tab** and **IPv6 Settings tab**.

Certificate Administration Information tab

This screen displays the detailed information of the SSL certificate currently in use by the Onboard Administrator. An SSL certificate is used to certify the identity of Onboard Administrator and is required by the underlying HTTP server to establish a secure (encrypted) communications channel with the client web browser.



Active Onboard Administrator Certificate Administration

SSL certificate for the Onboard Administrators web server.
These tools can be used to eliminate the security warning that pops up when browsing the Onboard Administrator.
This section describes the data items of the current certificate.

Cert Common Name(CN)	OA-80C16E7E1B6B

Certificate Information	
Issued by	OA-80C16E7E1B6B
Valid from	2015-05-30T08:23:17Z
Valid until	2025-05-27T08:23:17Z
Serial Number	89:82:43:08:01:EA:90:C1
Version	1
MD5 Fingerprint	17:8A:2A:11:72:EA:13:9F:6E:48:67:26:06:79:A2:BF
SHA1 Fingerprint	5C:ED:E0:63:EB:7F:55:D9:9A:9B:92:69:9B:90:58:8A:65:9C:8B:81
Public Key	RSA (2048 Bits)

Required Information	
Country (C)	
State or Province (ST)	
City or Locality (L)	
Organization Name (O)	Hewlett-Packard

Optional data	
Alternative Name	
Contact Person	
Email Address	
Organizational Unit	Onboard Administrator
Surname	
Given Name	
Initials	
DN Qualifier	

Certificate-signing request attributes	
Unstructured Name	

On initial startup, Onboard Administrator generates a default self-signed SSL certificate valid for 10 years, and the certificate is issued to the name of the Onboard Administrator. Because this default certificate is self-signed, the "issued by" field is also set to the same name.

Status information

Row	Description
Cert Common Name	The Certificate Subject Common Name.

Certificate Information

Row	Description
Issued by	The certificate authority that issued the certificate
Valid from	The date from which the certificate is valid

Table Continued

Row	Description
Valid until	The date the certificate expires
Serial Number	The serial number assigned to the certificate by the certificate authority
Version	Version number of current certificate
MD5 Fingerprint	This field is a validation of authenticity and is embedded in the certificate
SHA1 Fingerprint	This field is a validation of authenticity and is embedded in the certificate
Public Key	The name of the public key.

Required Information

Row	Description
Country (C):	The two character country code that identifies the country where the Onboard Administrator is located.
State or Province (ST):	The state or province where the Onboard Administrator is located.
City or Locality (L):	The city or locality where the Onboard Administrator is located.
Organization Name (O):	The company that owns this Onboard Administrator.

Optional data

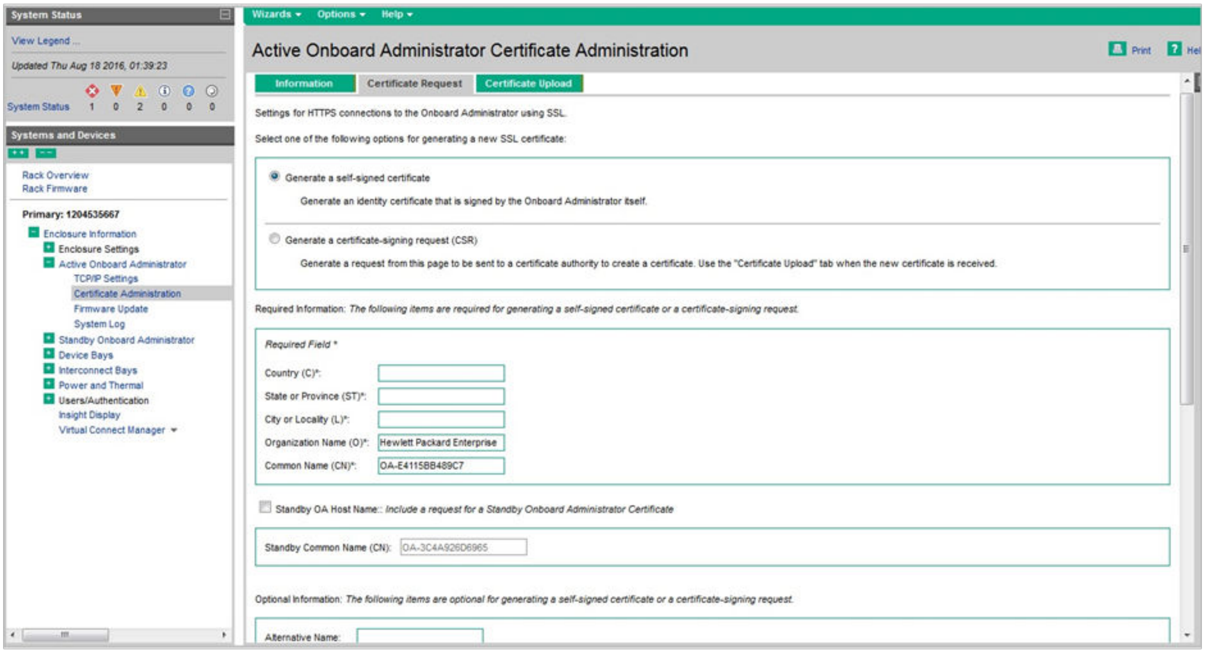
Row	Description
Alternative Name	An alternate name for the Onboard Administrator.
Contact Person	The person responsible for the Onboard Administrator.
Email Address	The email address of the person responsible for the Onboard Administrator.
Organizational Unit	The unit within the company or organization that owns the Onboard Administrator.
Surname	The surname of the person responsible for the Onboard Administrator.
Given Name	The given name of the person responsible for the Onboard Administrator.
Initials	The initials of the person responsible for the Onboard Administrator.
DN Qualifier	The distinguished name qualifier of the Onboard Administrator.

Certificate-signing request attributes

Row	Description
Unstructured Name	This is for additional information.

Certificate Request tab

The Certificate Request tab enables you to enter the information needed to generate a self-signed certificate or a standardized certificate-signing request to a certificate authority.



Active Onboard Administrator Certificate Administration

Settings for HTTPS connections to the Onboard Administrator using SSL.

Select one of the following options for generating a new SSL certificate:

● Generate a self-signed certificate

Generate an identity certificate that is signed by the Onboard Administrator itself.

○ Generate a certificate-signing request (CSR)

Generate a request from this page to be sent to a certificate authority to create a certificate. Use the "Certificate Upload" tab when the new certificate is received.

Required Information: *The following items are required for generating a self-signed certificate or a certificate-signing request.*

*Required Field **

Country (C)*:

State or Province (ST)*:

City or Locality (L)*:

Organization Name (O)*: Hewlett Packard Enterprise

Common Name (CN)*: OA-E4115BB489C7

□ Standby OA Host Name:: *Include a request for a Standby Onboard Administrator Certificate*

Standby Common Name (CN): OA-3C4A926D6965

Optional Information: *The following items are optional for generating a self-signed certificate or a certificate-signing request.*

Alternative Name:

Required information

Field	Possible values	Description
Country (C)	Must be one to two characters in length. Acceptable characters are all alphanumeric, a space, and the following punctuation marks: ' ( ) + , - . / : = ?	A valid country code that identifies the country where the Onboard Administrator is located.
State or Province (ST)	Must be 1 to 30 characters in length.	The state or province where the Onboard Administrator is located.
City or Locality (L)	Must be 1 to 50 characters in length.	The city or locality where the Onboard Administrator is located.
Organization Name (O)	Must be 1 to 60 characters in length.	The organization that owns this Onboard Administrator. When this information is used to generate a certificate signing request, the issuing certificate authority can verify that the organization requesting the certificate is legally entitled to claim ownership of the given company name or organization.
Common Name (CN)	Must be 1 to 60 characters in length. To prevent security alerts, the value of this field must match exactly the host name as it is known by the web browser. The web browser compares the host name in the resolved web address to the name that appears in the certificate. For example, if the web address in the address field is https://oa-001635.xyz.com, then the value must be oa-001635.xyz.com.	The Onboard Administrator name that appears in the browser web address field. This certificate attribute is generally referred to as the common name.

Optional information

Field	Possible values	Description
Alternative Name	Must be 0 to 511 characters in length.	An alternate name for the Onboard Administrator. The name is used for creating the X509v3 Subject Alternative Name extension attribute. The field must either be empty or contain a list of keyword:value pairs separated by commas. The valid keyword:value entries include IP:<ip address> and DNS:<domain name>.
Contact Person	Must be 0 to 60 characters in length.	The person responsible for the Onboard Administrator.
Email Address	Must be 0 to 60 characters in length.	The email address of the contact person responsible for the Onboard Administrator.
Organizational Unit	Must be 0 to 60 characters in length.	The unit within the company or organization that owns the Onboard Administrator.
Surname	Must be 0 to 60 characters in length.	The surname of the person responsible for the Onboard Administrator.
Given Name	Must be 0 to 60 characters in length.	The given name of the person responsible for the Onboard Administrator.
Initials	Must be 0 to 20 characters in length.	The initials of the person responsible for the Onboard Administrator.
DN Qualifier	Must be 0 to 60 characters in length. Acceptable characters are all alphanumeric, the space, and the following punctuation marks: ' ( ) + , - . / : = ?	The distinguished name qualifier of the Onboard Administrator.

Additional information

Field	Possible values	Description
Challenge Password	Must be 0 to 30 characters in length	The password for the certificate-signing request
Confirm Password	Must be 0 to 30 characters in length	Confirm the Challenge Password
Unstructured Name	Must be 0 to 60 characters in length	This is for additional information (for example, an unstructured name that is assigned to the Onboard Administrator)

Certificate Upload tab

To upload certificates for use in Onboard Administrator, the user must be logged in using the Administrator account.

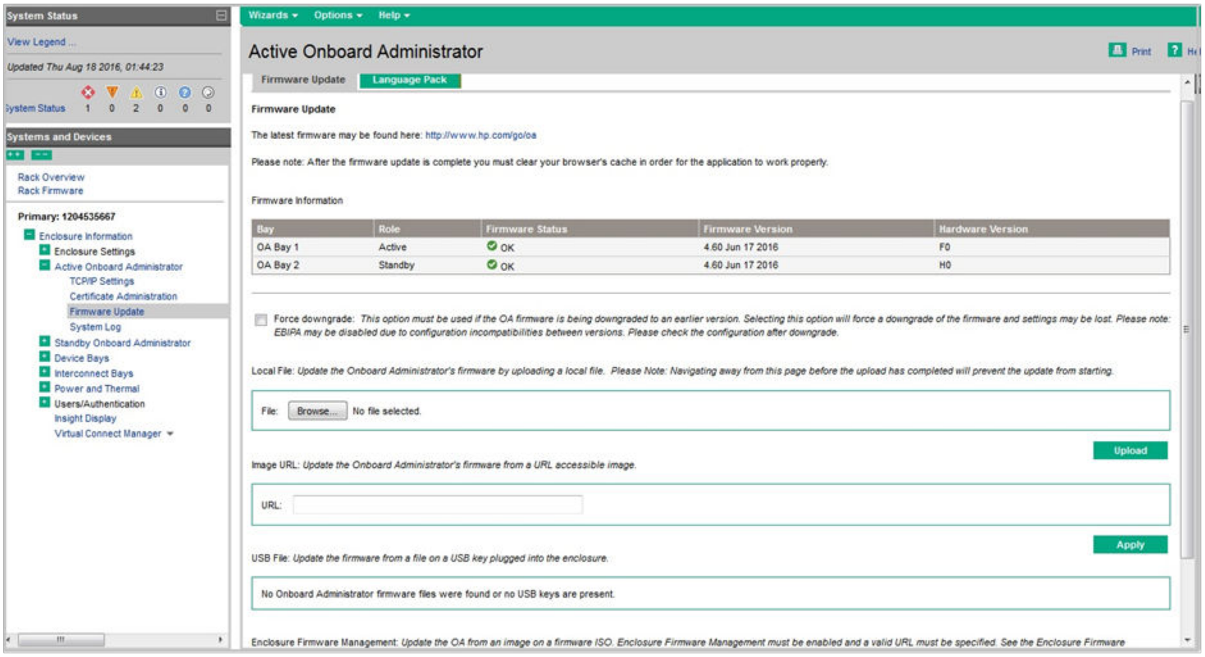
There are two methods for uploading certificates for use in Onboard Administrator:

- Paste certificate contents into the text field and click **Upload**.
- Paste the URL of the certificate into the URL field and click **Apply**.

The certificate to be uploaded must be from a certificate request sent out and signed by a certificate authority for this particular Onboard Administrator. Otherwise, the certificate fails to match the private keys used to generate the certificate request, and the certificate is rejected. Also, if the Onboard Administrator domain has been destroyed or reimported, then you must repeat the steps for generating a certificate request. It will be resigned by a certificate authority because the private keys are destroyed and recreated along with the Onboard Administrator domain.

If the new certificate is successfully accepted and installed by the Onboard Administrator, then you are automatically signed out. The HTTP server must be restarted for the new certificate to take effect.

Firmware update



Active Onboard Administrator

Firmware Update

The latest firmware may be found here: http://www.hp.com/go/oa

Please note: After the firmware update is complete you must clear your browser's cache in order for the application to work properly.

Firmware Information

Bay	Role	Firmware Status	Firmware Version	Hardware Version
OA Bay 1	Active	✓ OK	4.60 Jun 17 2016	F0
OA Bay 2	Standby	✓ OK	4.60 Jun 17 2016	H0

□ Force downgrade: *This option must be used if the OA firmware is being downgraded to an earlier version. Selecting this option will force a downgrade of the firmware and settings may be lost. Please note: EBIPA may be disabled due to configuration incompatibilities between versions. Please check the configuration after downgrade.*

Local File: *Update the Onboard Administrator's firmware by uploading a local file. Please Note: Navigating away from this page before the upload has completed will prevent the update from starting.*

File: No file selected.

Image URL: *Update the Onboard Administrator's firmware from a URL accessible image.*

URL:

USB File: *Update the firmware from a file on a USB key plugged into the enclosure.*

No Onboard Administrator firmware files were found or no USB keys are present.

Enclosure Firmware Management: *Update the OA from an image on a firmware ISO. Enclosure Firmware Management must be enabled and a valid URL must be specified. See the Enclosure Firmware*

CAUTION:

When a firmware upgrade is in process, do not disconnect or shut down the Onboard Administrator modules. Doing so could render the Onboard Administrator or server blade unusable.

The current firmware version installed on the Onboard Administrator, both Active and Standby, appears on this screen. The current Onboard Administrator hardware version also appears on this screen.

To obtain the latest firmware for your Onboard Administrator, see the **Onboard Administrator website**. For detailed information about upgrading Onboard Administrator modules in HPE BladeSystem c3000 and c7000 enclosures, see **Upgrading Onboard Administrator modules in an HPE BladeSystem Enclosure**.

Synchronize firmware

To synchronize the firmware on the Active and Standby Onboard Administrator to the same version of firmware, click **Synchronize Firmware**. A firmware image is created from the flash contents of the Onboard Administrator with the latest firmware version and is flashed to the Onboard Administrator with the oldest firmware version. The Onboard Administrator being upgraded reboots after the firmware is flashed.

To use the Synchronize Firmware feature:

- Both Onboard Administrators must be running firmware version 2.10 or later.
- If VLAN is enabled on the Active Onboard Administrator, the Standby Onboard Administrator must have firmware compatible with the VLAN feature. If the Standby Onboard Administrator has an older firmware version that does not support VLAN, you must remove the Standby Onboard Administrator and update the firmware to a compatible version from a different enclosure.

Downgrade firmware

Use the **Force Downgrade** option to force a downgrade of the Onboard Administrator to an earlier version. Selecting this option forces a downgrade of the firmware; current settings that are inapplicable to the earlier version may be lost. When the Onboard Administrator is in VC mode and IPv6 is enabled, the Virtual Connect Manager may specify a minimum expected firmware version for the Onboard Administrator. When this situation occurs, disabling Onboard Administrator IPv6 communication prior to the downgrade attempt makes it possible for VC to interoperate with older Onboard Administrator versions.

NOTE:

This feature is disabled while in the FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug.

Update firmware

△ **CAUTION:**

In FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug, an upgrade to the current version of the Onboard Administrator from a version earlier than 4.40 retains the first 21 local user accounts that were created, including any reserved accounts such as the Administrator or Virtual Connect users. The remainder of the users are deleted.

NOTE:

Updating the OA firmware from an OA version earlier than 3.50 to OA version 4.50 or later requires an intermediate update to OA 3.50 first. If you update the OA firmware from the Firmware Update screen, you must manually perform this intermediate update before updating to OA version 4.50 or later. The intermediate OA 3.50 firmware can be downloaded from the **Onboard Administrator website**.

Manual intermediate update is not required when updating the OA firmware from an FW ISO or when using the Synchronize Firmware feature from the Active Onboard Administrator Firmware Update screen.

- **Local File**

  To update firmware on the Active Onboard Administrator from a local file, browse to the firmware image file or enter the path of the firmware image file in the text box. The maximum number of characters in the file path is 256. Click **Upload**.
- **Image URL**

  To update firmware on the Active Onboard Administrator from a file located on a web server:

  1. Enter an http:// path to the firmware image file. Supported protocols are HTTP, FTP, and TFTP. The URL is formatted as: `protocol://host/path/filename`. The URL syntax for IPv6 addresses is:

     `protocol://[<ipv6 address>]/path/file`

     The maximum length of the URL is 511 characters. If your FTP server does not support anonymous logins, then you can specify a user name and password within the URL formatted as: `ftp://username:password@host/path/filename`

     NOTE:

     When using the FTP protocol, specify the image's URL path in this format, specifying a double slash (//) prior to the host/path/filename portion of the URL: ftp://user:password@//host/path/filename.

     Because of a change in behavior beginning with Onboard Administrator v4.11, if you specify a single slash (/) instead of double slashes, some FTP servers will search for the image file using your home directory as the relative root path (/home/user/path/filename). Specifying the recommended double slashes ensures that the FTP server will use the absolute path (/path/filename) to search for the image.
  2. Enter the URL, and then click **Apply**.

After clicking **Upload** or **Apply**, a window displays the progress of the firmware download. When the download completes, you are signed off the Onboard Administrator. You must sign in again.

- **USB File**

  To update firmware on the Active Onboard Administrator from an image located on a USB key, select a file from the menu, and then click **Apply**. This field appears only when a USB key is detected in the Active Onboard Administrator USB port and firmware images are present on the USB key. The maximum supported file size for USB keys formatted with FAT32 is 4GB. For SPP images greater than 4GB, use an ext2-formatted USB key.

If you initiated the firmware update, a timer appears and other users receive a dialog box informing them that the enclosure is powering down and rebooting. After the enclosure reboots, you must sign in again.

If two enclosures are attached, the firmware update process flashes the Standby Onboard Administrator first and then flashes the primary Onboard Administrator. If you are unable to connect immediately following a firmware update, wait 30 seconds for the enclosure to become available on the network.

Enclosure Firmware Management

Update the Onboard Administrator from an image on a firmware ISO. Enclosure Firmware Management must be enabled, and a valid URL must be specified in the Enclosure Firmware Management settings. For more information, see **Enclosure Firmware Management**.

To update the Onboard Administrator, click **Apply**.

Installing a previous version

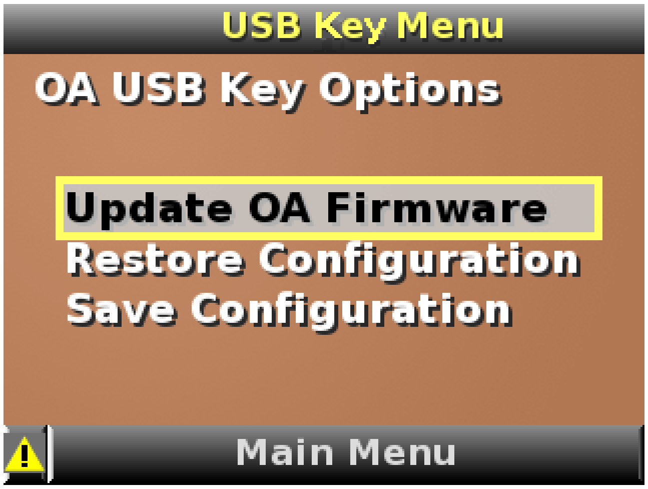
To install a previous version of the firmware, select the **Force downgrade** box from the Firmware Information section of the screen. Select the firmware file by browsing locally or by locating a URL using the input boxes. If you downgrade Onboard Administrator firmware to 2.31 or lower, you will lose any Directory groups beyond the first five groups. Onboard Administrator versions higher than 2.31 support 30 groups, while earlier versions only support five groups. After the first five groups, you will lock out additional directory users.

To downgrade to a previous version with IPv6 enabled, VC requires an Onboard Administrator minimum firmware version. To proceed with the downgrade, disable IPv6 and try again.

Upgrading Onboard Administrator modules in an HPE BladeSystem Enclosure

1. Insert the OA upgrade module into the enclosure.
   - For a c7000 Enclosure that contains two OA modules, replace the original Standby OA with the OA upgrade module.
   - For a c7000 Enclosure that contains only one OA module, insert the OA upgrade module into the empty OA module slot.
   - For a c3000 Enclosure, which contains two OA modules, ensure that the OA module to be replaced is in standby mode. Replace the Standby OA module with the OA upgrade module.
2. Update the firmware on the Active OA to the same firmware version as already running on the Active OA.

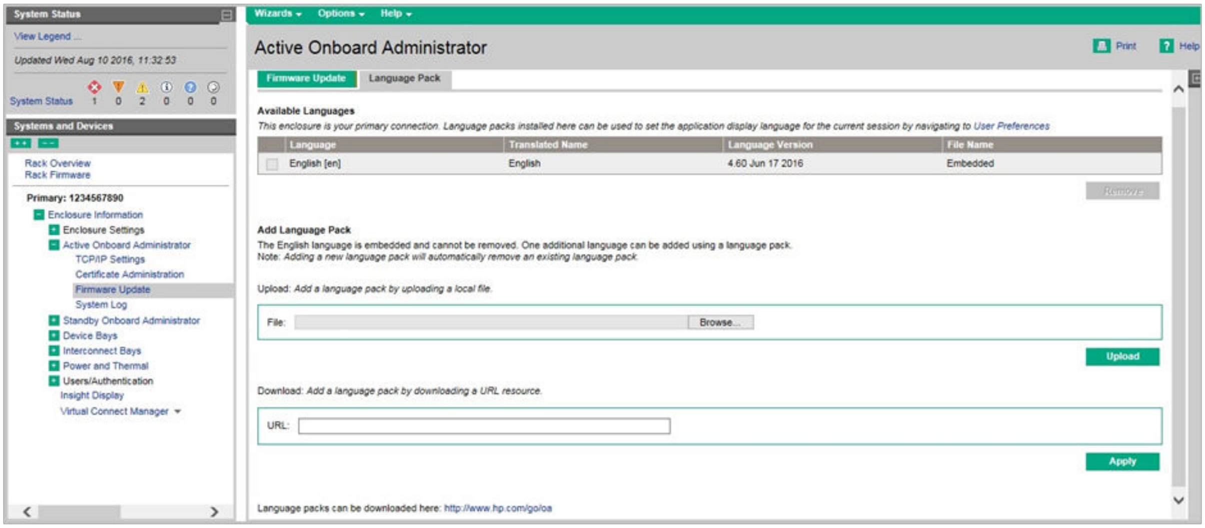
   To perform this step, update the firmware from the enclosure LCD with a FAT32-formatted USB key that contains the OA firmware bin file and is plugged into the Active OA (see the following menu example). This ensures that the OA upgrade module is running the same firmware version. This also results in synchronizing the enclosure configuration to the OA upgrade module.



3. For a c7000 Enclosure that contains two OA modules, ensure that the remaining original OA module is in standby mode. Remove the remaining original OA module and insert a second OA upgrade module. If the enclosure has only one OA module, skip to the next step.
    a. Ensure that the second OA upgrade module was automatically synchronized to the other upgrade OA module. To do this, examine the **Rack Firmware screen** and compare the OA firmware versions in that enclosure.
    b. If the firmware versions do not match, update the Active OA firmware. This synchronizes the enclosure configuration to the Active OA.
4. For a c7000 Enclosure that has only one OA module, after performing steps 1 and 2, remove the original OA module. This completes the upgrade process for the enclosure.

Active Onboard Administrator Language Pack tab

This screen displays a list of installed language packs. The English language is embedded and cannot be removed. Only one additional language can be added using a language pack. Adding a new language pack automatically removes an existing language pack. To remove an existing language pack, select the check box and click **Remove**.



Updated Wed Aug 10 2016, 11:32:53

Primary: 1234567890

Active Onboard Administrator

Available Languages

This enclosure is your primary connection. Language packs installed here can be used to set the application display language for the current session by navigating to User Preferences

	Language	Translated Name	Language Version	File Name
□	English [en]	English	4.60 Jun 17 2016	Embedded

Add Language Pack

The English language is embedded and cannot be removed. One additional language can be added using a language pack.
Note: *Adding a new language pack will automatically remove an existing language pack*

Upload: *Add a language pack by uploading a local file.*

File:

Download: *Add a language pack by downloading a URL resource.*

URL:

Language packs can be downloaded here: http://www.hp.com/go/oa

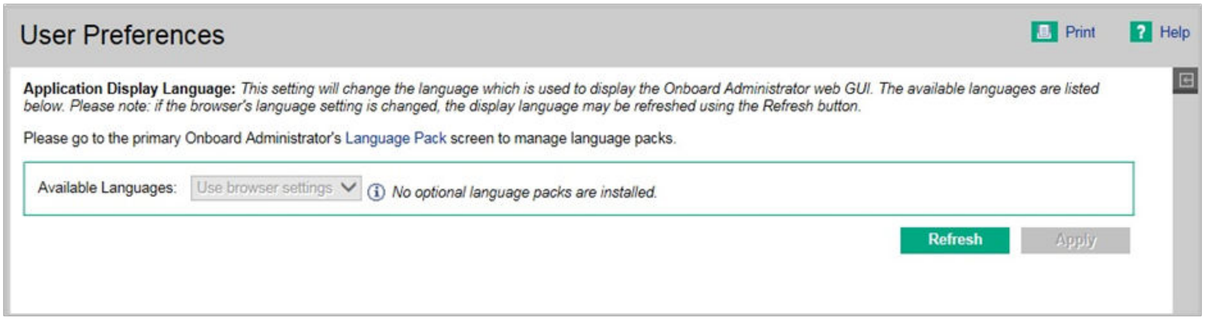
To add a language pack, you have two options:

- **Upload**

To add a language pack from a local file, browse to the language pack file or enter the path of the language pack file in the textbox. The maximum number of characters in the file path is 256. Click **Upload**.

- **Download**

  To add a language pack from a file located on a web server, enter an http:// path to the firmware image file. The maximum number of characters in the file path is 255. Supported protocols are HTTP, FTP, and TFTP. The URL is formatted as: `protocol://host/path/filename`. Enter the URL, and then click **Apply**. After clicking **Upload** or **Apply**, a window displays the progress of the firmware download. When the download completes, a popup window displays the language pack as added.



Application Display Language: *This setting will change the language which is used to display the Onboard Administrator web GUI. The available languages are listed below. Please note: if the browser's language setting is changed, the display language may be refreshed using the Refresh button.*

Please go to the primary Onboard Administrator's Language Pack screen to manage language packs.

Available Languages: Use browser settings *No optional language packs are installed.*

After installing a language pack, you can display the language on the Onboard Administrator GUI using your current browser's language preference option (preferred) or the Onboard Administrator User Preferences options:

- To use your browser's settings for language preferences, add the language to the top of the browser's preferred languages list, and then use the Onboard Administrator**User Preferences** screen to select "Use browser settings."

  This method is preferred because the setting applies to any subsequent Onboard Administrator GUI sessions using this browser and to sessions with other Onboard Administrators, providing that the same language is installed on the other Onboard Administrator GUIs and their User Preferences setting is the default "Use browser settings."
- To use the Onboard Administrator **User Preferences** screen to display a specific language, select the language from the User Preferences list of available languages and click **Apply**.

  This setting overrides the browser's current language preference setting and persists with subsequent GUI sessions connecting to the same Onboard Administrator. However, the setting does not apply for GUI sessions with other Onboard Administrators. (The setting relies on a cookie that is valid only for the current Onboard Administrator IP address. If the IP address changes, the setting must be applied again from the new address.) To ensure that all pages of the Onboard Administrator's GUI inherit the selected language, click **Refresh** at the bottom of the User Preferences screen.

Each of these settings is browser-specific. For example, a language setting for Internet Explorer does not affect the setting for Firefox. You do not have to use the same method on all browsers. After configuring your preferred language, to make the setting take effect, you may need to refresh or reload the web page.

NOTE:

If the display language does not load properly, clear the browser cache and refresh the application by refreshing or reloading the browser.

When logged in to a primary enclosure with linked enclosures, ensure that all linked enclosures have a compatible version of the language pack installed.

System log

The System Log displays logged information of events within the Onboard Administrator.

Events are logged from the top of the list to the bottom, with the most recent logged event appearing at the top of the list. The system log can be scrolled utilizing the scroll bar on the right side of the log screen (if the log is larger than the display box).

The log has a maximum capacity of approximately 18 KB. When the log reaches that capacity, it automatically deletes the oldest logged event first (first in, first out).

To clear the list of all logged events in the system log, click **Clear Log** on the lower-right below the system log display.

Extended system log

The Onboard Administrator automatically saves 300 KB of the latest system log history. This extended system log is retained during a reboot, restart, and power off, if those actions are performed gracefully. In optimal circumstances, the Onboard Administrator automatically saves up to 400 KB of the latest system log history. If power to the Onboard Administrator is removed unexpectedly or the Onboard Administrator is removed from the enclosure without a proper shutdown, the latest (unsaved) portions of the extended system log might be lost.

To view the extended system log, use the CLI `SHOW SYSLOG HISTORY` command.

Remote system logging

You can use remote system logging to send Onboard Administrator syslog messages to a remote server on the network for persistent storage. To set up this feature, use the **Log Options tab**.

Log Options tab

This screen enables you to send system log messages to a remote server on the network for persistent storage. By default, the local system log is enabled. To manage the system log settings, you must be an Administrator or Operator with OA bay permissions.

The syslog messages are sent from Onboard Administrator using the UDP protocol on a port that can be specified by the user. The default remote syslog port is 514.

Onboard Administrators Remote System Logging feature follows the guidelines in **RFC3164**.

In most Linux systems, remote system logging can be enabled by starting syslog with the "-r" option. The remote syslog port must also be opened in the firewall. For additional information, see documentation for your particular distribution. Windows® operating systems do not have native support for remote system logging. Any application that listens on UDP port 514 or the specified syslog port can receive remote system log messages from the Onboard Administrator.

To send system log messages to a remote host, select the **Enable remote system logging** check box. Specify the server and port.

When configured, the Onboard Administrator remote system logging feature can be tested using the GUI Test button or using the CLI `TEST SYSLOG` command.

Field	Possible value	Description
Syslog Server Address	• IPv4 address—###.###.###.### where ### ranges from 0 to 255 • IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. • DNS name—1 to 64 characters including all alphanumeric characters and the dash (-)	An IPv4 address, IPv6 address, or the DNS name of the remote host [1]
Port	An integer between 1 and 65535	The IP port of the remote host.

[1] *Use an IPv6 address as the remote system log server.*

To send a test message to the remote host address and to the local system log, click **Test Remote Log.** To use this function, you must enable remote system logging.

To save the settings, click **Apply.**

NOTE:

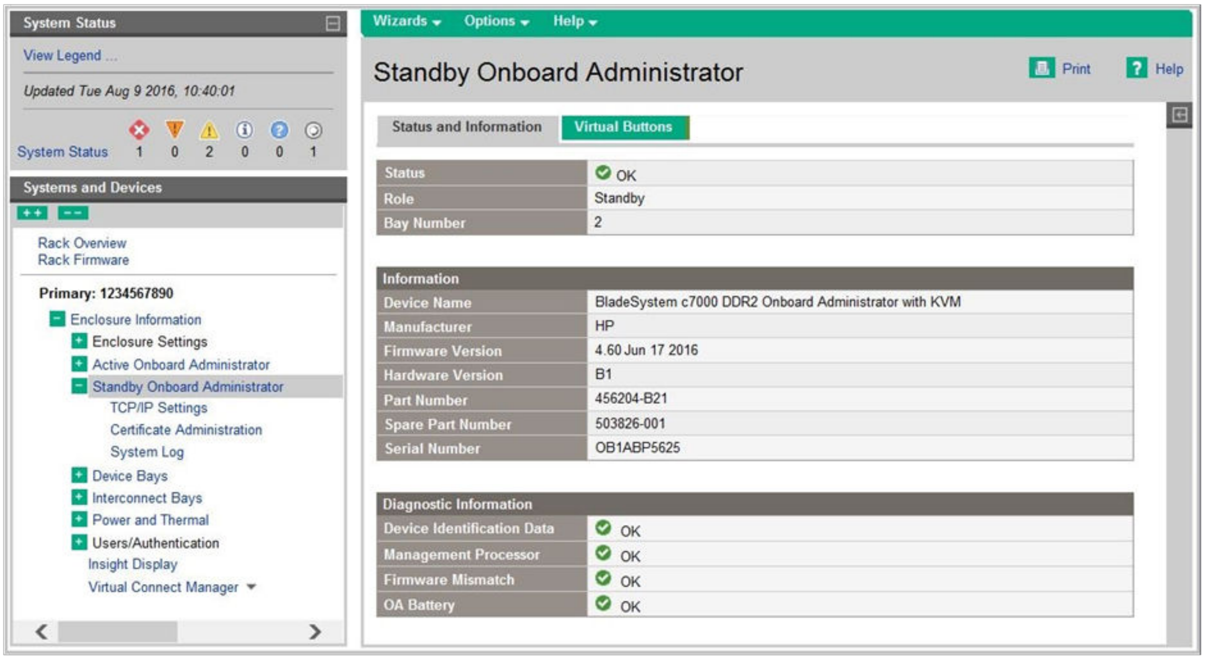
If the OA is in a dual stack IPv4/IPv6 network, the remote syslog client software needs to be configured to listen to both IPv4 and Ipv6 addresses.

Standby Onboard Administrator Module

Standby Onboard Administrator screen

When a second Onboard Administrator is placed in the enclosure, it becomes the Standby Onboard Administrator. The Standby Onboard Administrator is normally placed in the available Onboard Administrator tray in the rear of the enclosure. By selecting the Active to Standby screen, you can force a transition within the Onboard Administrator user interface to make the active Onboard Administrator become the Standby Onboard Administrator.

For an Active/Standby relationship, the two Onboard Administrator modules must have the same firmware version installed. If the firmware versions are not identical, the Insight Display and the main status screen of the Onboard Administrator identifies this error and alerts the user through SNMP if enabled.



Standby Onboard Administrator

Status	✓ OK
Role	Standby
Bay Number	2

Information	
Device Name	BladeSystem c7000 DDR2 Onboard Administrator with KVM
Manufacturer	HP
Firmware Version	4.60 Jun 17 2016
Hardware Version	B1
Part Number	456204-B21
Spare Part Number	503826-001
Serial Number	OB1ABP5625

Diagnostic Information	
Device Identification Data	✓ OK
Management Processor	✓ OK
Firmware Mismatch	✓ OK
OA Battery	✓ OK

If using two Onboard Administrators, each Onboard Administrator has a unique IP address. See the Insight Display to obtain the IP addresses for the Active and Standby Onboard Administrators and write them down. When looking at the enclosure from the rear, the bay on the left is bay 1, while the bay on the right is bay 2. When the Active Onboard Administrator transitions to the Standby Onboard Administrator, the DNS host name and IP addresses remains the same. To connect to the new Active Onboard Administrator, you must completely close your browser and connect to the host name or IP address of the former Standby Onboard Administrator.

Status, Information, and Virtual Buttons tabs

The information contained under the Status, Information, and Virtual Buttons tabs is the same as it is for an Active Onboard Administrator. For information on these tabs, see **Active Onboard Administrator screen** .

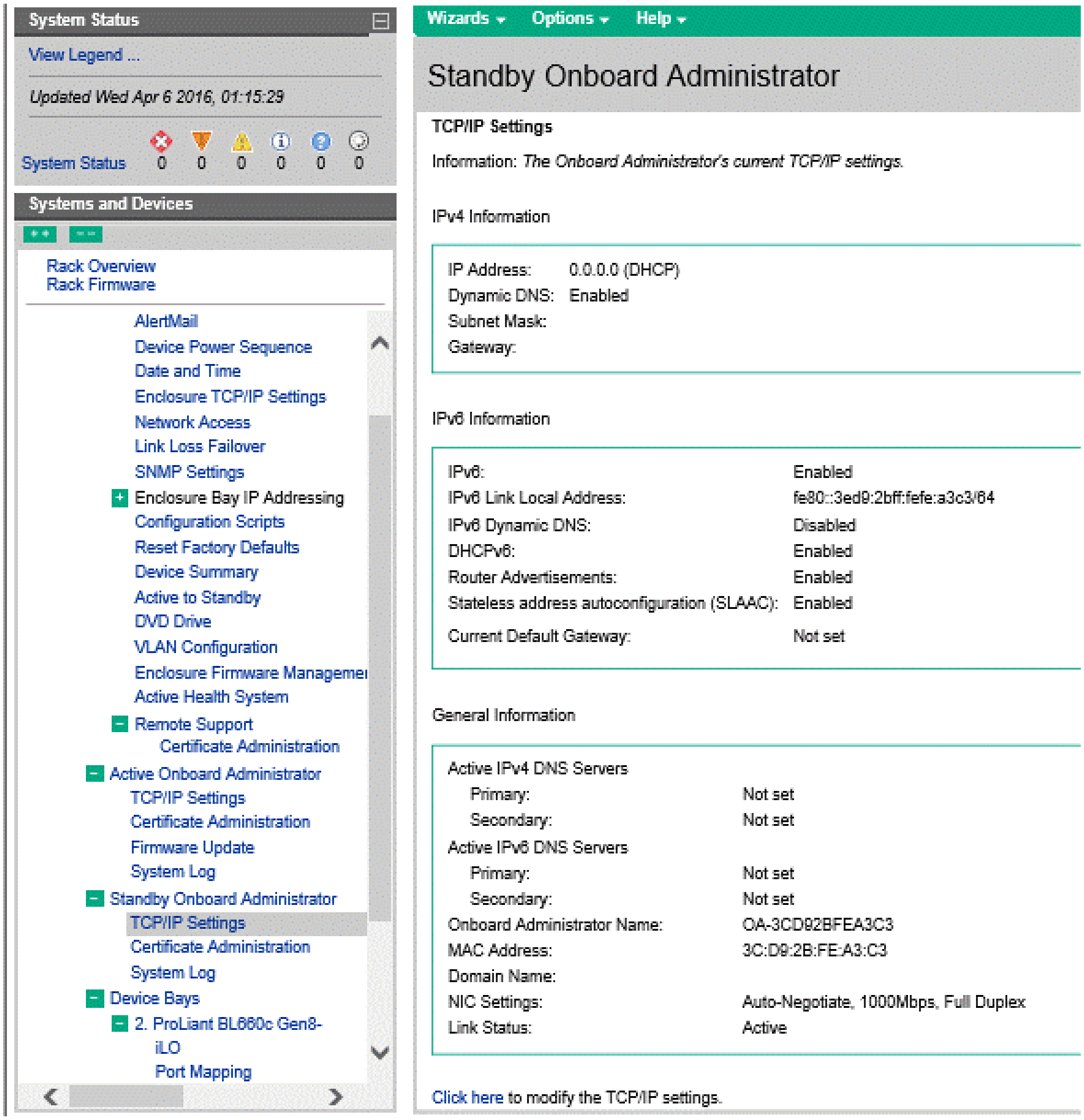
When a network cable is attached to, or removed from, the Standby Onboard Administrator, an SNMP trap (if enabled) identifying the corresponding network link status change is sent by the Active Onboard Administrator.

Standby Onboard Administrator Virtual Buttons tab

Click **Reset** to reset the Onboard Administrator. A confirmation screen appears, asking if you are sure that you want to perform the action and that you are signed out and disconnected from the Onboard Administrator. Click **OK** to proceed, or click **Cancel** to exit without a change.

Click **Toggle On/Off** to change the Onboard Administrator module UID light. This identifies a particular Onboard Administrator when there are more than one.

TCP/IP Settings for Standby OA viewed from the Active OA



Standby Onboard Administrator

TCP/IP Settings

Information: *The Onboard Administrator's current TCP/IP settings.*

IPv4 Information

IP Address: 0.0.0.0 (DHCP)
Dynamic DNS: Enabled
Subnet Mask:
Gateway:

IPv6 Information

IPv6: Enabled
IPv6 Link Local Address: fe80::3ed9:2bff:fefe:a3c3/64
IPv6 Dynamic DNS: Disabled
DHCPv6: Enabled
Router Advertisements: Enabled
Stateless address autoconfiguration (SLAAC): Enabled
Current Default Gateway: Not set

General Information

Active IPv4 DNS Servers
Primary: Not set
Secondary: Not set
Active IPv6 DNS Servers
Primary: Not set
Secondary: Not set
Onboard Administrator Name: OA-3CD92BFEA3C3
MAC Address: 3C:D9:2B:FE:A3:C3
Domain Name:
NIC Settings: Auto-Negotiate, 1000Mbps, Full Duplex
Link Status: Active

Click here to modify the TCP/IP settings.

This screen, as seen from the Active Onboard Administrator GUI, displays the current enclosure TCP/IP settings for the Standby Onboard Administrator.

For information about the TCP/IP settings that appear on this screen, see **Active Onboard Administrator TCP/IP Settings screen**.

To modify the TCP/IP settings, select **Click here** . For information about the TCP/IP settings that you can modify, see **Enclosure TCP/IP Settings**.

Standby TCP/IP settings viewed from the Standby Onboard Administrator GUI

The TCP/IP Settings screen viewed from the Standby Onboard Administrator GUI includes four tabs:

- IPv4 Settings
- IPv6 Settings
- NIC Options
- Advanced Settings

These tabs display the settings seen in the previous screen example but also allow you to modify many of the settings directly.

The IPv4 Settings and IPv6 Settings tabs allow you to modify most of the settings modifiable from the corresponding tabs on the Active Onboard Administrator GUI's Enclosure TCP/IP Settings screen. The exceptions are described in the sections that follow. The NIC Options and Advanced Settings tabs allow you to modify the same settings that can be modified from the corresponding tabs on the Active Onboard Administrator GUI's Enclosure TCP/IP Settings screen.

IPv4 Settings exceptions

You cannot modify the **Enclosure IP Mode** setting from the Standby Onboard Administrator GUI. Modify it from the Active Onboard Administrator GUI's Enclosure TCP/IP Settings **IPv4 Settings tab**.

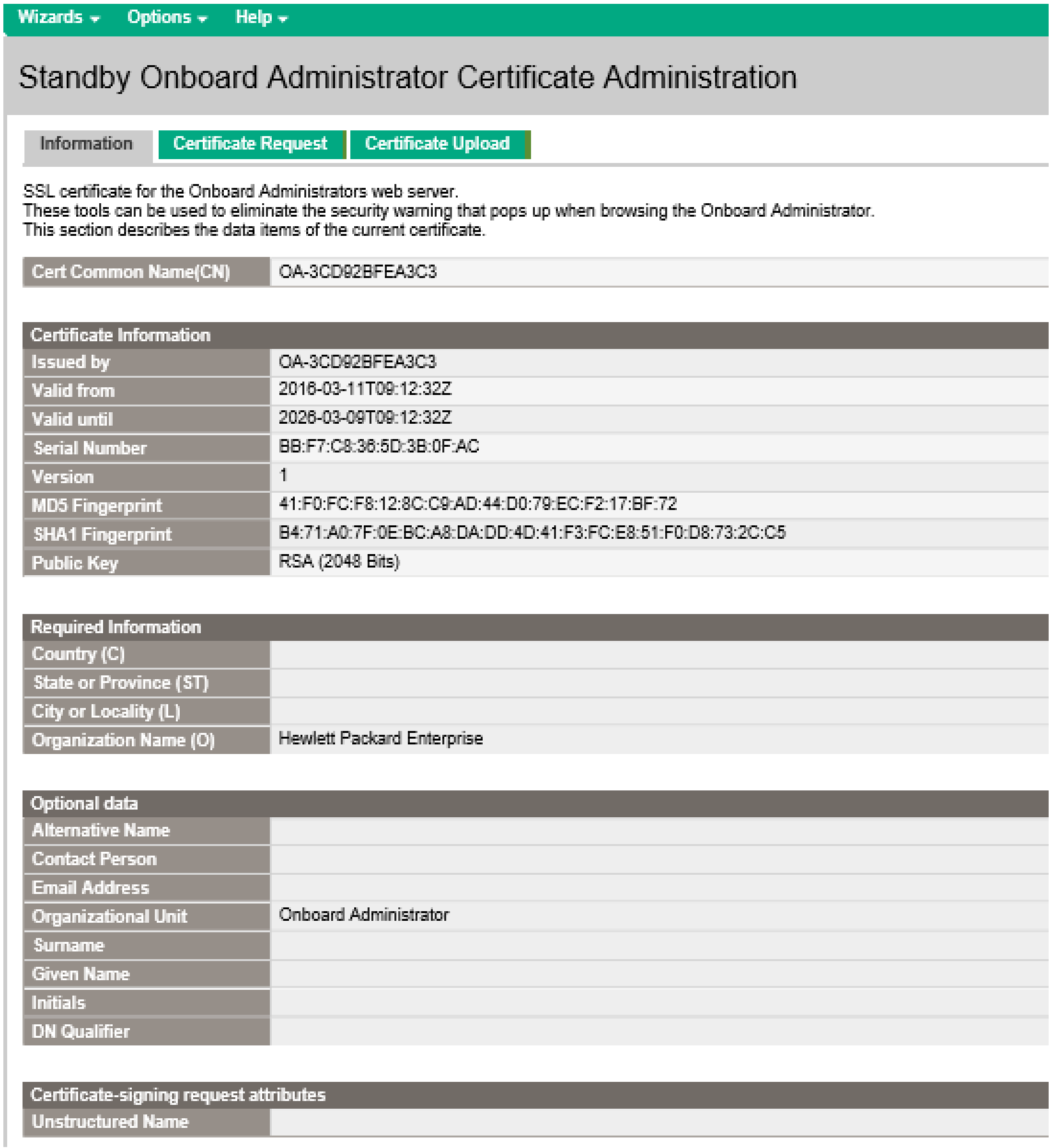
IPv6 Settings exceptions

You cannot modify the following settings from the Standby Onboard Administrator GUI. Modify them using the Active Onboard Administrator GUI's Enclosure TCP/IP Settings **IPv6 Settings tab**.

- **Enclosure IP Mode**
- **Enable IPv6**
- **Enable Router Advertisements**
- **Enable SLAAC**
- **Enable DHCPv6**

Standby Onboard Administrator Certificate Administration Information tab

This screen displays the detailed information of the SSL certificate currently in use by the Onboard Administrator. An SSL certificate is used to certify the identity of Onboard Administrator and is required by the underlying HTTP server to establish a secure (encrypted) communications channel with the client web browser.



Standby Onboard Administrator Certificate Administration

SSL certificate for the Onboard Administrators web server.
These tools can be used to eliminate the security warning that pops up when browsing the Onboard Administrator.
This section describes the data items of the current certificate.

Cert Common Name(CN)	OA-3CD92BFEA3C3

Certificate Information	
Issued by	OA-3CD92BFEA3C3
Valid from	2016-03-11T09:12:32Z
Valid until	2026-03-09T09:12:32Z
Serial Number	BB:F7:C8:36:5D:3B:0F:AC
Version	1
MD5 Fingerprint	41:F0:FC:F8:12:8C:C9:AD:44:D0:79:EC:F2:17:BF:72
SHA1 Fingerprint	B4:71:A0:7F:0E:BC:A8:DA:DD:4D:41:F3:FC:E8:51:F0:D8:73:2C:C5
Public Key	RSA (2048 Bits)

Required Information	
Country (C)	
State or Province (ST)	
City or Locality (L)	
Organization Name (O)	Hewlett Packard Enterprise

Optional data	
Alternative Name	
Contact Person	
Email Address	
Organizational Unit	Onboard Administrator
Surname	
Given Name	
Initials	
DN Qualifier	

Certificate-signing request attributes	
Unstructured Name	

On initial startup, Onboard Administrator generates a default self-signed SSL certificate valid for 10 years, and the certificate is issued to the name of the Onboard Administrator. Because this default certificate is self-signed, the "issued by" field is also set to the same name.

Status information

Row	Description
Cert Common Name	The Certificate Subject Common Name.

Certificate Information

Row	Description
Issued by	The certificate authority that issued the certificate
Valid from	The date from which the certificate is valid

Table Continued

Row	Description
Valid until	The date the certificate expires
Serial Number	The serial number assigned to the certificate by the certificate authority
Version	Version number of current certificate
MD5 Fingerprint	This field is a validation of authenticity and is embedded in the certificate
SHA1 Fingerprint	This field is a validation of authenticity and is embedded in the certificate
Public Key	The name of the public key.

Required Information

Row	Description
Country (C):	The two character country code that identifies the country where the Onboard Administrator is located.
State or Province (ST):	The state or province where the Onboard Administrator is located.
City or Locality (L):	The city or locality where the Onboard Administrator is located.
Organization Name (O):	The company that owns this Onboard Administrator.

Optional data

Row	Description
Alternative Name	An alternate name for the Onboard Administrator.
Contact Person	The person responsible for the Onboard Administrator.
Email Address	The email address of the person responsible for the Onboard Administrator.
Organizational Unit	The unit within the company or organization that owns the Onboard Administrator.
Surname	The surname of the person responsible for the Onboard Administrator.
Given Name	The given name of the person responsible for the Onboard Administrator.
Initials	The initials of the person responsible for the Onboard Administrator.
DN Qualifier	The distinguished name qualifier of the Onboard Administrator.

Certificate-signing request attributes

Row	Description
Unstructured Name	This is for additional information.

Standby Certificate Request tab

The Standby Certificate Request tab enables you to enter the information needed to generate a self-signed certificate or a standardized certificate-signing request to a certificate authority.

Required Information

Field	Possible values	Description
Country (C)	Must be one to two characters in length. Acceptable characters are all alphanumeric, a space, and the following punctuation marks: ' ( ) + , - . / : = ?	A valid country code that identifies the country where the Onboard Administrator is located.
State or Province (ST)	Must be 1 to 30 characters in length.	The state or province where the Onboard Administrator is located.
City or Locality (L)	Must be 1 to 50 characters in length.	The city or locality where the Onboard Administrator is located.
Organization Name (O)	Must be 1 to 60 characters in length.	The organization that owns this Onboard Administrator. When this information is used to generate a certificate signing request, the issuing certificate authority can verify that the organization requesting the certificate is legally entitled to claim ownership of the given company name or organization.
Common Name (CN)	Must be 1 to 60 characters in length. To prevent security alerts, the value of this field must match exactly the host name as it is known by the web browser. The web browser compares the host name in the resolved web address to the name that appears in the certificate. For example, if the web address in the address field is https://oa-001635.xyz.com, then the value must be oa-001635.xyz.com.	The Onboard Administrator name that appears in the browser web address field. This certificate attribute is generally referred to as the common name.

To include a request for an Active Onboard Administrator certificate, select **Active OA Host Name**. Enter the information in the **Active Common Name (CN)** field, which must be 1 to 60 characters in length.

Optional information

Field	Possible values	Description
Alternative Name	Must be 0 to 511 characters in length.	An alternate name for the Onboard Administrator. The name is used for creating the X509v3 Subject Alternative Name extension attribute. The field must either be empty or contain a list of keyword:value pairs separated by commas. The valid keyword:value entries include IP:<ip address> and DNS:<domain name>.
Contact Person	Must be 0 to 60 characters in length.	The person responsible for the Onboard Administrator.
Email Address	Must be 0 to 60 characters in length.	The email address of the contact person responsible for the Onboard Administrator.
Organizational Unit	Must be 0 to 60 characters in length.	The unit within the company or organization that owns the Onboard Administrator.

Table Continued

Field	Possible values	Description
Surname	Must be 0 to 60 characters in length.	The surname of the person responsible for the Onboard Administrator.
Given Name	Must be 0 to 60 characters in length.	The given name of the person responsible for the Onboard Administrator.
Initials	Must be 0 to 20 characters in length.	The initials of the person responsible for the Onboard Administrator.
DN Qualifier	Must be 0 to 60 characters in length. Acceptable characters are all alphanumeric, the space, and the following punctuation marks: ' ( ) + , - . / : = ?	The distinguished name qualifier of the Onboard Administrator.

Certificate-signing request attributes

Field	Possible values	Description
Challenge Password	Must be 0 to 30 characters in length	The password for the certificate-signing request
Confirm Password	Must be 0 to 30 characters in length	Confirm the Challenge Password
Unstructured Name	Must be 0 to 60 characters in length	This is for additional information (for example, an unstructured name that is assigned to the Onboard Administrator)

To generate a self-signed certificate or a standardized certificate-signing request, click **Apply**.

Standardized certificate-signing request

This screen displays a standardized certificate signing request generated by the Onboard Administrator. The content of the request in the text box may be sent to a certificate authority of your choice for signing. Once signed and returned from the certificate authority, the certificate can be uploaded under the "Certificate Upload" tab.

If a static IP address is configured for Onboard Administrator when this certificate request is generated, the certificate request will be issued to the static IP address. Otherwise, it is issued to the dynamic DNS name of the Onboard Administrator. The certificate, by default, requests a valid duration of 10 years (this value is currently not configurable).

When submitting the request to the certificate authority, be sure to:

- Use the Onboard Administrator URL for the server.
- Request the certificate be generated in the RAW format.
- Include the Begin and End certificate lines.

Standby Certificate Upload tab

There are two methods for uploading certificates for use in Onboard Administrator:

- Paste certificate contents into the text field and click **Upload**.
- Paste the URL of the certificate into the URL field and click **Apply**.

The certificate to be uploaded must be from a certificate request sent out and signed by a certificate authority for this particular Onboard Administrator. Otherwise, the certificate fails to match the private keys used to generate the certificate request, and the certificate is rejected. Also, if the Onboard Administrator domain has been destroyed or reimported, then you must repeat the steps for generating a certificate request. It will be resigned by a certificate authority because the private keys are destroyed and recreated along with the Onboard Administrator domain.

If the new certificate is successfully accepted and installed by the Onboard Administrator, then you are automatically signed out. The HTTP server must be restarted for the new certificate to take effect.

For more information on the System Log subcategory, see **System Log**.

System Log for Standby Onboard Administrator

The System Log displays logged information of events within the Onboard Administrator.

Events are logged from the top of the list to the bottom, with the most recent logged event appearing at the bottom of the list. If the list is longer than the display box, you can scroll using the scroll bar on the right side of the log screen.

When the log reaches maximum capacity, it automatically deletes the oldest logged event first (first in, first out).

To clear the list of all logged events, click **Clear Log** (below the system log display).

Standby to Active

To force the Standby Onboard Administrator to Active, click **Transition Standby to Active.** A confirmation screen appears, asking if you are sure that you want to perform the action. To proceed, click **OK.** To exit without a change, click **Cancel**.

This functionality is only available when you are signed into the Standby Onboard Administrator.

You can also force the Standby Onboard Administrator to Active by using the FORCE TAKEOVER CLI command.

The transition times from Standby to Active and Active to Standby vary, depending on the configuration, enclosure population, and various other factors. Removing the previously Active Onboard Administrator early in the transition process forces the transition time of the Standby to Active to increase.

Device bays

Device Bay Summary

In the Systems and Devices menu, the Device Bays category lists all blades in the enclosure. Selecting the Device Bays from the menu, the device list appears with a grid showing the status of each blade in the enclosure.

The check box in the first column on the top row toggles all check boxes for all blades in the enclosure, which can be used to cycle power to all server blades in the enclosure. Optionally, you can use individual check boxes to select a specific blade. After selecting blades, choose Virtual Power, UID State, One Time Boot, DVD, or Enclosure Firmware Management from the menus to perform the appropriate action. Virtual commands are not applicable to storage blades.

Device List

Column	Description
Check box	Select bays by selecting the check box for the blades you want to apply the Virtual Power, UID State, One Time Boot, DVD, or Firmware Management action.
Bay	The device bay within the enclosure.
Status	The overall status of the device. Possible values are OK and Enclosure Firmware Management.

Table Continued

Column	Description
UID	The status of the UID on the device. Possible values are On (blue), Off (gray) or Blink. When the UID light is in a blink state, a critical operation is being performed on the device and you must not interrupt the operation.
Power State	The power state of the device. Possible values are On or Off.
iLO IP Address	The IP address of the iLO within the server blade. Not applicable for storage blades. To connect to the iLO, click the IP address link. To see all iLO IP address links available, click the down arrow button to the right of the iLO IP address. A popup displays the web address links that you can use to connect to the iLO. If FQDN link support is enabled and certain DNS configuration requirements are met, an FQDN-based web address is the default selection. For information about enabling FQDN link support, see the **Network Access** page.
iLO Name	The DNS name of the iLO within the server blade. Not applicable for storage blades.
iLO DVD Status	The status of the DVD connection to the server blade. Possible values are Connected, Disconnected, or Unknown. A status of Incompatible Firmware indicates that the DVD feature is not supported with the iLO firmware installed on the device. A status of Unknown indicates there is an iLO connectivity problem.

Information on this page is current as of the last download. To view updated information, click **Refresh**.

UID State

The UID State dropdown menu is used to set the UID light on the blades. Turning on the UID light aids in locating a specific blade within an enclosure. The UID lights can be turned on or off one at a time or as groups, depending on the check boxes.

Virtual Power

Virtual power commands do not apply to partner blades.

Button	Description
Momentary Press	This button mimics a physical momentary press of the power button on the server blade. Clicking this button powers the server blade on or off gracefully.
Press and Hold	This button mimics a physical press and hold of the power button on the server blade. Clicking this button forces the server blade to shut power off without regard for first shutting down the OS before turning power off. This option is not available when the server blade is off.
Cold Boot	Clicking this button immediately removes power from the system. This option is not available when the server blade is off.
Reset	Clicking this button performs a system reset. This option is not available when the server blade is off.

One Time Boot

If Secure Boot is in effect on the blade in a selected bay, this operation cannot be performed from the Onboard Administrator GUI or CLI. It can be performed only from the device configured in BIOS by the Administrator.

If you specify one time boot settings, the settings are valid only for the next reboot of the server blade. After the boot is complete, the server blade uses the default settings for subsequent reboots.

Option	Description
No one time Boot	Forces the server blade to clear the one time boot settings.
Diskette Drive (A:)	Forces the server blade to reboot to the diskette drive. Be sure the diskette drive is attached to the server blade before selecting this option.
CD-ROM	Forces the server blade to reboot to the CD-ROM drive. Be sure the CD-ROM drive is attached to the server blade before selecting this option.
Hard Drive C:	Forces the server blade to reboot to the hard disk.
RBSU	Forces the server blade to boot to the ROM-Based Setup Utility.
PXE NIC	Forces the server blade to boot to PXE NIC.
USB	Forces the server blade to boot to USB.
Embedded UEFI Shell	Forces the server blade to boot to Embedded UEFI Shell. This option is grayed out if multiple servers are selected or if the selected server is not a UEFI-capable server.
UEFI Target	Forces the server blade to boot to UEFI Target device. This operation can be performed only on one server, after the selection of a server. This option is grayed out if multiple servers are selected, or if the selected server is not a UEFI-capable server or is a UEFI-capable server in Legacy Boot BIOS Mode.

DVD

The DVD menu enables you to connect or disconnect the shared DVD drive by selecting **Connect to Enclosure DVD** or **Disconnect DVD Hardware**. You can connect the shared DVD drive to multiple server blades. After you connect the shared DVD, the Virtual Power menu can be used to reboot the selected server blades in the list. If multiple media disks are required for an installation, you might need to disconnect and reconnect for every server when the new media disk is inserted in the DVD drive.

When a USB key is detected in the Active Onboard Administrator USB port and ISO images are present, they appear on the DVD menu. Select the server blades you want to deploy an ISO image to, and then select the ISO image from the menu. The ISO image deploys.

Enclosure Firmware Management

Manual discovery of one or more servers can be initiated to simplify the collection of the existing firmware versions.

After initiating a manual firmware discovery, the Manual Discovery Device Bay Selection screen appears. Select one or more device bays on which to perform the discovery, or select the **Discover All Servers** check box to select all servers for the discovery. By default, all device bays and the Discover All Servers check box are selected.

If Secure Boot is configured on a server blade, you cannot select the associated bay (a padlock icon is displayed). Secure Boot mode restricts users from performing manual discovery from the Onboard Administrator GUI or CLI. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

To start the discovery process on the selected servers, click **Start Manual Discovery**.

A manual update of one or more servers to the designated firmware image versions can be initiated. To initiate a firmware update on one or more servers, click **Manual Update**.

After initiating a manual firmware update the Manual Update Device Bay Selection screen appears. Select one or more device bays on which to perform the update, or select the **Update All Servers** check box to select all servers for the update. By default, all device bays and the **Discover All Servers** check box are selected.

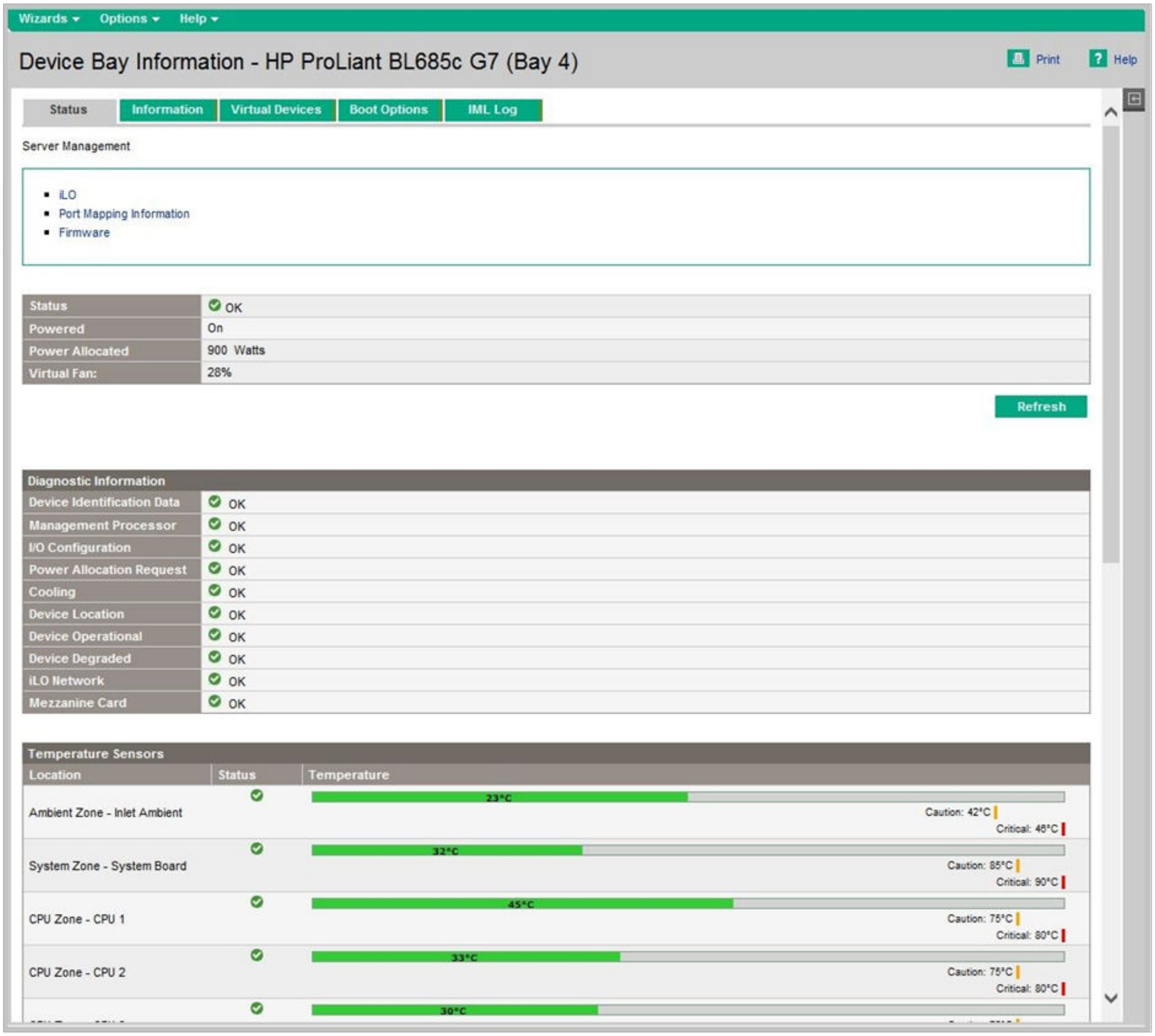
If Secure Boot is configured on a server blade, you cannot select the associated bay (a padlock icon is displayed). Secure Boot mode restricts users from performing a manual update from the Onboard Administrator GUI or CLI. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

To start the update process on the selected servers, click **Start Manual Update**.

Device Bay Status tab

Selecting a specific blade within the enclosure opens the Device Bay Information screen for Bay xx, where xx is the bay selected. This screen provides tabs for Status, Information, Virtual Devices, Boot Options, and IML Log.

The Server Management section of the page contains links to aid the management of the server blade in the device bay.



Device Bay Information - HP ProLiant BL685c G7 (Bay 4)

Server Management

- iLO
- Port Mapping Information
- Firmware

Status	✓ OK
Powered	On
Power Allocated	900 Watts
Virtual Fan:	28%

Diagnostic Information	
Device Identification Data	✓ OK
Management Processor	✓ OK
I/O Configuration	✓ OK
Power Allocation Request	✓ OK
Cooling	✓ OK
Device Location	✓ OK
Device Operational	✓ OK
Device Degraded	✓ OK
iLO Network	✓ OK
Mezzanine Card	✓ OK

Temperature Sensors

Location	Status	Temperature
Ambient Zone - Inlet Ambient	✓	23°C Caution: 42°C Critical: 46°C
System Zone - System Board	✓	32°C Caution: 85°C Critical: 90°C
CPU Zone - CPU 1	✓	45°C Caution: 75°C Critical: 80°C
CPU Zone - CPU 2	✓	33°C Caution: 75°C Critical: 80°C
	✓	30°C

Row	Description
System Event Health	The internal System Event Health that the device is reporting. If the status is not OK, examine the blade System Event Log on the iLO to determine the cause of the condition. Possible values are OK, Degraded, or Failed.
Status	The overall status of the blade. Possible values are Unknown, OK, Degraded, Failed, or Other with an informational icon. The informational icon with an Other status displays until the server blade is configured for Virtual Connect Manager. See the Diagnostic Information table for further information.
Powered	The power state of the blade. Possible values are On or Off.
Power Delay Remaining	The number of seconds remaining before the device powers on.
Power Allocated	The amount of power allocated to the blade in watts.
Partner Device	The storage/expansion blade the server blade is partnered with. This information does not display if there is no partner device.
Virtual Fan	The percentage of maximum RPM of the virtual fan.

Diagnostic Information

Row	Description
Device Identification Data	Model name, part number, serial number, and other information used to identify the device is checked. This data is also referred to as FRU data. If the data is not present or not readable by the Onboard Administrator, then a device identification data error appears. Possible values are OK or Error.
Management Processor	Status of the iLO. Possible values are OK or Error.
Temperature	Temperature is above the warning threshold. Possible values are OK or Temperature Warning.
Overheat Check	Temperature is above the danger threshold. Possible values are OK or Critical temperature threshold reached.
I/O Configuration	Device bay configuration is incorrect. If a storage blade is partnered with a full-height server blade, and the server blade does not have the correct mezzanine card, then an invalid I/O configuration results. Possible values are OK or I/O mismatch detected.
Power Allocation Request	Available power is insufficient to adequately power this server blade. Possible values are OK or Insufficient enclosure power.
Cooling	The number of fans is insufficient to properly cool this server blade, or the fan configuration is incorrect. Possible values are OK or Insufficient fans for enclosure cooling.
Device Location	The server blade has been placed in the wrong slot in the enclosure according to the current fan configuration. Possible values are OK or Incorrect location for proper device cooling.
Device Operational	Device has failed. Status was not requested by the Onboard Administrator. Possible values are OK or Error.
Device Degraded	Device has failed. Status was requested by the Onboard Administrator. Possible values are OK or Error.

Table Continued

Row	Description
iLO Network	Detects an iLO network configuration problem. Possible values are OK or iLO network configuration problem, check connectivity to iLO default gateway. If the problem continues, then attempt to reset the iLO using the iLO GUI or the Onboard Administrator CLI `RESET ILO` command. You can also use the CLI `HPONCFG` command to send a script command to reset iLO.
Memory Error	A memory error occurred on the server blade. To correct the error, follow the instructions provided.
Mezzanine Card	Displays an error if a missing mezzanine card prevents the server blade from partnering. Displays OK if no partnering issues were discovered while diagnosing a power-on request. This status will be reset if the Onboard Administrator reboots.
Duplicate IP Address	A check to see if a duplicate IP address exists on the network during assignment. Possible values are OK or an informational message indicating there is a duplicate IP address on the network.
Enclosure Dynamic Power Capping	A warning that communication with iLO has been lost and power capping cannot be set.
Partner Device Link	Server blade partner device link status. Possible values are OK or Inappropriate device in adjacent bay. If the server blade is not partnered with a storage blade, this information does not appear.
Virtual Connect Configured	Possible values are Configured for Virtual Connect or Not configured for Virtual Connect. When the server blade is not configured for Virtual Connect, an informational icon with an Other status appears. To configure the server blade profile, go to the Virtual Connect Manager.
Low Power Request	The server blade reported an abnormally low power requirement. The server blade was powered off and did not release all of the power. The server blade will continue to operate properly, but correct the issue by contacting a service representative.
Firmware Management	The status of firmware management on the server.
Power Denial-Discovery	A warning that device power delayed during device discovery.
Power Denial-SAS Storage	A warning that device power delayed until SAS storage is ready.
Power Denial-Partnering	A warning that device power delayed until device is configured for partnership.
Power Denial-VC Profile	A warning that device power delayed until VC profile is applied.
Power Denial-OA Initialization	A warning that device power delayed until the OA has completed initialization.
Power Denial-Power Delay	A warning that device power delayed until the configured Power Delay for this bay has elapsed.
Power Denial-Firmware Management	A warning that device power delayed until Firmware Management process completes.
Power Denial-I/O Discovery	A warning that device power delayed until interconnect discovery is complete.
Power Denial-Settings	A warning that device power delayed until device settings are updated. Please retry power operation.

Table Continued

Row	Description
Power Denial-Partner Discovery	A warning that device power delayed until potential partner devices are discovered.
Power Denial-I/O Ready	A warning that device power delayed until corresponding interconnect is ready.
Power Denial-I/O Missing	A warning that device power delayed until corresponding interconnect is inserted into enclosure.
Power Denial-SAS Mezz	A warning that device power delayed until SAS Mezz discovery is complete.
Power Denial-Blade Link Discovery	A warning that device power delayed during MMP Blade Link device discovery.

Temperature Sensors Information

Column	Description
Location	Location of sensor in the device.
Status	This is the status of the temperature sensor. The status matches the graphic presentation of the temperature.
Temperature	Graphic presentation of temperature.

iLO

The iLO for the server blade in the device bay is available by clicking **iLO**. The Onboard Administrator iLO page appears, as described in the Device Bay **iLO screen** section.

The Device Bay iLO screen provides links to several different iLO interfaces. When you click on any of these links, the Onboard Administrator provides a one-time login (login bypass) to ProLiant iLO management processors. The iLO access levels are mapped by the Onboard Administrator privilege level (user must have access to the bay):

- **Onboard Administrator Administrator** - Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, Configure iLO settings.
- **Onboard Administrator Operator** - Remote Console Access, Virtual Power and Reset, Virtual Media.

When an Onboard Administrator user launches the iLO web interface or an iLO remote console, a temporary iLO user is created . The Onboard Administrator can create up to three temporary accounts for each iLO. If three or more temporary Onboard Administrator accounts are already on an iLO, then the Onboard Administrator deletes the oldest temporary users in iLO user databases.

Port Mapping Information

Port mapping information is available by clicking **Port Mapping Information on the Device Bay Information screen**.

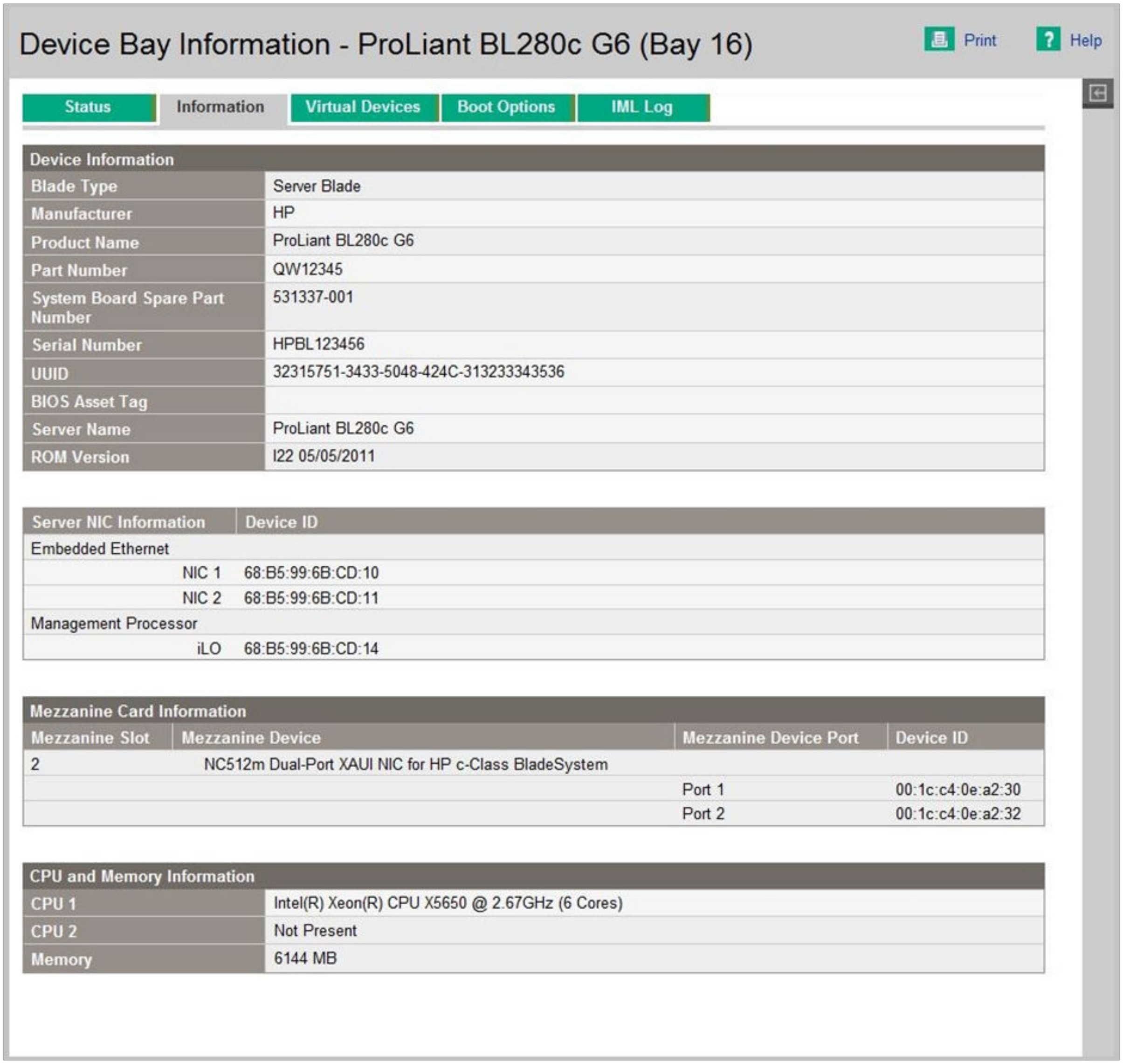
For more information, see **Port Mapping**.

Firmware

Firmware information for devices in the device bay is available by clicking **Firmware**.

For more information, see **Firmware**.

Server Blade Information tab



Device Bay Information - ProLiant BL280c G6 (Bay 16)

Device Information	
Blade Type	Server Blade
Manufacturer	HP
Product Name	ProLiant BL280c G6
Part Number	QW12345
System Board Spare Part Number	531337-001
Serial Number	HPBL123456
UUID	32315751-3433-5048-424C-313233343536
BIOS Asset Tag	
Server Name	ProLiant BL280c G6
ROM Version	I22 05/05/2011

Server NIC Information	Device ID
Embedded Ethernet	
NIC 1	68:B5:99:6B:CD:10
NIC 2	68:B5:99:6B:CD:11
Management Processor	
iLO	68:B5:99:6B:CD:14

Mezzanine Card Information

Mezzanine Slot	Mezzanine Device	Mezzanine Device Port	Device ID
2	NC512m Dual-Port XAUI NIC for HP c-Class BladeSystem		
		Port 1	00:1c:c4:0e:a2:30
		Port 2	00:1c:c4:0e:a2:32

CPU and Memory Information	
CPU 1	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (6 Cores)
CPU 2	Not Present
Memory	6144 MB

Device information

Row	Description
Blade Type	Server blade
Manufacturer	Name of the company that manufactured the server blade
Product Name	Common descriptive name for the server blade
Part Number	Part number used when ordering an additional or replacement server blade of this type
System Board Spare Part Number	Part number used when ordering an additional or replacement system board of this type
Serial Number	The static factory serial number for the server blade
Serial Number (Logical)	A logical serial number assigned to the server blade

Table Continued

Row	Description
UUID	The UUID assigned to the server blade
UUID (Logical)	A logical UUID assigned to the server blade
BIOS Asset Tag	If configured, this is the asset tag of the installed server blade.
Server Name	If configured through the BIOS, this appears as the ProLiant server name. For ProLiant or Integrity server blades with Hewlett Packard Enterprise OS agents installed, this is the server host name. [1]
ROM Version	ROM version number
Boot Mode	Booting mode for the server blade. Boot Mode displays only if the server blade supports the Unified Extensible Firmware Interface (UEFI). Possible values are Legacy, UEFI, or UEFI Optimized.
Secure Boot	BIOS Secure Boot mode status for the server blade. Secure Boot status is displayed only if the server blade is configured in UEFI or UEFI Optimized boot mode. Possible values are Enabled or Disabled. Secure Boot restricts users (including the Administrator) from changing the default boot device settings or performing certain boot operations from the Onboard Administrator GUI or CLI. All changes to boot settings must be made in BIOS by the Administrator. Boot operations can be performed only from the boot device configured in BIOS by the Administrator. Secure Boot is not reported for Gen8 and earlier generations of server blades. For more information about Secure Boot, see the *UEFI System Utilities User Guide* on the **Hewlett Packard Enterprise website**.

[1] *The iLO web console enables you to change the server name. The iLO 2 servers have a limitation in which the iLO only alerts the Onboard Administrator when any of the first 28 characters of the name are changed. Otherwise, no notification is sent to Onboard Administrator. As a result, the server name shown in Onboard Administrator might differ from the iLO server name.*

Server NIC information

Row	Description
Ethernet FlexNIC LOM:(x)-(a-d)	A Flex-10 enable 10Gb NIC configured in Virtual Connect. The four FlexNICs on port x of a server LOM that supports Flex-10 are numbered LOM:x-a, LOM:x-b, LOM:x-c, and LOM:x-d, where x is the port 1–4. See the HPE Virtual Connect c-Class BladeSystem User Guide for detailed information on configuring Flex-10 NICs.
Ethernet FlexNIC (NIC x) LOM: (y)-(a-d)	A Flex-10 enable 10Gb NIC configured in Virtual Connect, where x is a NIC 1–32. The four FlexNICs on port y of a server LOM that supports Flex-10 are numbered LOM:y-a, LOM:y-b, LOM:y-c, and LOM:y-d, where y is the port 1–8. See the Virtual Connect c-Class BladeSystem user guide for detailed information on configuring Flex-10 NICs.
Port: NIC x	The MAC address of this NIC port, where x is a NIC port 1-4.
Port: iLO	The MAC address of the iLO port for the server blade in this enclosure slot
Port: iSCSI x	The MAC address of this iSCSI port, where x is an iSCSI port 1–8.

Table Continued

Row	Description
Ethernet FCoE FlexFabric Adapter: (y)-(a-d)	A FCoE FlexFabric adapter consists of 4 NICs.The four FlexNICs on port y of a server LOM that supports Flex-10 are numbered LOM:y-a, LOM:y-b, LOM:y-c, and LOM:y-d, where y is the port 1–8 LOM:y-b can be used to configure FCoE traffic.
Ethernet iSCSI FlexFabric adapter: (y)-(a-d)	A iSCSI FlexFabric adapter consists of 4 NICs.The four FlexNICs on port y of a server LOM that supports Flex-10 are numbered LOM:y-a, LOM:y-b, LOM:y-c, and LOM:y-d, where y is the port 1–8 LOM:y-b can be used to configure iSCSI traffic.

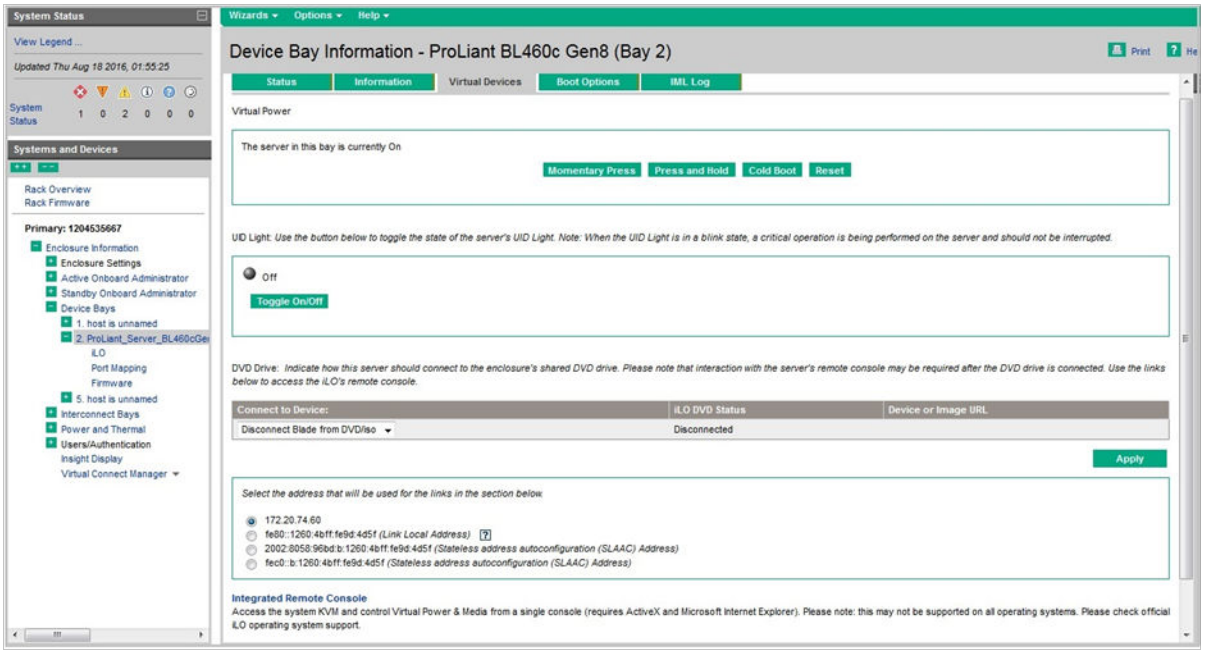
Mezzanine card information

Column	Description
Mezzanine Slot	The physical slot in which the mezzanine card is located
Mezzanine Device	The common or product name of the mezzanine device
Mezzanine Device Port	The port assigned to the mezzanine device
Device ID	The MAC address of the interconnect bay port

CPU and memory information

Row	Description
CPU 1 through CPU (x)	CPU type and speed or Not present
Memory	Memory size

Server Blade Virtual Devices tab



Updated Thu Aug 18 2016, 01:55:25

System Status	1	0	2	0	0	0

Primary: 1204535667

Device Bay Information - ProLiant BL460c Gen8 (Bay 2)

Virtual Power

The server in this bay is currently On

UID Light: *Use the button below to toggle the state of the server's UID Light. Note: When the UID Light is in a blink state, a critical operation is being performed on the server and should not be interrupted.*

Off

DVD Drive: *Indicate how this server should connect to the enclosure's shared DVD drive. Please note that interaction with the server's remote console may be required after the DVD drive is connected. Use the links below to access the iLO's remote console.*

Connect to Device:	iLO DVD Status	Device or Image URL
Disconnect Blade from DVD/iso	Disconnected	

Select the address that will be used for the links in the section below

- ● 172.20.74.60
- ○ fe80::1260:4bff:fe9d:4d5f *(Link Local Address)*
- ○ 2002:8058:96bd:b:1260:4bff:fe9d:4d5f *(Stateless address autoconfiguration (SLAAC) Address)*
- ○ fec0::b:1260:4bff:fe9d:4d5f *(Stateless address autoconfiguration (SLAAC) Address)*

Access the system KVM and control Virtual Power & Media from a single console (requires ActiveX and Microsoft Internet Explorer). Please note: this may not be supported on all operating systems. Please check official iLO operating system support.

Virtual Power

Button	Description
Momentary Press	This button mimics a physical momentary press of the power button on the server blade. Clicking this button powers the server blade on or off gracefully.
Press and Hold	This button mimics a physical press and hold of the power button on the server blade. Clicking this button forces the server blade to shut power off without regard for first shutting down the OS before turning power off. This option is not available when the server blade is off.
Cold Boot	Clicking this button immediately removes power from the system. This option is not available when the server blade is off.
Reset	Clicking this button performs a system reset. This option is not available when the server blade is off.

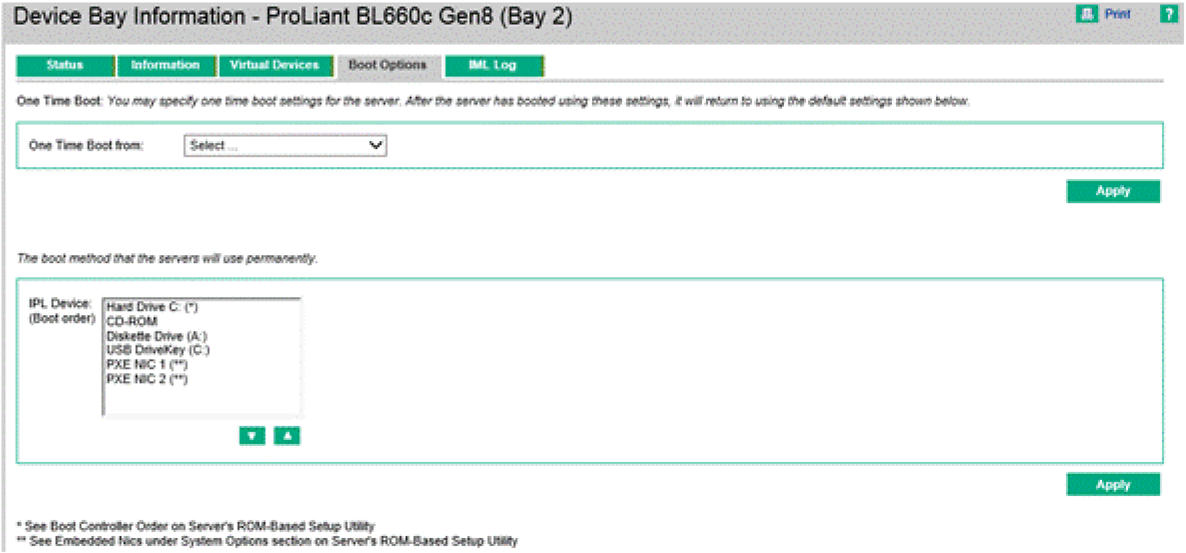
UID Light

To help identify a specific server blade, click **Toggle On/Off** to turn the server blade's UID light on (blue) or off (gray).

DVD Drive

Column	Description
Connect to Device	The menu enables you to connect or disconnect the shared DVD drive by selecting **Connect to Enclosure DVD** or **Disconnect DVD Hardware**.
iLO DVD Status	This field indicates whether the server blade has a Virtual Media connection. Possible values are Connected or Disconnected. A status of Incompatible Firmware means the DVD feature is not supported with the iLO firmware installed on the device.
Device or Image URL	This field displays the current Virtual Media connection of the blade. Possible values are: • Virtual Media Applet is connected • Feature not supported on Integrity iLO version x.xx • SSH is disabled on this blade's iLO processor • Upgrade ProLiant iLO version x.xx to 1.30 or higher • Enclosure DVD • Tray Open or No Media • URL to USB key ISO image file • iLO has no IP address

Boot Options tab



Device Bay Information - ProLiant BL660c Gen8 (Bay 2)

One Time Boot: *You may specify one time boot settings for the server. After the server has booted using these settings, it will return to using the default settings shown below.*

One Time Boot from: Select ...

The boot method that the servers will use permanently.

IPL Device: (Boot order)

Hard Drive C: (*)
CD-ROM
Diskette Drive (A:)
USB DriveKey (C:)
PXE NIC 1 (**)
PXE NIC 2 (**)

* See Boot Controller Order on Server's ROM-Based Setup Utility
** See Embedded Nics under System Options section on Server's ROM-Based Setup Utility

One Time Boot from selections

If you specify one time boot settings, the settings are valid only for the next reboot of the server blade. After the boot is complete, the server blade uses the default settings (the IPL device boot order) for subsequent reboots.

Option	Description
Select	The default option when viewing for the first time or before making any changes.
No one time Boot	Forces the server blade to clear the one time boot settings.
Diskette Drive (A:)	Forces the server blade to reboot to the diskette drive. Be sure the diskette drive is attached to the server blade before selecting this option.
CD-ROM	Forces the server blade to reboot to the CD-ROM drive. Be sure the CD-ROM drive is attached to the server blade before selecting this option.
Hard Drive C:	Forces the server blade to reboot to the hard disk.
RBSU	Forces the server blade to boot to the ROM-Based Setup Utility.
PXE NIC	Forces the server blade to boot to PXE NIC.
USB	Forces the server blade to boot to USB.
Embedded UEFI Shell	Forces the server blade to boot to Embedded UEFI Shell. This option is not available for non UEFI-capable blade.
UEFI Target	Forces the server blade to boot to UEFI Target device. This option is not available for non UEFI-capable server or UEFI-capable server in Legacy Boot BIOS Mode.

To save settings, click **Apply**.

If Secure Boot is configured on the server blade, the One Time Boot option cannot be selected. The option is grayed out. Secure Boot restricts users (including the Administrator) from performing this operation from the Onboard Administrator GUI or CLI. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

Standard Boot Order (IPL)

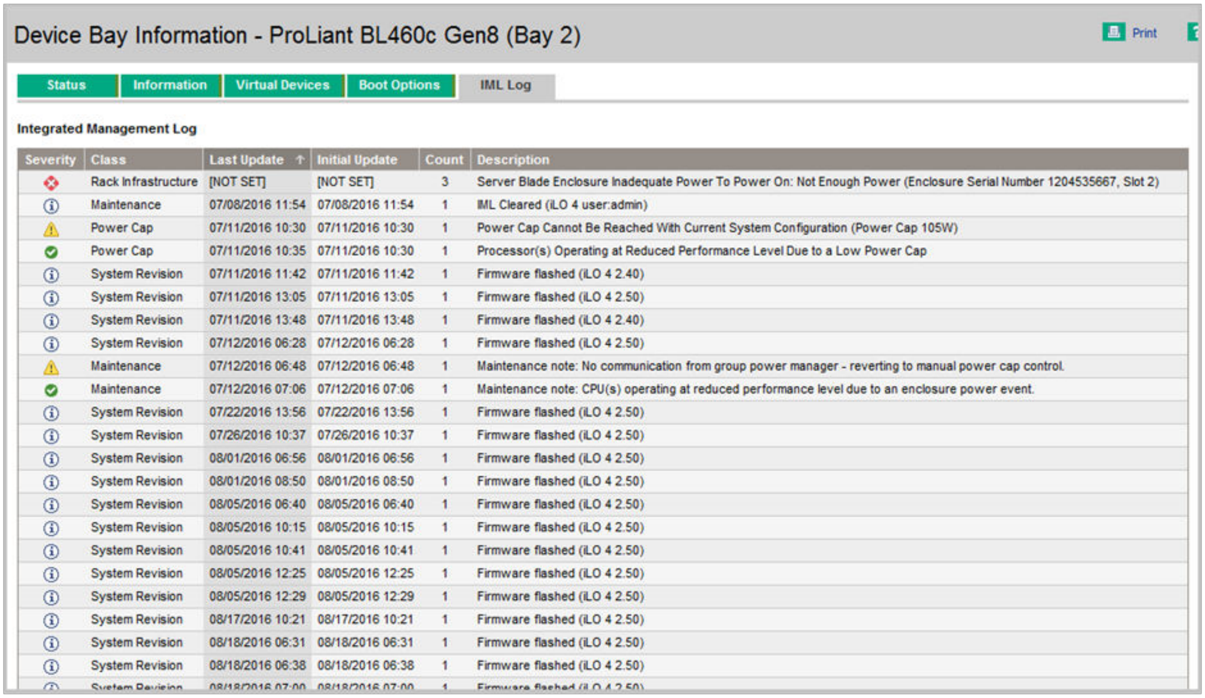
To specify a Standard Boot Order, select a device in the boot order list, and use the up and down arrows to move the boot device. Continue this process until you have arranged the devices in the order you want them used. Alternately, the RBSU can be used to set the Standard Boot Order. All reboots, unless using the One Time Boot option, use the boot order specified in the Standard Boot Order settings.

To save settings, click **Apply**.

If Secure Boot is configured on the server blade, the IPL devices cannot be selected. The device list is grayed out. Secure Boot restricts users (including the Administrator) from performing this operation from the Onboard Administrator GUI or CLI. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

IML Log tab

The IML Log tab displays information saved on the server blade's IML. The log items can include informational, warning, or critical statuses. Last Update and Initial Update columns display dates, and the Count column displays the number of times the entry was logged. The Description column displays the verbose entry, describing the entry in more detail.

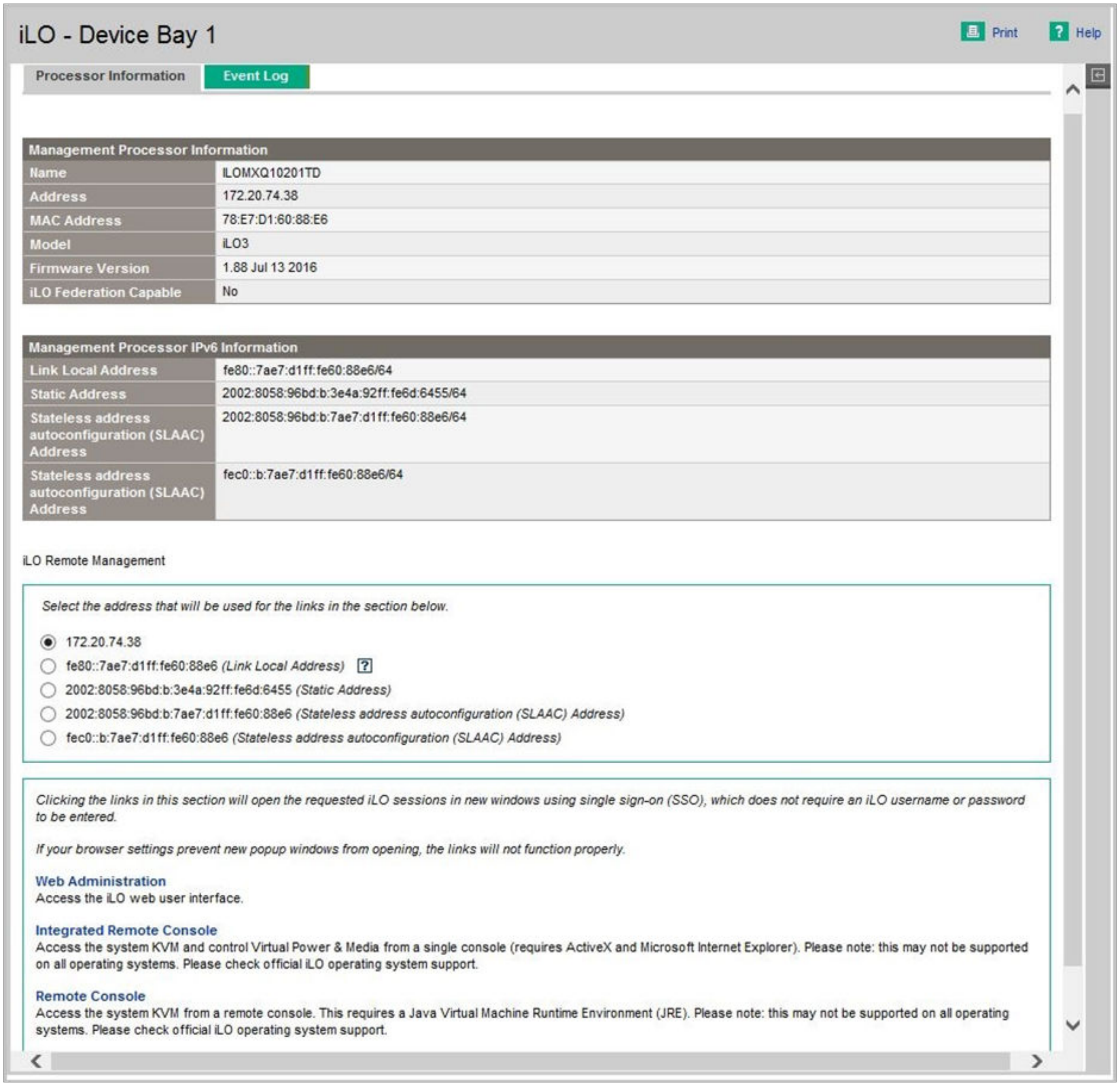


Device Bay Information - ProLiant BL460c Gen8 (Bay 2)

Integrated Management Log

Severity	Class	Last Update ↑	Initial Update	Count	Description
✖	Rack Infrastructure	[NOT SET]	[NOT SET]	3	Server Blade Enclosure Inadequate Power To Power On: Not Enough Power (Enclosure Serial Number 1204535667, Slot 2)
ⓘ	Maintenance	07/08/2016 11:54	07/08/2016 11:54	1	IML Cleared (iLO 4 user:admin)
⚠	Power Cap	07/11/2016 10:30	07/11/2016 10:30	1	Power Cap Cannot Be Reached With Current System Configuration (Power Cap 105W)
✓	Power Cap	07/11/2016 10:35	07/11/2016 10:30	1	Processor(s) Operating at Reduced Performance Level Due to a Low Power Cap
ⓘ	System Revision	07/11/2016 11:42	07/11/2016 11:42	1	Firmware flashed (iLO 4 2.40)
ⓘ	System Revision	07/11/2016 13:05	07/11/2016 13:05	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	07/11/2016 13:48	07/11/2016 13:48	1	Firmware flashed (iLO 4 2.40)
ⓘ	System Revision	07/12/2016 06:28	07/12/2016 06:28	1	Firmware flashed (iLO 4 2.50)
⚠	Maintenance	07/12/2016 06:48	07/12/2016 06:48	1	Maintenance note: No communication from group power manager - reverting to manual power cap control.
✓	Maintenance	07/12/2016 07:06	07/12/2016 07:06	1	Maintenance note: CPU(s) operating at reduced performance level due to an enclosure power event.
ⓘ	System Revision	07/22/2016 13:56	07/22/2016 13:56	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	07/26/2016 10:37	07/26/2016 10:37	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/01/2016 06:56	08/01/2016 06:56	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/01/2016 08:50	08/01/2016 08:50	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/05/2016 06:40	08/05/2016 06:40	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/05/2016 10:15	08/05/2016 10:15	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/05/2016 10:41	08/05/2016 10:41	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/05/2016 12:25	08/05/2016 12:25	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/05/2016 12:29	08/05/2016 12:29	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/17/2016 10:21	08/17/2016 10:21	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/18/2016 06:31	08/18/2016 06:31	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/18/2016 06:38	08/18/2016 06:38	1	Firmware flashed (iLO 4 2.50)
ⓘ	System Revision	08/18/2016 07:00	08/18/2016 07:00	1	Firmware flashed (iLO 4 2.50)

iLO screen



Management Processor Information	
Name	ILOMXQ10201TD
Address	172.20.74.38
MAC Address	78:E7:D1:60:88:E6
Model	iLO3
Firmware Version	1.88 Jul 13 2016
iLO Federation Capable	No

Management Processor IPv6 Information	
Link Local Address	fe80::7ae7:d1ff:fe60:88e6/64
Static Address	2002:8058:96bd:b:3e4a:92ff:fe6d:6455/64
Stateless address autoconfiguration (SLAAC) Address	2002:8058:96bd:b:7ae7:d1ff:fe60:88e6/64
Stateless address autoconfiguration (SLAAC) Address	fec0::b:7ae7:d1ff:fe60:88e6/64

iLO Remote Management

Select the address that will be used for the links in the section below.

● 172.20.74.38
○ fe80::7ae7:d1ff:fe60:88e6 *(Link Local Address)* ?
○ 2002:8058:96bd:b:3e4a:92ff:fe6d:6455 *(Static Address)*
○ 2002:8058:96bd:b:7ae7:d1ff:fe60:88e6 *(Stateless address autoconfiguration (SLAAC) Address)*
○ fec0::b:7ae7:d1ff:fe60:88e6 *(Stateless address autoconfiguration (SLAAC) Address)*

Clicking the links in this section will open the requested iLO sessions in new windows using single sign-on (SSO), which does not require an iLO username or password to be entered.

If your browser settings prevent new popup windows from opening, the links will not function properly.

Web Administration
Access the iLO web user interface.

Integrated Remote Console
Access the system KVM and control Virtual Power & Media from a single console (requires ActiveX and Microsoft Internet Explorer). Please note: this may not be supported on all operating systems. Please check official iLO operating system support.

Remote Console
Access the system KVM from a remote console. This requires a Java Virtual Machine Runtime Environment (JRE). Please note: this may not be supported on all operating systems. Please check official iLO operating system support.

Information provided on this screen includes tabs for Processor Information, Processor IPv6 Information, and Event Log. To display the front and rear views of the device bay, click the **Left Arrow** button in the upper right corner of the screen.

Processor Information tab

Row	Description
Name	The DNS name of the iLO processor.
Address	The IP address of the iLO processor.
MAC Address	The MAC address of the iLO processor.
Model	The common descriptor of the iLO processor.
Firmware Version	The installed firmware version of the iLO processor.

Table Continued

Row	Description
VLAN ID (Name)	The VLAN ID number and (VLAN Name) of the device bay when VLAN is enabled.
iLO Federation Capable	Indicates whether the server blade is capable of iLO Federation. This only indicates that the iLO is capable of being configured to participate in iLO Federation. It does not indicate that the iLO is currently configured for actual participation in iLO Federation. To fully enable iLO Federation, Enclosure iLO Federation Support must be enabled on the Onboard Administrator, (see the **Network Access**) and each iLO must have the appropriate firmware and be configured to support iLO Federation. For more information, see the *iLO 4 User Guide* at the **Hewlett Packard Enterprise website**.

Processor IPv6 Information

Row	Description
Link Local Address	The link local IPv6 address of the iLO processor
Static Address	The static IPv6 address of the iLO processor
EBIPA Address	The EBIPA IPv6 address of the iLO processor
DHCPv6 Address	The DHCP IPv6 address of the iLO processor
SLAAC Address	The SLAAC IPv6 address of the iLO processor

iLO Remote Management

This section provides links to the requested iLO sessions.

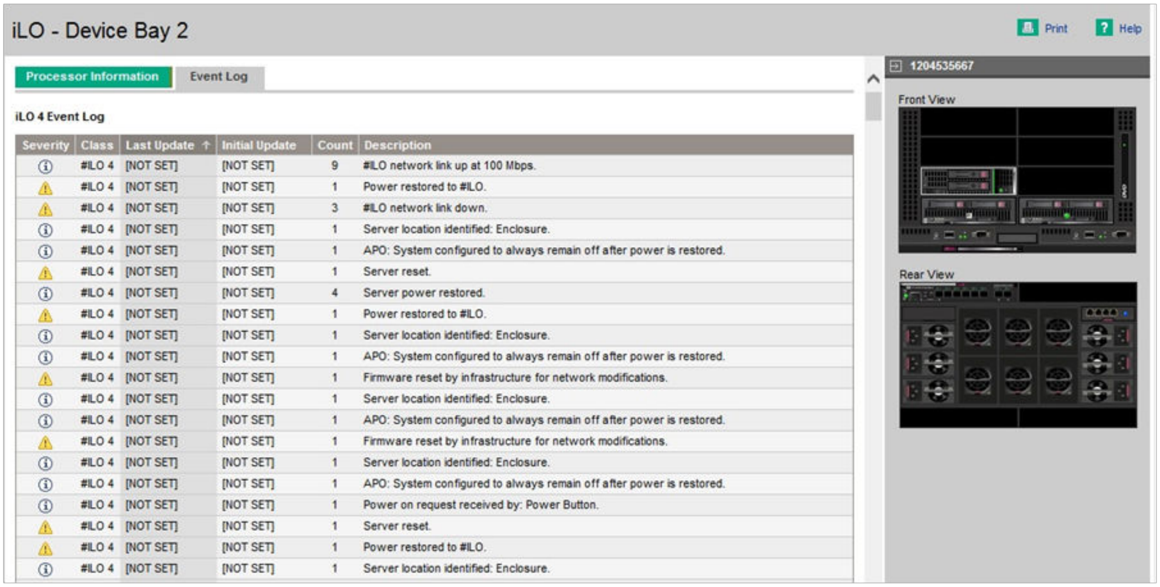
When the IPv6 protocol is enabled, or FQDN link support is enabled, an IP address group box appears. This group box allows you to select the IP address to be used for the links accessing the iLO sessions. If FQDN link support is enabled and certain DNS configuration requirements are met, an FQDN-based address is the default selection. For more information about enabling FQDN link support, see the **Network Access** page.

If you are trying to use a feature that requires popup window support and the feature does not work properly, make sure your browser settings are not preventing popup windows from opening. For help with turning off popup window blockers, see your specific browser help files.

NOTE:

When the Onboard Administrator is in FIPS Mode Top-Secret/Top-Secret Debug, the SSL/TLS and SSH connection to iLO 2,iLO 3 and iLO 4 cannot be established.

iLO Event Log tab



iLO 4 Event Log

Severity	Class	Last Update ↑	Initial Update	Count	Description
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	9	#ILO network link up at 100 Mbps.
⚠	#ILO 4	[NOT SET]	[NOT SET]	1	Power restored to #ILO.
⚠	#ILO 4	[NOT SET]	[NOT SET]	3	#ILO network link down.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	Server location identified: Enclosure.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	APO: System configured to always remain off after power is restored.
⚠	#ILO 4	[NOT SET]	[NOT SET]	1	Server reset.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	4	Server power restored.
⚠	#ILO 4	[NOT SET]	[NOT SET]	1	Power restored to #ILO.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	Server location identified: Enclosure.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	APO: System configured to always remain off after power is restored.
⚠	#ILO 4	[NOT SET]	[NOT SET]	1	Firmware reset by infrastructure for network modifications.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	Server location identified: Enclosure.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	APO: System configured to always remain off after power is restored.
⚠	#ILO 4	[NOT SET]	[NOT SET]	1	Firmware reset by infrastructure for network modifications.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	Server location identified: Enclosure.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	APO: System configured to always remain off after power is restored.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	Power on request received by: Power Button.
⚠	#ILO 4	[NOT SET]	[NOT SET]	1	Server reset.
⚠	#ILO 4	[NOT SET]	[NOT SET]	1	Power restored to #ILO.
ⓘ	#ILO 4	[NOT SET]	[NOT SET]	1	Server location identified: Enclosure.

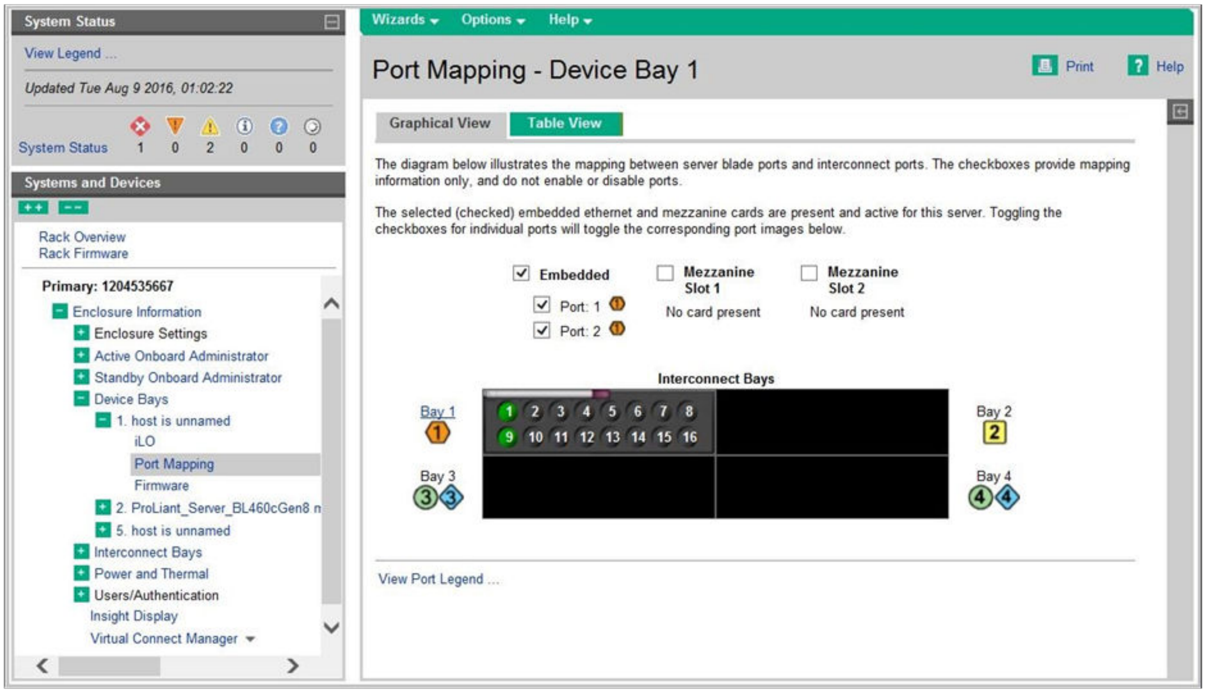
This tab displays the iLO Event Log information from iLO. It cannot be edited from the Onboard Administrator GUI. See the iLO documentation for detailed information on the iLO Event Log.

Port Mapping

The Port Mapping screen appears when you click **Port Mapping Information** from the Device Bay Information screen.

The following two screens show examples of the Port Mapping **Graphical View** and **Table View** tabs.

Graphical View



The diagram below illustrates the mapping between server blade ports and interconnect ports. The checkboxes provide mapping information only, and do not enable or disable ports.

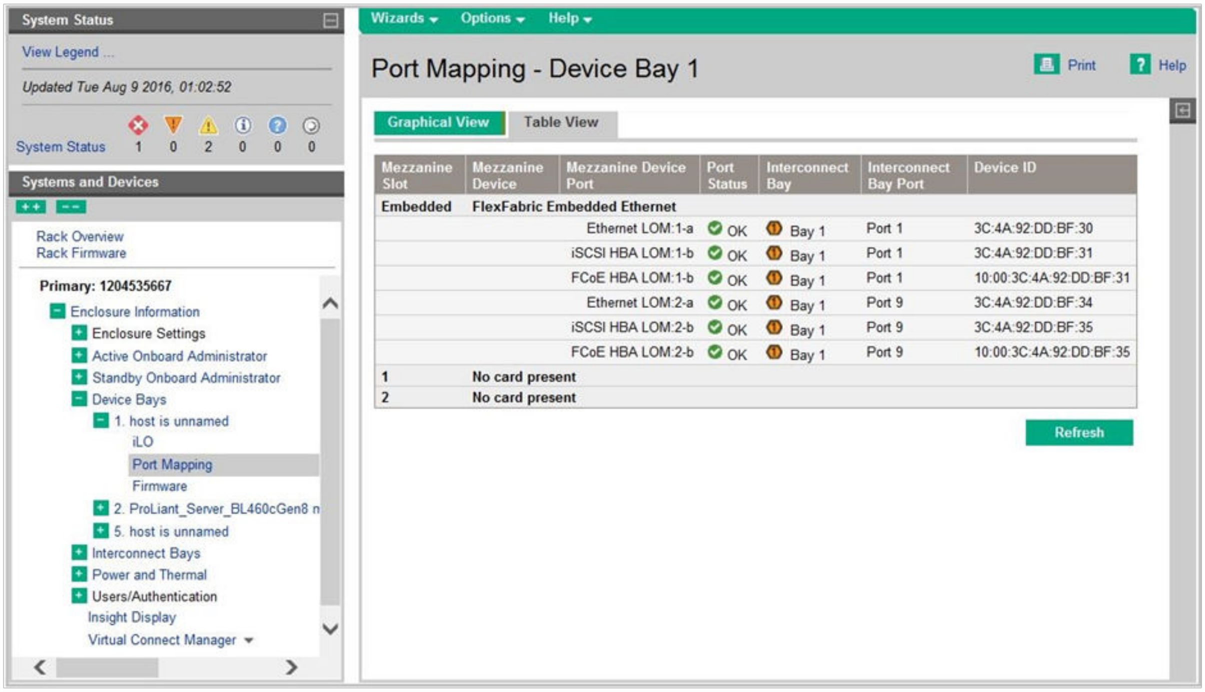
The selected (checked) embedded ethernet and mezzanine cards are present and active for this server. Toggling the checkboxes for individual ports will toggle the corresponding port images below.

☑ Embedded
☑ Port: 1
☑ Port: 2

☐ Mezzanine Slot 1
No card present

☐ Mezzanine Slot 2
No card present

Table View



Port Mapping - Device Bay 1

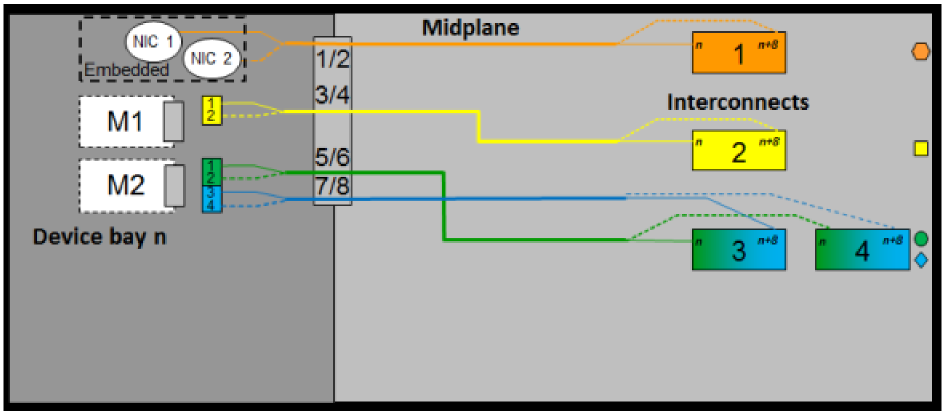
Mezzanine Slot	Mezzanine Device	Mezzanine Device Port	Port Status	Interconnect Bay	Interconnect Bay Port	Device ID
Embedded	FlexFabric Embedded Ethernet					
		Ethernet LOM:1-a	✓ OK	Bay 1	Port 1	3C:4A:92:DD:BF:30
		iSCSI HBA LOM:1-b	✓ OK	Bay 1	Port 1	3C:4A:92:DD:BF:31
		FCoE HBA LOM:1-b	✓ OK	Bay 1	Port 1	10:00:3C:4A:92:DD:BF:31
		Ethernet LOM:2-a	✓ OK	Bay 1	Port 9	3C:4A:92:DD:BF:34
		iSCSI HBA LOM:2-b	✓ OK	Bay 1	Port 9	3C:4A:92:DD:BF:35
		FCoE HBA LOM:2-b	✓ OK	Bay 1	Port 9	10:00:3C:4A:92:DD:BF:35
1	No card present					
2	No card present					

For more information, see the following sections in this document. In addition, see the latest c3000 Enclosure and c7000 Enclosure documentation in the **BladeSystem Information Library**.

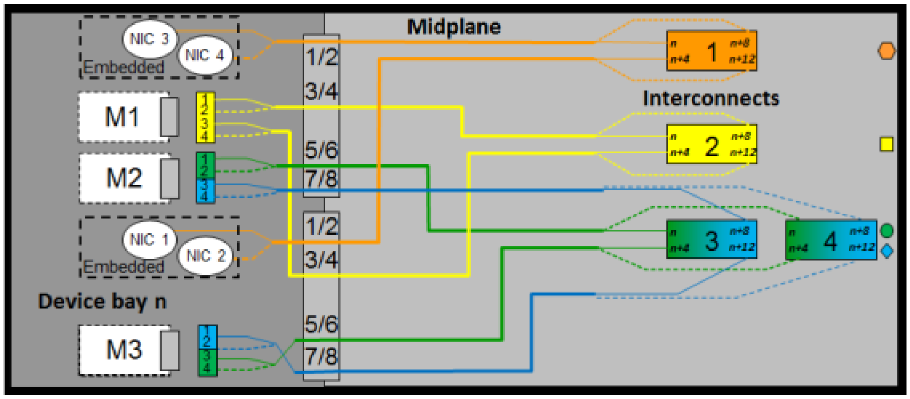
- **Device bay port mapping graphical view for c3000 Enclosure**
- **Device bay port mapping table for c3000 Enclosure**
- **Device bay port mapping graphical view for c7000 Enclosure**
- **Device bay port mapping table for c7000 Enclosure**

Device bay port mapping graphical view for c3000 Enclosure

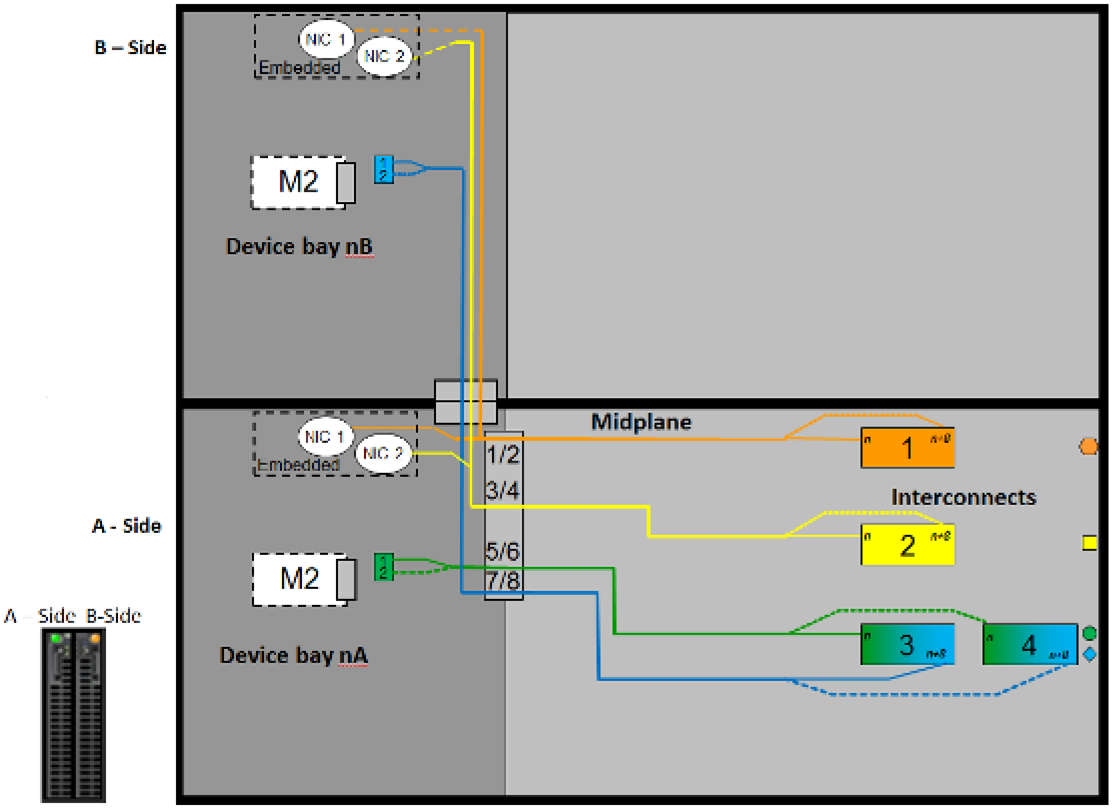
Half-height, single-wide server blades (such as an HPE ProLiant BL260c, BL280c, BL420c, BL465c, BL490c, BL495c, and WS460c)



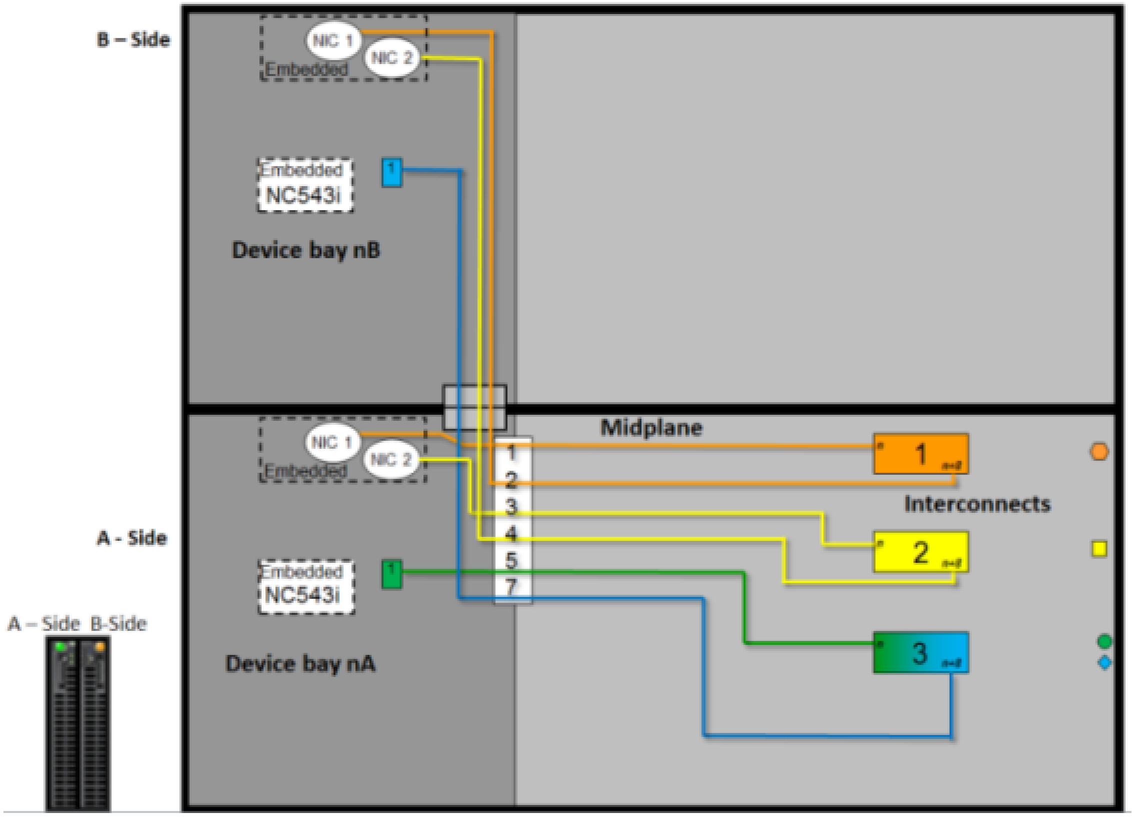
Full-height, single-wide server blade (such as an HPE ProLiant BL680c (G1), BL680c Gen5, and BL480c, BL620c, BL660c, and BL685c)



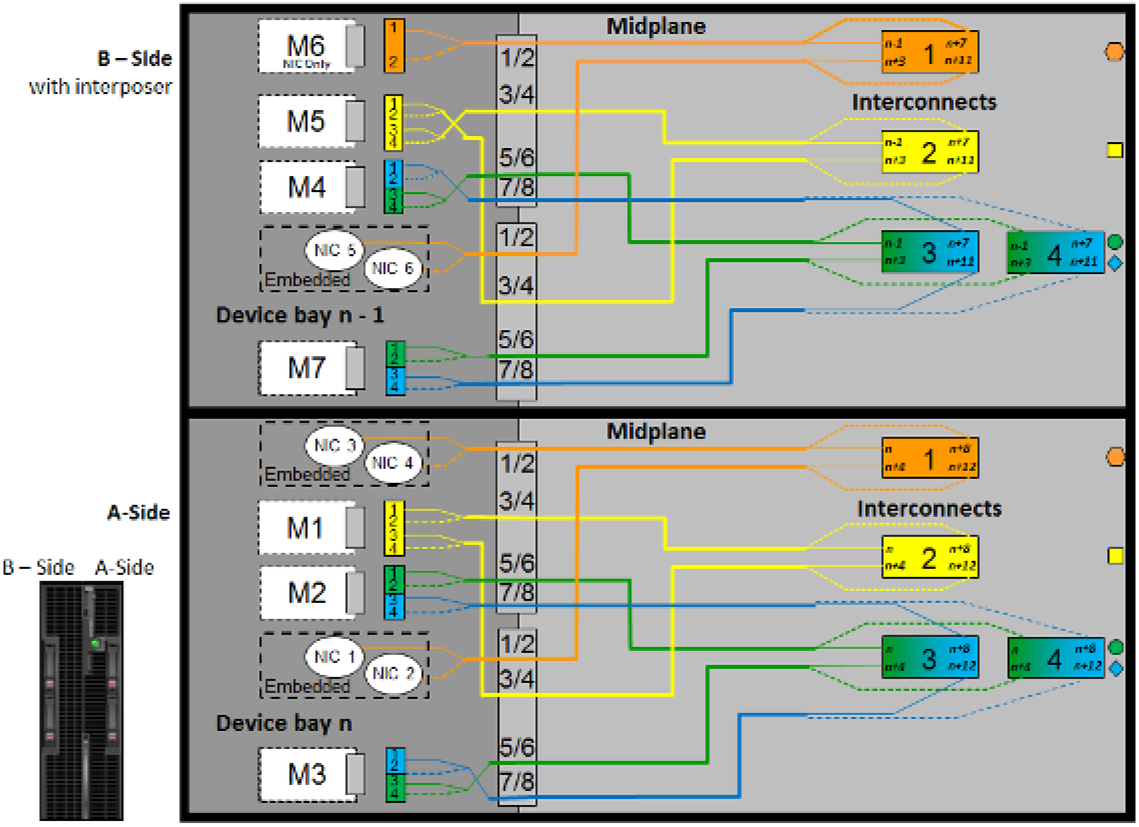
Half-height, double dense server blades such as an HPE ProLiant BL2x220c (G1)–G6



Half-height, double dense server blades such as an HPE ProLiant BL2x220c G7



Full-height, double-wide server blades such as an HPE ProLiant BL680c G7



Device bay port mapping table for c3000 Enclosure

The server blades are mapped to the interconnect bays in the following manner. The terms 1x, 2x, or 4x refer to the number of interconnect lanes per port provided by the controller. If a device is not present, the check box is disabled and the port cannot be viewed.

- Examples of 1x ports are 1GB Ethernet (1 GbE), 10GB Ethernet (10 GbE), and all Fibre Channel devices.
- Examples of 2x ports are 20GB Ethernet (20 GbE) and all serial-attached SCSI (SAS) devices.
- Examples of 4x ports are all InfiniBand devices.
- The following tables refer to the Ethernet ports as NICs.

NOTE:

1x and 2x port mezzanine cards interface with single-wide interconnect modules. 4x port mezzanine cards interface with double-wide interconnect modules.

Half-height, single-wide server blades

The following table lists the port mapping for half-height server blades installed in a c3000 half-height device bay N (1-8). Examples of such half-height server blades include HPE ProLiant BL260c, BL280c, BL420c, BL460c, BL465c, BL490c, BL495c, and WS460c servers.

Connection	Port number	Connects to interconnect bay/port	Comments
NIC [1]	NIC 1 (Port:1) NIC 2 (Port:2)	1/Port N 1/Port N+8	One single-wide Ethernet interconnect module
Mezzanine slot 1—1x or 2x cards (4x cards are not supported in this slot)	1x/2x port 1 1x/2x port 2	2/Port N 2/Port N+8	• One single-wide interconnect module • Only two ports will be connected. • Four port cards will only connect the first two ports.
Mezzanine slot 2—1x or 2x cards	1x/2x port 1 1x/2x port 2 1x/2x port 3 1x/2x port 4	3/Port N 4/Port N 3/Port N+8 4/Port N+8	One or two single-wide interconnect modules
Mezzanine slot 2—4x cards	4x port 1 4x port 2	3/Port N 3/Port N+8	One double-wide interconnect module

[1] *G7 and earlier generations of server blades include Ethernet ports embedded on the system board. With Gen8 and later generations of server blades, the Ethernet ports are located on a user-selectable card known as a FlexibleLOM adapter. The FlexibleLOM adapter ports and the embedded network adapter ports have the same mapping.*

Full-height, single-wide server blades

The following table lists the port mapping for full-height single-wide server blades installed in a c3000 full-height device bay N (1-4). Examples of such full-height server blades include ProLiant BL680c (G1), BL680c Gen5, and BL480c, BL620c, BL660c, and BL685c.

Connection	Port number	Connects to interconnect bay/port	Comments
NIC [1]	NIC 1 (Port:1) NIC 2 (Port:2) NIC 3 (Port:3) NIC 4 (Port:4)	1/Port N+4 1/Port N+12 1/Port N 1/Port N+8	One single-wide Ethernet interconnect module
Mezzanine slot 1—1x or 2x cards (4x cards are not supported in this slot)	1x/2x port 1 1x/2x port 2 1x/2x port 3 1x/2x port 4	2/Port N 2/Port N+8 2/Port N+4 2/Port N+12	One single-wide interconnect module
Mezzanine slot 2—1x or 2x cards	1x/2x port 1 1x/2x port 2 1x/2x port 3 1x/2x port 4	3/Port N 4/Port N 3/Port N+8 4/Port N+8	One or two single-wide interconnect modules
Mezzanine slot 2—4x cards	4x port 1 4x port 2	3/Port N 3/Port N+8	One double-wide interconnect module
Mezzanine slot 3—1x or 2x cards	1x/2x port 1 1x/2x port 2 1x/2x port 3 1x/2x port 4	3/Port N+12 4/Port N+12 3/Port N+4 4/Port N+4	One or two single-wide interconnect modules
Mezzanine slot 3—4x cards	4x port 1 4x port 2	3/Port N+12 3/Port N+4	One double-wide interconnect module

[1] *G7 and earlier generations of server blades include Ethernet ports embedded on the system board. With Gen8 and later generations of server blades, the Ethernet ports are located on a user-selectable card known as a FlexibleLOM adapter. The FlexibleLOM adapter ports and the embedded network adapter ports have the same mapping.*

Half-height, double dense server blades such as ProLiant BL2x220 (G1) - G6

The following table lists the available configurations for double dense server blades installed in a c3000 half-height device bay N (1-8). Examples of these double dense server blades include HPE ProLiant BL2x220c (G1) - G6.

Connection	Port Number	Connects to interconnect bay/ port
Server A Embedded NIC	NIC 1 (Port:1) NIC 2 (Port:2)	1/Port N 2/Port N
Server A Mezzanine	Port 1 Port 2	3/Port N 4/Port N

Table Continued

Connection	Port Number	Connects to interconnect bay/ port
Server B Embedded NIC	NIC 1 (Port:1) NIC 2 (Port:2)	1/Port N+8 2/Port N+8
Server B Mezzanine	Port 1 Port 2	3/Port N+8 4/Port N+8

Half-height, double dense server blades such as ProLiant BL2x220c G7

The following table lists the available configurations for double dense devices such as HPE ProLiant BL2x220c G7 installed in a c3000 half-height device bay N (1-8).

Connection	Port Number	Connects to interconnect bay/ port
Server A Embedded NIC	NIC 1 (Port:1) NIC 2 (Port:2)	1/Port N 2/Port N
Server A Embedded NC543i [1]	Port 1	3/Port N
Server B Embedded NIC	NIC 1 (Port:1) NIC 2 (Port:2)	1/Port N+8 2/Port N+8
Server B Embedded NC543i [1]	Port 1	3/Port N+8

[1] *The ProLiant BL2x220c G7 Server Blade embedded NC543i is automatically configured by the Onboard Administrator to Ethernet, if an Ethernet interconnect module is installed in bay 3, or to InfiniBand if a double-wide InfiniBand interconnect is installed in bay 3. To change the NC543i configuration from one type to another, power off all the ProLiant BL2x220c G7 Server Blades, and replace the interconnect module with the other type. Reboot the active Onboard Administrator or reseat all the ProLiant BL2x220c G7 Server Blades; the Onboard Administrator reconfigures all the embedded NC543i devices for the new interconnect type.*

AMC Telco I/O expansion blade

The table lists the available configurations for AMC Telco devices installed in a c3000 half-height device bay N (1-8).

Connection	Port Number	Connects to interconnect bay/ port
AMC Embedded (1)	Port 1 Port 3	1/Port N 2/Port N
AMC Embedded (2)	Port 5 Port 7	3/Port N 4/Port N

Full-height, double-wide server blades such as ProLiant BL680c G7

The following table lists the available configurations for full-height, double-wide server blades such as the ProLiant BL680c G7 installed in a c3000 device bay N (2 or 4).

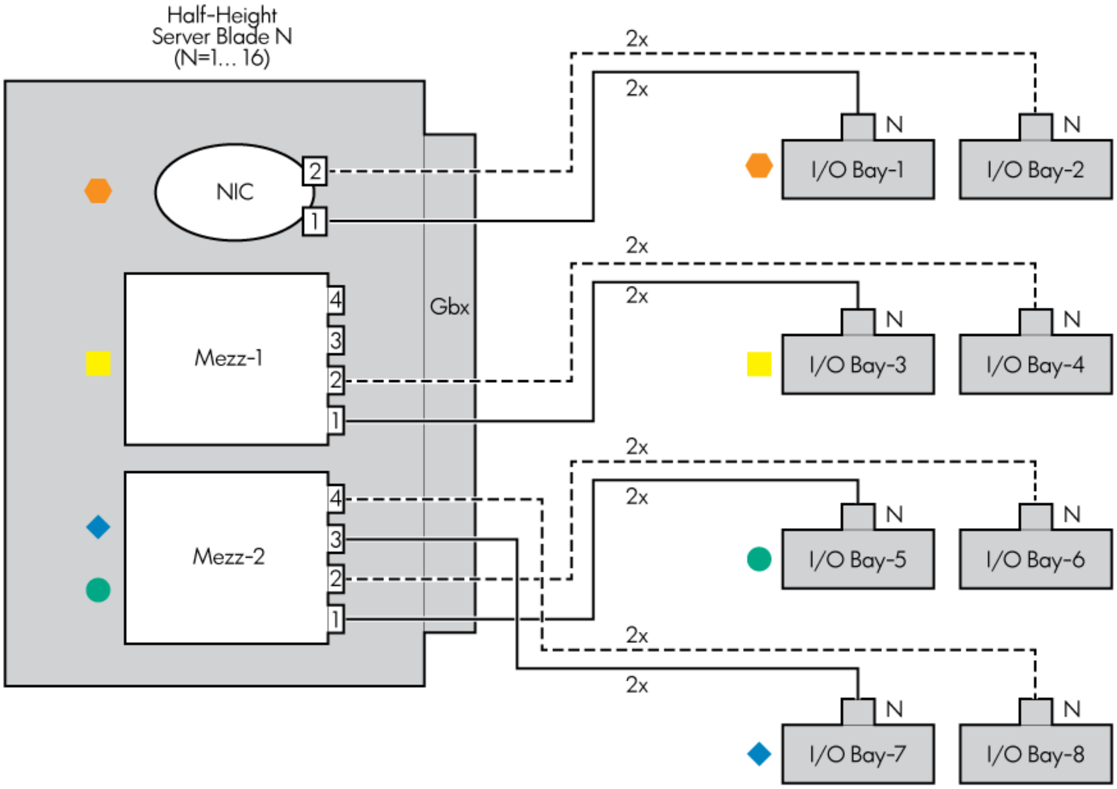
Connection	Port Number	Connects to interconnect bay/ port
A-Side Embedded NIC	NIC 1	1/Port N+4
	NIC 2	1/Port N+12
	NIC 3	1/Port N
	NIC 4	1 Port N+8
B-Side Embedded NIC	NIC 5	1/Port N+3
	NIC 6	1/Port N+11
A-Side Mezzanine 1	Port 1	2/Port N
	Port 2	2/Port N+8
	Port 3	2/Port N+4
	Port 4	2/Port N+12
A-Side Mezzanine 2	Port 1	3/Port N
	Port 2	4/Port N
	Port 3	3/Port N+8
	Port 4	4/Port N+8
A-Side Mezzanine 3	Port 1	3/Port N+12
	Port 2	4/Port N+12
	Port 3	3/Port N+4
	Port 4	4/Port N+4
B-Side Mezzanine 4	Port 1	3/Port N+7
	Port 2	4/Port N+7
	Port 3	3/Port N-1
	Port 4	4/Port N-1
B-Side Mezzanine 5	Port 1	2/Port N+3
	Port 2	2/Port N+11
	Port 3	2/Port N-1
	Port 4	2/Port N+7

Table Continued

Connection	Port Number	Connects to interconnect bay/ port
B-Side Mezzanine 6 NIC only	Port 1 Port 2	1/Port N-1 1/Port N+7
B-Side Mezzanine 7	Port 1 Port 2 Port 3 Port 4	3/Port N+11 4/Port N+11 3/Port N+3 4/Port N+3

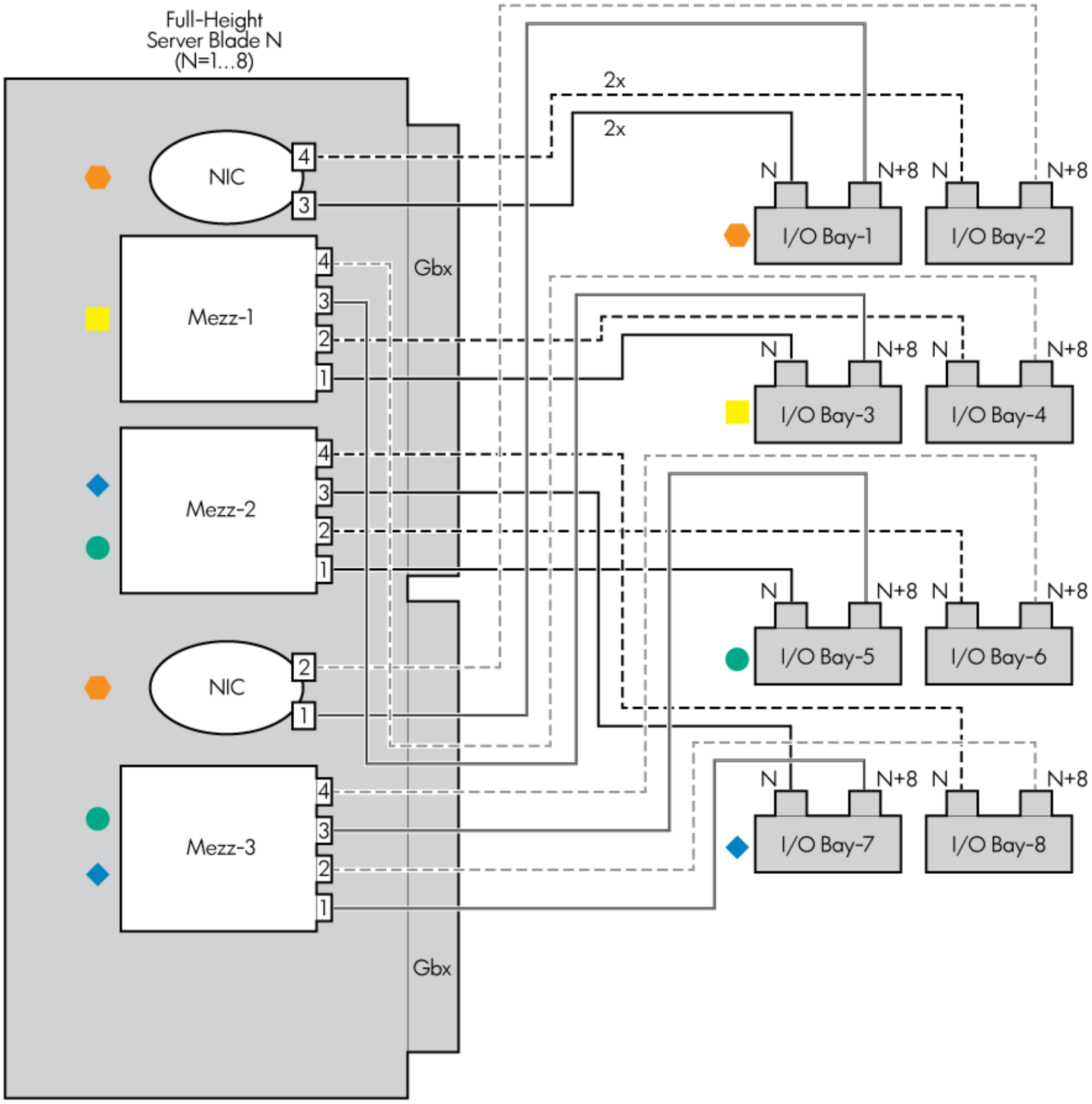
Device bay port mapping graphical view for c7000 Enclosure

Half-height, single-wide server blades (such as ProLiant BL260c, BL280c, BL420c, BL460c, BL465c, BL490c, BL495c, and WS460c)



In this diagram, N equals the number of the server blade in the enclosure and the port number on the switch. For example, if a server blade is inserted into slot 1, it is considered device 1, and the ports that will be used in switch 1 and switch 2 are ports 1 and 1, respectively. If a server blade is inserted into slot 2, then the ports used on switch 1 and switch 2 are ports 2 and 2. This convention changes for the full-height server blades as seen in the next diagram.

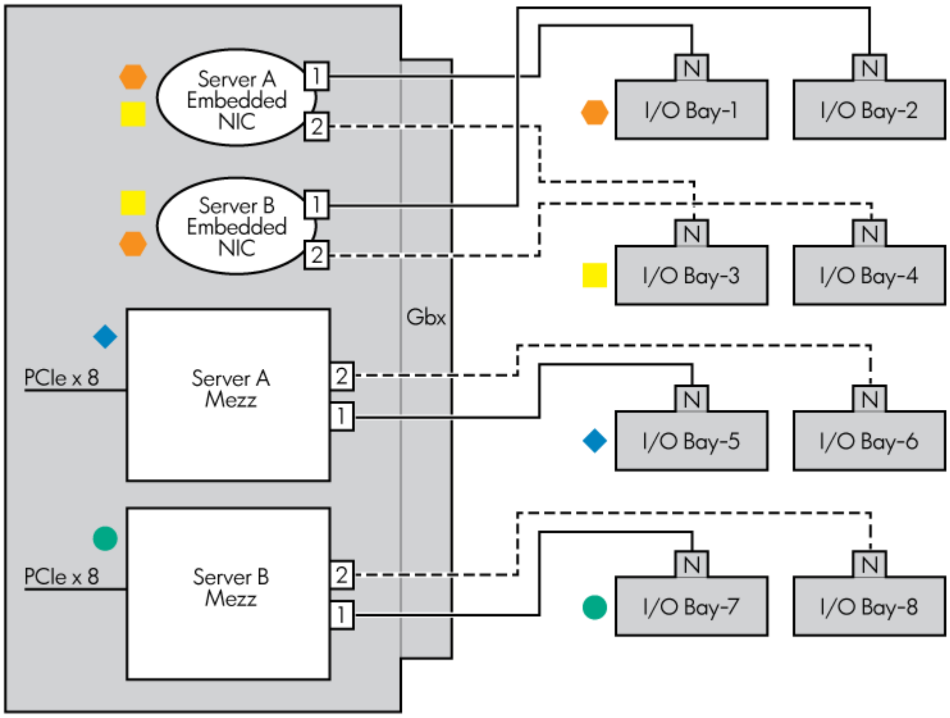
Full-height, single-wide server blades (such as ProLiant BL680c (G1), BL680c Gen5, and BL480c, BL620c, BL660c, and BL685c)



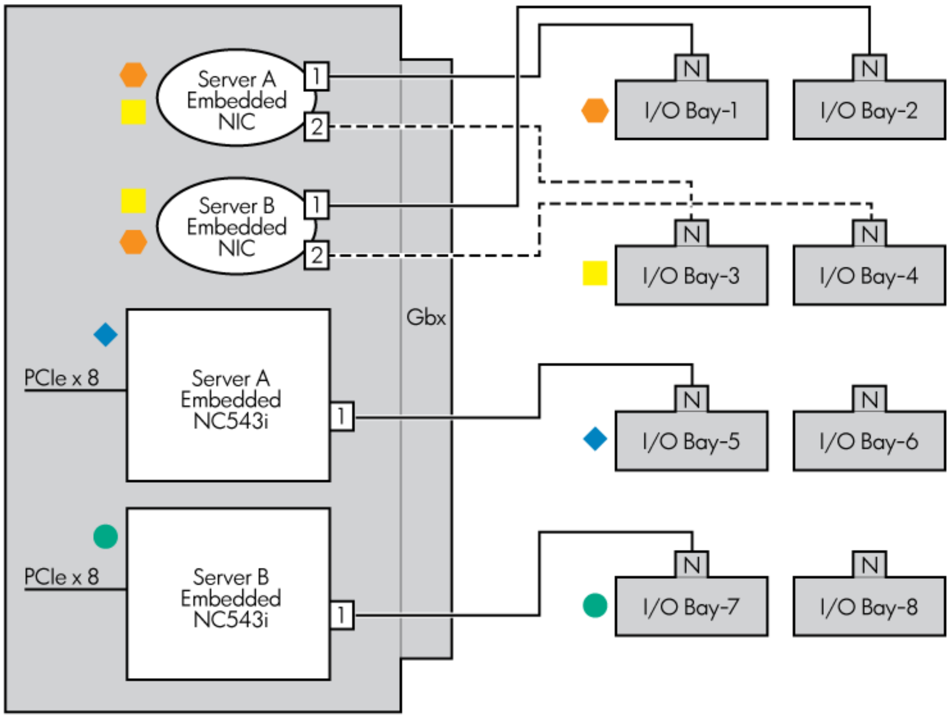
In this diagram, N equals the number of the blade in the enclosure and the port number for the switch. For example, if a blade is inserted into slot 1, it is considered device 1. Because full-height, single-wide server blades take up the space of two half-height server blades, the enclosure is limited to a maximum of eight full-height, single-wide server blades. Port mapping from these full-height, single-wide server blades might initially appear to be different than the half-height server blades, but they use very similar conventions.

Just as in a half-height server blade, if a blade is inserted into slot 1, it is considered device 1, but it has a second set of ports that will also map to switches 1 and 2. With the full-height, single-wide server blade, an N/N+8 scheme is used on the switches. Therefore, server blade 1 will map to ports 1 and 9 on both switches, as N=1. For a server blade inserted into slot 2, the four ports used on switches 1 and 2 would then be 2 and 10, as N=2.

Half-height, double dense server blades such as ProLiant BL2x220c (G1)–G6

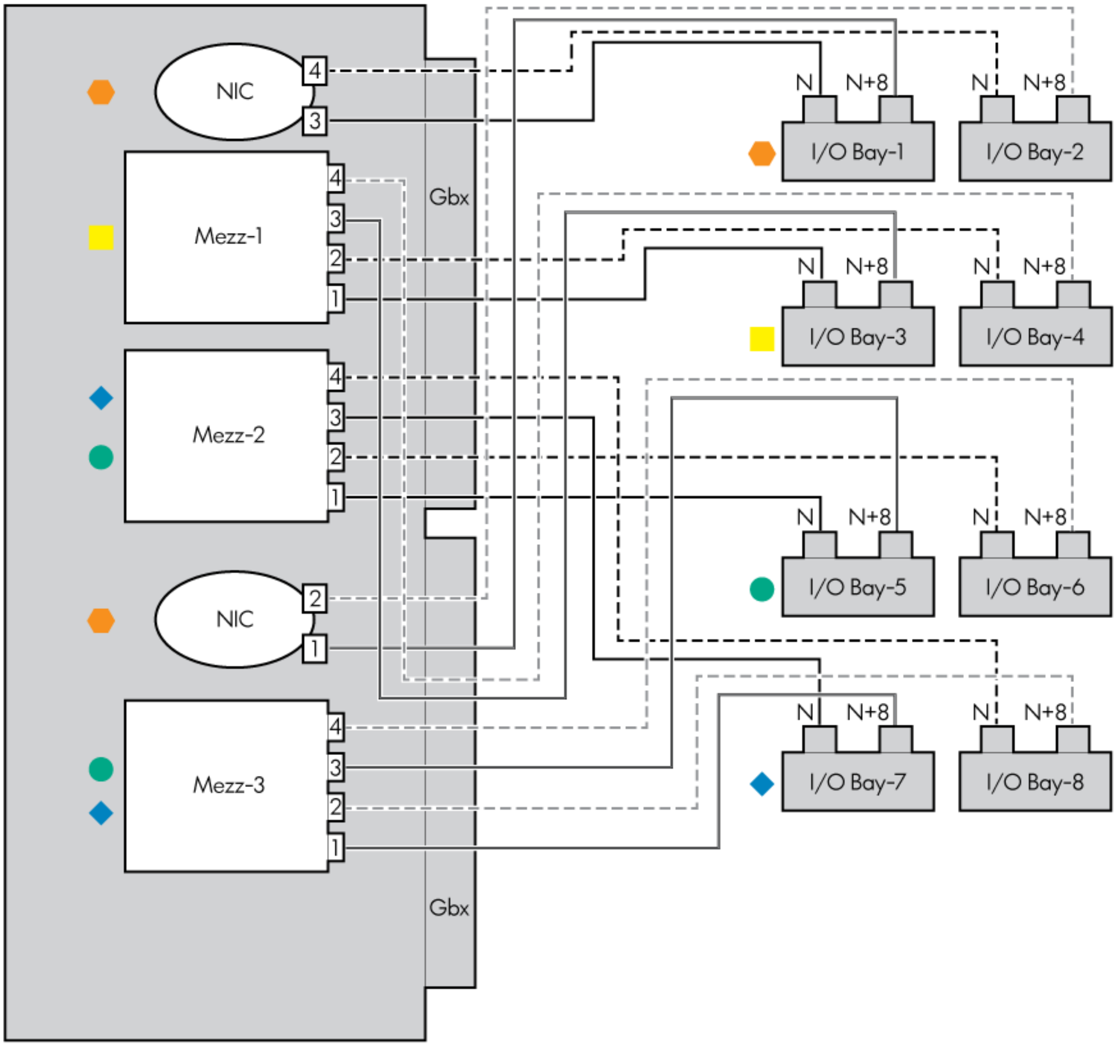


Half-height, double dense server blades such as ProLiant BL2x220c G7

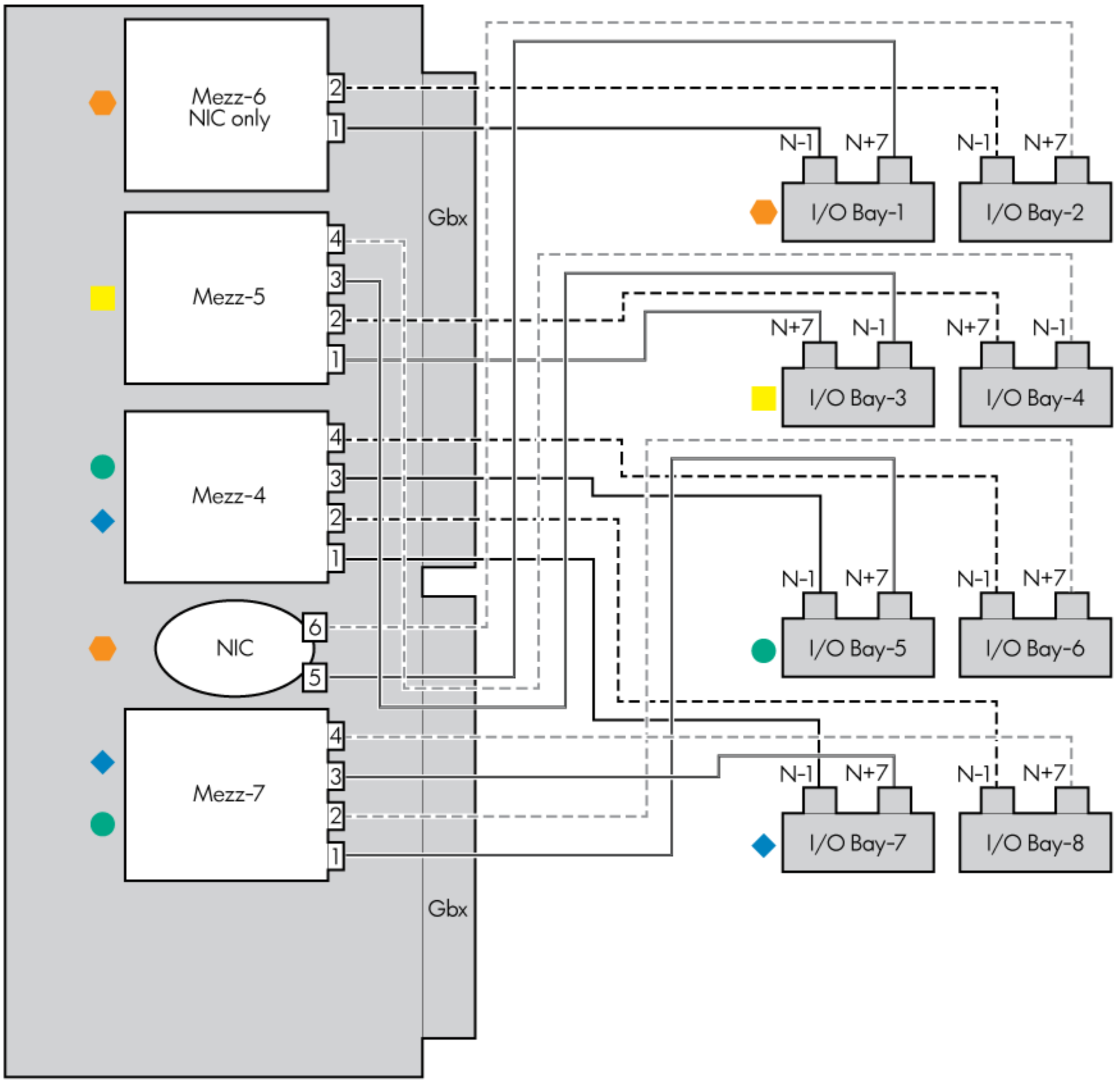


Full-height, double-wide server blades such as ProLiant BL680c G7

A-side


NIC
4
3
Mezz-1
4
3
2
1
Gbx
Mezz-2
4
3
2
1
NIC
2
1
Mezz-3
4
3
2
1
Gbx
N
N+8
I/O Bay-1
I/O Bay-2
I/O Bay-3
I/O Bay-4
I/O Bay-5
I/O Bay-6
I/O Bay-7
I/O Bay-8

B-side



Device bay port mapping table for c7000 Enclosure

The server blades are mapped to the interconnect bays in the following manner. The terms 1x, 2x, or 4x refer to the number of interconnect lanes per port provided by the controller. If a device is not present, the check box is disabled and the port cannot be viewed.

- Examples of 1x ports are 1GB Ethernet (1 GbE), 10GB Ethernet (10 GbE), and all Fibre Channel devices.
- Examples of 2x ports are 20GB Ethernet (20 GbE) and all serial-attached SCSI (SAS) devices.
- Examples of 4x ports are all InfiniBand devices.
- The following tables refer to the Ethernet ports as NICs.

Half-height, single-wide server blades

The following table lists the port mapping for half-height server blades installed in a c7000 half-height device bay N (1-16). Examples of such half-height server blades include ProLiant BL260c, BL280c, BL420c, BL465c, BL490c, BL495c, and WS460c servers.

Connection	Port number	Connects to interconnect bay/port	Comments
NIC [1]	NIC 1 NIC 2	1/Port N 2/Port N	One or two single-wide Ethernet interconnect modules
Mezzanine slot 1—1x or 2x cards	1x/2x port 1 1x/2x port 2	3/Port N 4/Port N	• One single-wide interconnect module • Four port cards will only connect the first two ports.
Mezzanine slot 1—4x cards	4x port 1	3/Port N	• One double-wide interconnect module • Only port 1 of a two port card will be connected.
Mezzanine slot 2—1x or 2x cards	1x/2x port 1 1x/2x port 2 1x/2x port 3 1x/2x port 4	5 / port N 6 / port N 7 / port N [2] 8 / port N[2]	One or two single-wide interconnect modules
Mezzanine slot 2—4x cards	4x port 1 4x port 2	5/Port N 7/Port N[2]	One or two double-wide interconnect modules

[1] G7 and earlier generations of server blades include Ethernet ports embedded on the system board. With Gen8 and later generations of server blades, the Ethernet ports are located on a user-selectable card known as a FlexibleLOM adapter. The FlexibleLOM adapter ports and the embedded network adapter ports have the same mapping.

[2] Connectivity to interconnect bays 7 and 8 is only available with four-port mezzanine cards or port 2 of 4x card in Mezzanine slot 2.

Full-height, single-wide server blades

The following table lists the port mapping for full-height, single-wide server blades installed in device bay N (1-8). Examples of such full-height server blades include ProLiant BL680c (G1), BL680c Gen5, and BL480c, BL620c, BL660c, and BL685c.

Connection	Port number	Connects to interconnect bay/port	Comments
NIC [1]	NIC 1 NIC 2 NIC 3 NIC 4	1/Port N+8 2/Port N+8 1/Port N 2/Port N	One or two single-wide Ethernet interconnect modules
Mezzanine slot 1—1x or 2x cards	1x/2x port 1 1x/2x port 2 1x/2x port 3 1x/2x port 4	3/Port N 4/Port N 3/Port N+8 4/Port N+8	One or two single-wide interconnect modules

Table Continued

Connection	Port number	Connects to interconnect bay/port	Comments
Mezzanine slot 1—4x cards	4x port 1	3/Port N	• One double-wide interconnect module • Only port 1 of a two-port card can be connected
Mezzanine slot 2—1x or 2x cards	1x/2x port 1 1x/2x port 2 1x/2x port 3 1x/2x port 4	5/Port N 6/Port N 7/Port N [2] 8/Port N [2]	Up to four single-wide interconnect modules
Mezzanine slot 2—4x cards	4x port 1 4x port 2	5/Port N 7/Port N [2]	One or two double-wide interconnect modules
Mezzanine slot 3—1x or 2x cards	1x/2x port 1 1x/2x port 2 1x/2x port 3 1x/2x port 4	7/Port N+8 * 8/Port N+8 * 5/Port N+8 6/Port N+8	Up to four single-wide interconnect modules
Mezzanine slot 3—4x cards	4x port 1 4x port 2	5/Port N+8 7/Port N+8 *	One or two double-wide interconnect modules

[1] G7 and earlier generations of server blades include Ethernet ports embedded on the system board. With Gen8 and later generations of server blades, the Ethernet ports are located on a user-selectable card known as a FlexibleLOM adapter. The FlexibleLOM adapter ports and the embedded network adapter ports have the same mapping.

[2] Connectivity to interconnect bays 7 and 8 is only available with four-port mezzanine cards or port 2 of 4x card in Mezzanine slot 2.

Half-height double dense server blades

The following table lists the available configurations for double dense server blades installed in a c7000 half-height device bay N (1-16). Examples of such double dense server blades include ProLiant BL2x220c (G1) - G6.

Connection	Port Number	Connects to interconnect bay/ port
Server A Embedded NIC	NIC 1 (Port:1) NIC 2 (Port:2)	1/Port N 3/Port N
Server A Mezzanine	Port 1 Port 2	5/Port N 6/Port N

Table Continued

Connection	Port Number	Connects to interconnect bay/ port
Server B Embedded NIC	NIC 1 (Port:1) NIC 2 (Port:2)	2/Port 4/Port N
Server B Mezzanine	Port 1 Port 2	7/Port N 8/Port N

Half-height double dense server blades such as ProLiant BL2x220c G7

The following table lists the available configurations for double dense server blades such as ProLiant BL2x220c G7 installed in c7000 half-height device bay N (1-16).

Connection	Port Number	Connects to interconnect bay/ port
Server A Embedded NIC	NIC 1 (Port:1) NIC 2 (Port:2)	1/Port N 3/Port N
Server A NC543i [1]	Port 1	5/Port N
Server B Embedded NIC	NIC 1 (Port:1) NIC 2 (Port:2)	2/Port N 4/Port N
Server B NC543i*	Port 1	7/Port N

[1] *The ProLiant BL2x220c G7 Server Blade embedded NC543i is automatically configured by the Onboard Administrator to Ethernet, if an Ethernet interconnect module is installed in bay 3, or to InfiniBand if a double-wide InfiniBand interconnect is installed in bay 3. To change the NC543i configuration from one type to another, power off all the ProLiant BL2x220c G7 Server Blades, and replace the interconnect module with the other type. Reboot the active Onboard Administrator or reseat all the ProLiant BL2x220c G7 Server Blades; the Onboard Administrator reconfigures all the embedded NC543i devices for the new interconnect type.*

AMC Telco I/O expansion blade

The following table lists the available configurations for AMC Telco devices installed in a c7000 device bay N (1-16).

Connection	Port Number	Connects to interconnect bay/ port
AMC Embedded (1)	Port 1 Port 2 Port 3 Port 4	1/Port N 2/Port N 3/Port N 4/Port N
AMC Embedded (2)	Port 5 Port 6 Port 7 Port 8	5/Port N 6/Port N 7/Port N 8/Port N

Full-height, double wide server blades such as ProLiant BL680c G7 Server

The following table lists the port mapping for full-height, double-wide server blades such as ProLiant BL680c G7 installed in c7000 full-height device bay N (2, 4, 6, or 8).

Connection	Port Number	Connects to interconnect bay/ port
A-Side Embedded NIC	NIC 1 NIC 2 NIC 3 NIC 4	1/Port N+8 2/Port N+8 1/Port N 2/Port N
B-Side Embedded NIC	NIC 5 NIC 6	1/Port N+7 2/Port N+7
A-Side Mezzanine 1	Port 1 Port 2 Port 3 Port 4	3/Port N 4/Port N 3/Port N+8 4/Port N+8
A-Side Mezzanine 2	Port 1 Port 2 Port 3 Port 4	5/Port N 6/Port N 7/Port N 8/Port N
A-Side Mezzanine 3	Port 1 Port 2 Port 3 Port 4	7/Port N+8 8/Port N+8 5/Port N+8 6/Port N+8
B-Side Mezzanine 4	Port 1 Port 2 Port 3 Port 4	7/Port N-1 8/Port N-1 5/Port N-1 6/Port N-1
B-Side Mezzanine 5	Port 1 Port 2 Port 3 Port 4	3/Port N+7 4/Port N+7 3/Port N-1 4/Port N-1

Table Continued

Connection	Port Number	Connects to interconnect bay/ port
B-Side Mezzanine 6 NIC only	Port 1 Port 2	1/Port N-1 2/Port N-1
B-Side Mezzanine 7	Port 1 Port 2 Port 3 Port 4	5/Port N+7 6/Port N+7 7/Port N+7 8/Port N+7

Firmware

To view firmware information for the device bay components and perform a manual discovery and manual update of firmware, click **Firmware**. For information about support requirements and performance issues, see **Enclosure Firmware Management**.

Firmware summary information

Row	Description
Bay	The device bay within the enclosure.
Device Model	The model number of the device.
Firmware Component	The component for which the firmware information is provided.
Current Version	The version of the firmware installed on the component.
Firmware ISO Version	The latest version of firmware available for installation on the component.

NOTE:

If the blade firmware does not match the DVD ISO firmware after a server is discovered or updated, an informational icon is displayed.

A letter included after the firmware version indicates a smart component release note revision. This revision is not a functional firmware update.

Manual discovery

A manual discovery performs a boot for discovery on the server, collects extended firmware information for that server, and reboots the server into normal operation.

To start the discovery process on the selected server, click **Start Manual Discovery**.

If Secure Boot is configured on the server blade, you cannot perform a manual discovery. The **Start Manual Discovery** button is grayed out. Secure Boot restricts users (including the Administrator) from performing this operation from the server blade OS or the iLO. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

Manual update

A manual update performs a boot for update on the server, updates the firmware for that server, and then reboots the server into normal operation.

To start the update process on the selected servers, click **Start Manual Update**.

If Secure Boot is configured on the server blade, you cannot perform a manual update. The **Start Manual Update** button is grayed out. Secure Boot restricts users (including the Administrator) from performing this operation from the server blade OS or the iLO. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

For more information about manual discovery and manual update, see **Initiating a manual update or discovery**.

Firmware log

This log displays detailed information for the last Enclosure Firmware Management operation executed on the server. This log is specific for the server, and is cleared any time a new Enclosure Firmware Management operation is started on the server. This log is also cleared when the server is removed from the enclosure and when in set factory mode.

The firmware log is the most useful resource to determine the progress of an Enclosure Firmware Management operation on a particular server.

For more information on the firmware log, see **Firmware management logs**.

Session log

This log displays detailed information for the last Enclosure Firmware Management operation executed on the server and logs the entire session to the iLO VSP. This log is specific for the server, and is cleared anytime a new Enclosure Firmware Management operation is started on the server. This log is also cleared when the server is removed from the enclosure.

For more information on the session log, see **Firmware management logs**.

Initiating a manual update or discovery

CAUTION:

Enclosure Firmware Management updates using an SPP image greater than 4GB and hosted from a web server might not work reliably.

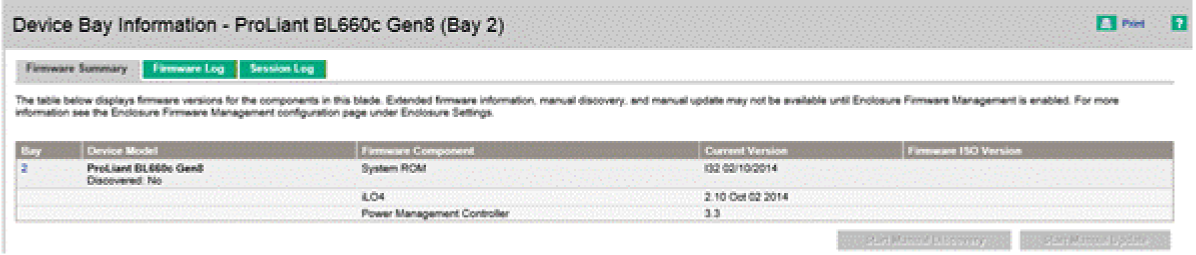
IMPORTANT:

While any Enclosure Firmware Management task is in progress, do not reboot the Onboard Administrator. Avoid shutting down or pulling out the blade from the enclosure.

NOTE:

If Secure Boot is configured on the server blade, you cannot perform a manual discovery or manual update. The **Start Manual Discovery** and **Start Manual Update** buttons are grayed out. Secure Boot restricts users (including the Administrator) from performing these operations from the server blade OS or the iLO. Boot operations can be performed only from the boot device configured in BIOS by the Administrator.

Initiating a manual update or discovery on individual servers



Device Bay Information - ProLiant BL660c Gen8 (Bay 2)

The table below displays firmware versions for the components in this blade. Extended firmware information, manual discovery, and manual update may not be available until Enclosure Firmware Management is enabled. For more information see the Enclosure Firmware Management configuration page under Enclosure Settings.

Bay	Device Model	Firmware Component	Current Version	Firmware ISO Version
2	ProLiant BL660c Gen8 Discovered: No	System ROM	I32 02/10/2014	
		iLO4	2.10 Oct 02 2014	
		Power Management Controller	3.3	

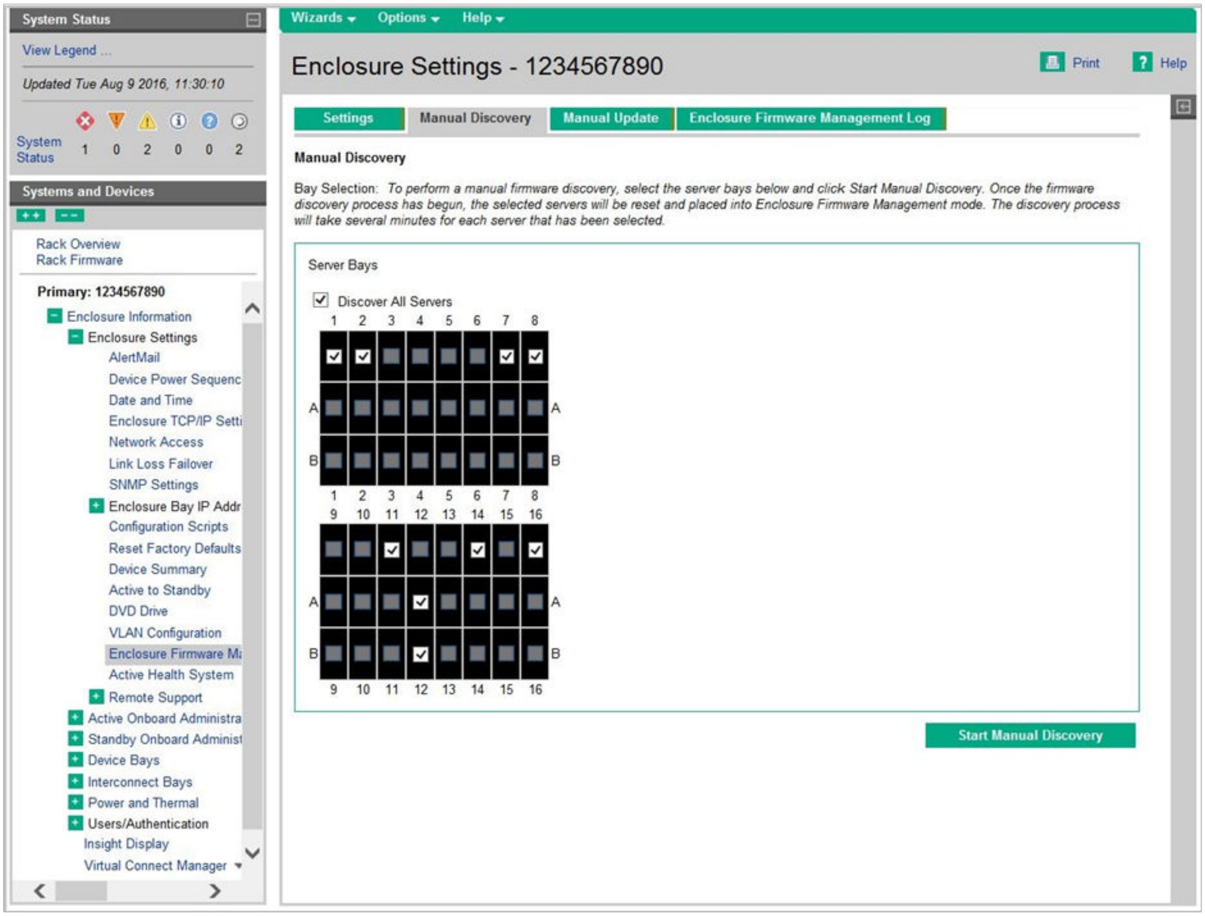
Procedure

1. Select **Device Bays** in the left tree view.
2. Select the appropriate bay to view, and then select **Firmware**.
3. Click **Start Manual Discovery** or **Start Manual Update**.

Initiating a manual discovery on multiple servers

Procedure

1. In the left tree view, select **Enclosure Settings** > **Enclosure Firmware Management**.
2. Select the **Manual Discovery** tab.



Enclosure Settings - 1234567890

Manual Discovery

Bay Selection: *To perform a manual firmware discovery, select the server bays below and click Start Manual Discovery. Once the firmware discovery process has begun, the selected servers will be reset and placed into Enclosure Firmware Management mode. The discovery process will take several minutes for each server that has been selected.*

Server Bays

☑ Discover All Servers

	1	2	3	4	5	6	7	8	
	☑	☑	□	□	□	□	☑	☑	
A	□	□	□	□	□	□	□	□	A
B	□	□	□	□	□	□	□	□	B
	1	2	3	4	5	6	7	8	

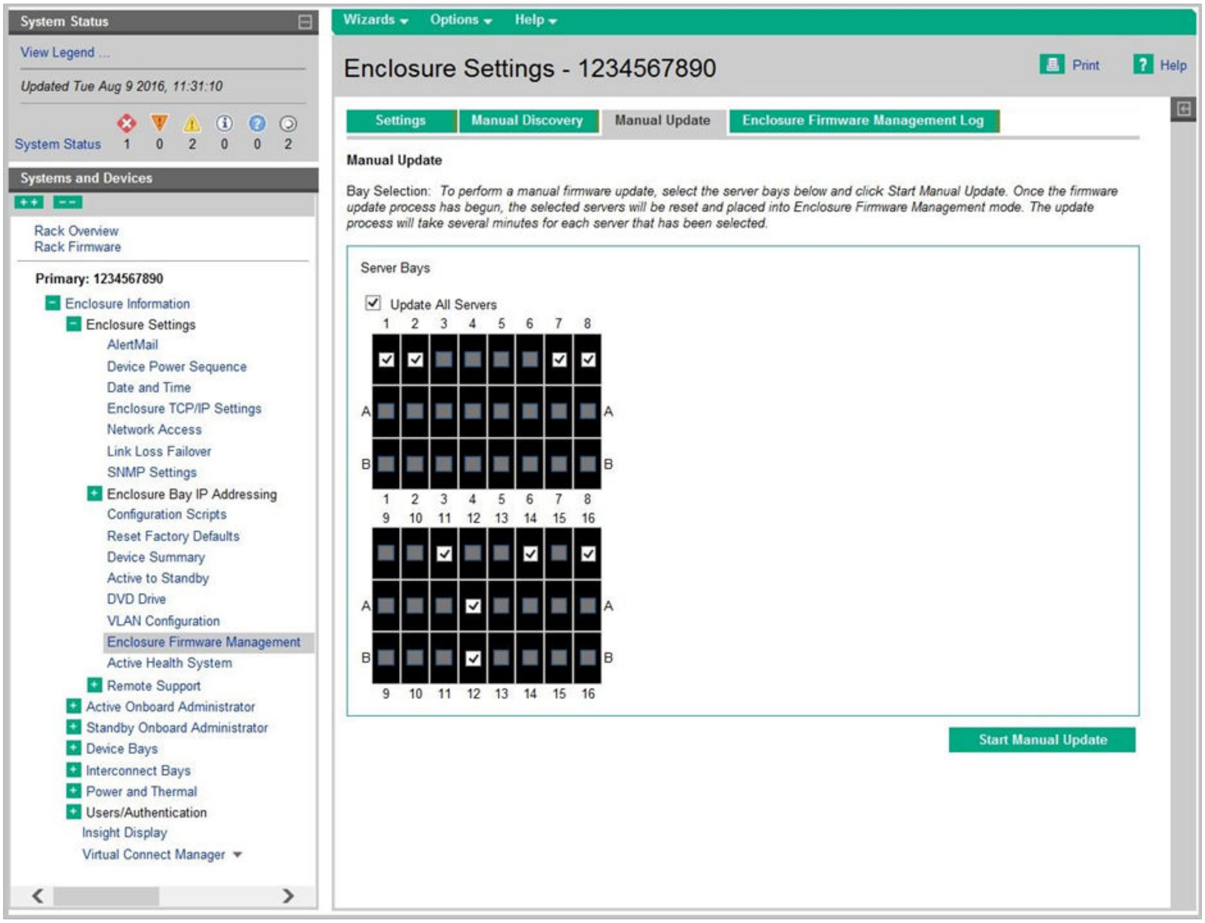
	9	10	11	12	13	14	15	16	
	□	□	☑	□	□	☑	□	☑	
A	□	□	□	☑	□	□	□	□	A
B	□	□	□	☑	□	□	□	□	B
	9	10	11	12	13	14	15	16	

3. Select the check box next to each of the appropriate server bays, or select the **Discover All Servers** check box.
4. Click **Start Manual Discovery**.

Initiating a manual update on multiple servers

Procedure

1. In the left tree view, select **Enclosure Settings** > **Enclosure Firmware Management**.
2. Select the **Manual Update** tab.



Enclosure Settings - 1234567890

Manual Update

Bay Selection: *To perform a manual firmware update, select the server bays below and click Start Manual Update. Once the firmware update process has begun, the selected servers will be reset and placed into Enclosure Firmware Management mode. The update process will take several minutes for each server that has been selected.*

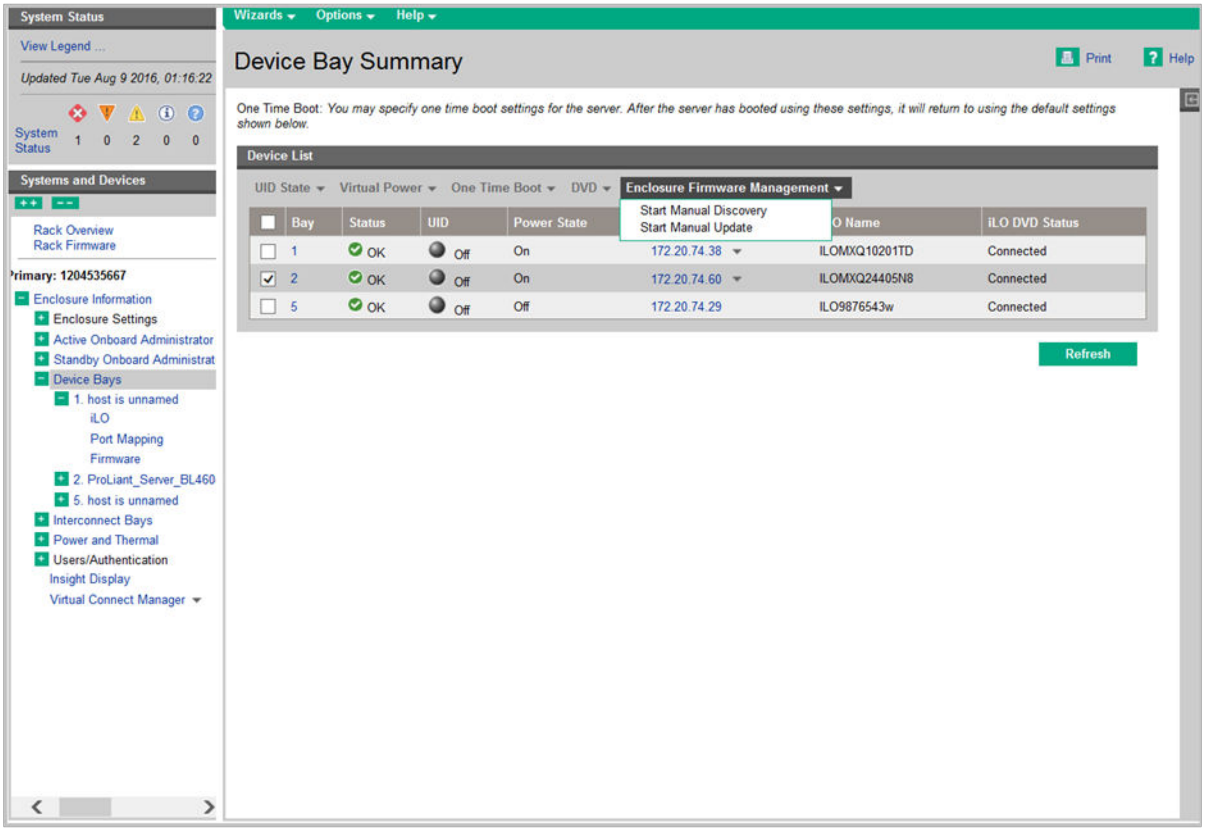
☑ Update All Servers

3. Select the check box next to each of the appropriate server bays, or select the **Update All Servers** check box.
4. Click **Start Manual Update**.

Initiating a manual discovery or update from the Device Bays screen

Procedure

1. In the left tree view, select **Device Bays**.
2. Select the check box next to the appropriate bay.
3. From the Firmware Management menu, select **Start Manual Discovery** or **Start Manual Update**.



Device Bay Summary

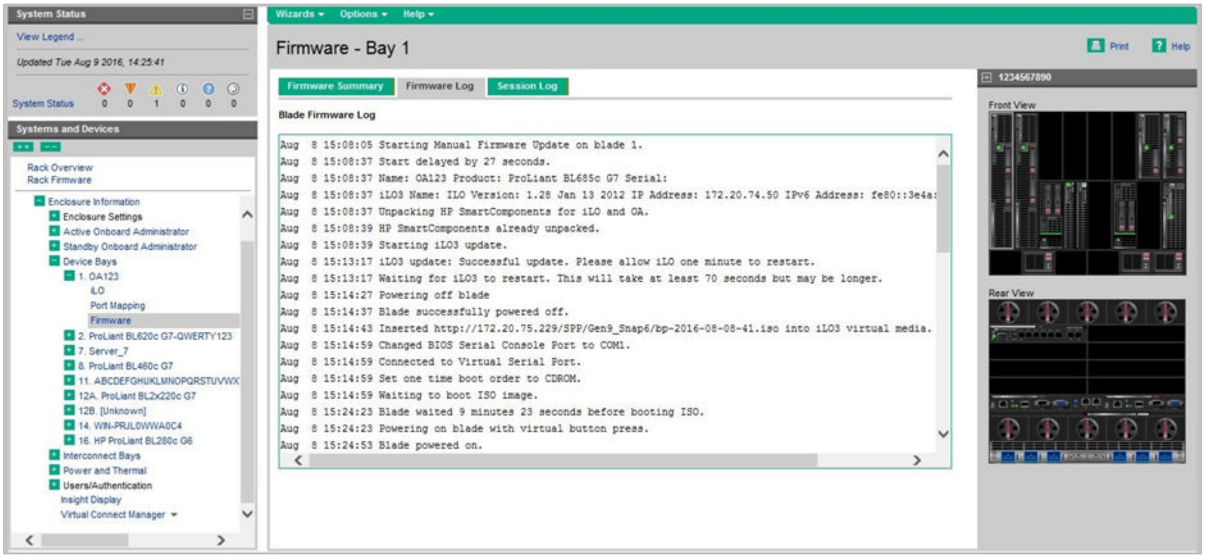
One Time Boot: *You may specify one time boot settings for the server. After the server has booted using these settings, it will return to using the default settings shown below.*

□	Bay	Status	UID	Power State		O Name	iLO DVD Status
□	1	OK	Off	On	172.20.74.38	ILOMXQ10201TD	Connected
☑	2	OK	Off	On	172.20.74.60	ILOMXQ24405N8	Connected
□	5	OK	Off	Off	172.20.74.29	ILO9876543w	Connected

Firmware management logs

Enclosure Firmware Management events are written to three logs. The following sections describe the type of events that are included in each log. All logs can be used to verify progress and completion tasks and for troubleshooting purposes.

Firmware Log



Firmware - Bay 1

Blade Firmware Log

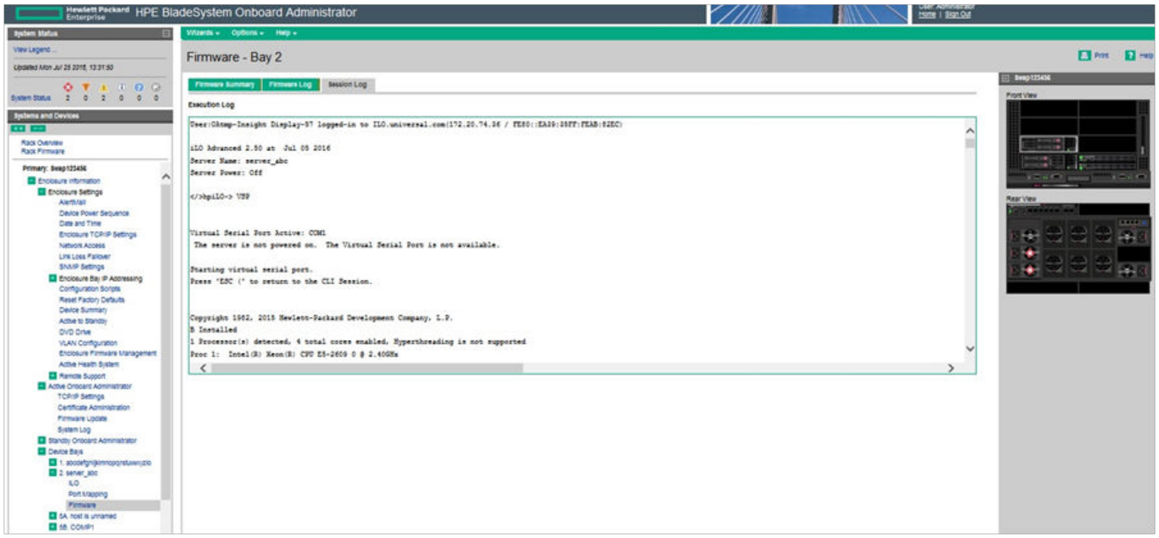
```
Aug  8 15:08:05 Starting Manual Firmware Update on blade 1.
Aug  8 15:08:37 Start delayed by 27 seconds.
Aug  8 15:08:37 Name: OA123 Product: ProLiant BL685c G7 Serial:
Aug  8 15:08:37 iLO3 Name: ILO Version: 1.28 Jan 13 2012 IP Address: 172.20.74.50 IPv6 Address: fe80::3e4a:
Aug  8 15:08:37 Unpacking HP SmartComponents for iLO and OA.
Aug  8 15:08:39 HP SmartComponents already unpacked.
Aug  8 15:08:39 Starting iLO3 update.
Aug  8 15:13:17 iLO3 update: Successful update. Please allow iLO one minute to restart.
Aug  8 15:13:17 Waiting for iLO3 to restart. This will take at least 70 seconds but may be longer.
Aug  8 15:14:27 Powering off blade
Aug  8 15:14:37 Blade successfully powered off.
Aug  8 15:14:43 Inserted http://172.20.75.229/SPP/Gen9_Snap6/bp-2016-08-08-41.iso into iLO3 virtual media.
Aug  8 15:14:59 Changed BIOS Serial Console Port to COM1.
Aug  8 15:14:59 Connected to Virtual Serial Port.
Aug  8 15:14:59 Set one time boot order to CDROM.
Aug  8 15:14:59 Waiting to boot ISO image.
Aug  8 15:24:23 Blade waited 9 minutes 23 seconds before booting ISO.
Aug  8 15:24:23 Powering on blade with virtual button press.
Aug  8 15:24:53 Blade powered on.
```

This log displays detailed information for the last Enclosure Firmware Management operation executed on the server. This log is specific for the server, and is cleared any time a new Enclosure Firmware Management operation is started on the server. This log is also cleared when the server is removed from the enclosure and when in set factory mode.

This log persists across OA reboots and power losses. It is retained on the Standby OA, if present.

The firmware log is the most useful resource to determine the progress of an Enclosure Firmware Management operation on a particular server.

Session Log

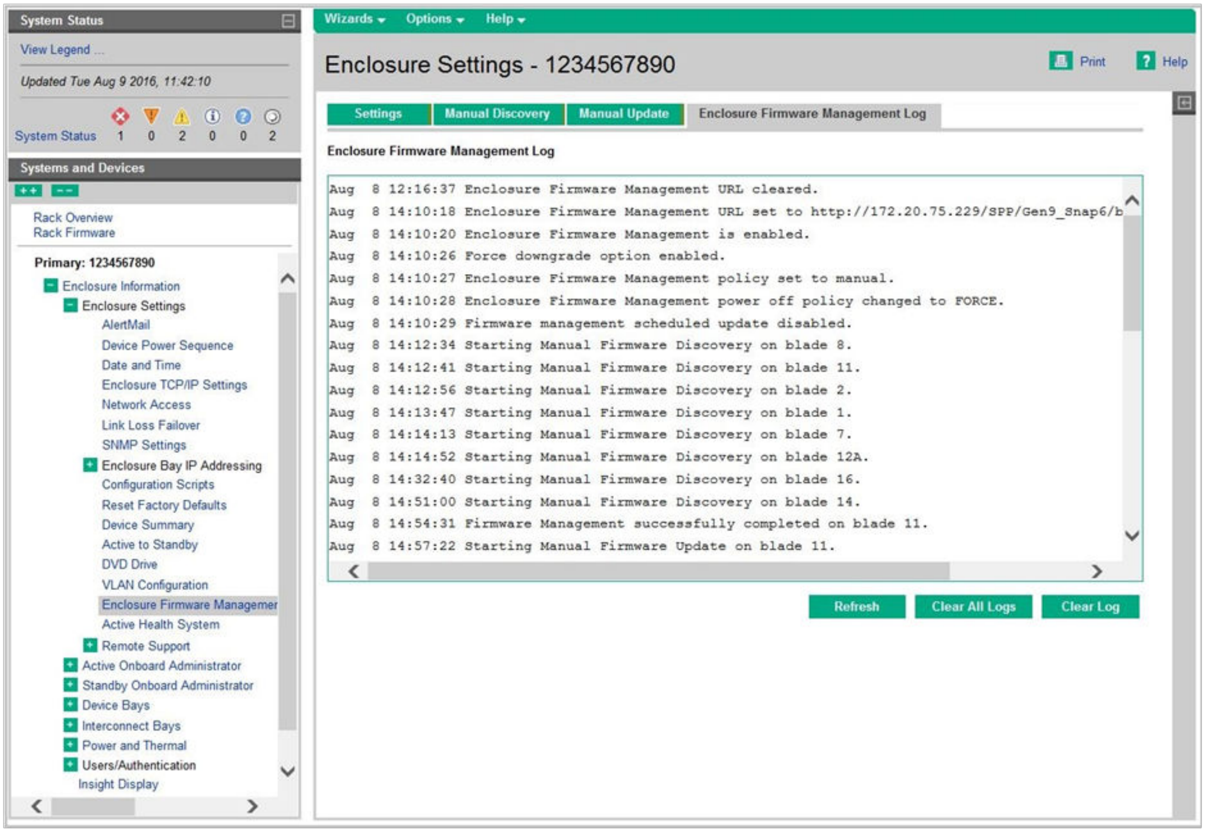


```
User:Oktmp-Insight Display-57 logged-in to ILO.universal.com(172.20.74.36 / FE80::EA39:35FF:FEAB:82EC)

iLO Advanced 2.50 at  Jul 05 2016
Server Name: server_abc
Server Power: Off

</>hpiLO-> VSP


Virtual Serial Port Active: COM1
 The server is not powered on.  The Virtual Serial Port is not available.

Starting virtual serial port.
Press 'ESC (' to return to the CLI Session.


Copyright 1982, 2015 Hewlett-Packard Development Company, L.P.
B Installed
1 Processor(s) detected, 4 total cores enabled, Hyperthreading is not supported
Proc 1:  Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz
```

This log displays detailed information for the last Enclosure Firmware Management operation executed on the server and logs the entire session to the iLO VSP. This log is specific for the server, and is cleared anytime a new Enclosure Firmware Management operation is started on the server. This log is also cleared when the server is removed from the enclosure.

This log persists across OA reboots and power losses. It is retained on the Standby OA, if present.

Enclosure Firmware Management Log



```
Aug  8 12:16:37 Enclosure Firmware Management URL cleared.
Aug  8 14:10:18 Enclosure Firmware Management URL set to http://172.20.75.229/SPP/Gen9_Snap6/b
Aug  8 14:10:20 Enclosure Firmware Management is enabled.
Aug  8 14:10:26 Force downgrade option enabled.
Aug  8 14:10:27 Enclosure Firmware Management policy set to manual.
Aug  8 14:10:28 Enclosure Firmware Management power off policy changed to FORCE.
Aug  8 14:10:29 Firmware management scheduled update disabled.
Aug  8 14:12:34 Starting Manual Firmware Discovery on blade 8.
Aug  8 14:12:41 Starting Manual Firmware Discovery on blade 11.
Aug  8 14:12:56 Starting Manual Firmware Discovery on blade 2.
Aug  8 14:13:47 Starting Manual Firmware Discovery on blade 1.
Aug  8 14:14:13 Starting Manual Firmware Discovery on blade 7.
Aug  8 14:14:52 Starting Manual Firmware Discovery on blade 12A.
Aug  8 14:32:40 Starting Manual Firmware Discovery on blade 16.
Aug  8 14:51:00 Starting Manual Firmware Discovery on blade 14.
Aug  8 14:54:31 Firmware Management successfully completed on blade 11.
Aug  8 14:57:22 Starting Manual Firmware Update on blade 11.
```

The Enclosure Firmware Management log provides a consolidated view of major Enclosure Firmware Management events, such as firmware image selections, policy and schedule changes, and firmware operations initiating and completing. This log does not contain the step-by-step details included in the firmware log for each server.

The Enclosure Firmware Management log persists across OA reboots and power losses. It is retained on the Standby OA, if present.

To view updated log information, click **Refresh**.

To clear information for the Enclosure Firmware Management log and the server-specific Firmware log and Session log, click **Clear All Logs**.

To clear information for the Enclosure Firmware Management log, click **Clear Log**.

CAUTION:

Once deleted, this data cannot be restored.

For information about event failures, see **Enclosure Firmware Management log**.

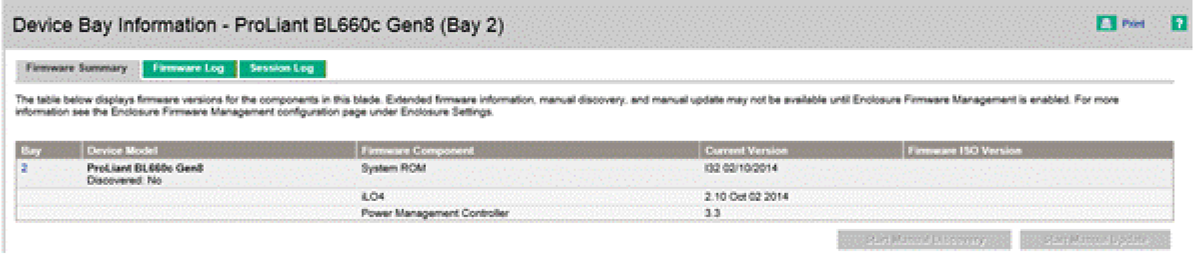
Viewing firmware versions

After an Enclosure Firmware Management task has successfully completed, review the firmware versions for all devices that were selected for updating. Successful completion of an Enclosure Firmware Management task might not indicate that firmware was updated to the versions on the ISO image. For more information, see **Firmware version variations**.

Server firmware

Select **Device Bays** in the left tree view. Select the appropriate bay to view, and then click **Firmware**.

The extended server firmware information appears on the Onboard Administrator GUI and CLI for each server. A firmware management log for each server blade displays the log of steps during the last firmware update or discovery event, and the firmware summary shows the date and time that the last discover or update occurred. If the server blade is removed from the enclosure, then this log is cleared. These logs are synchronized to the standby Onboard Administrator, if present, and the logs are stored in flash so the information is available after an Onboard Administrator reboot.



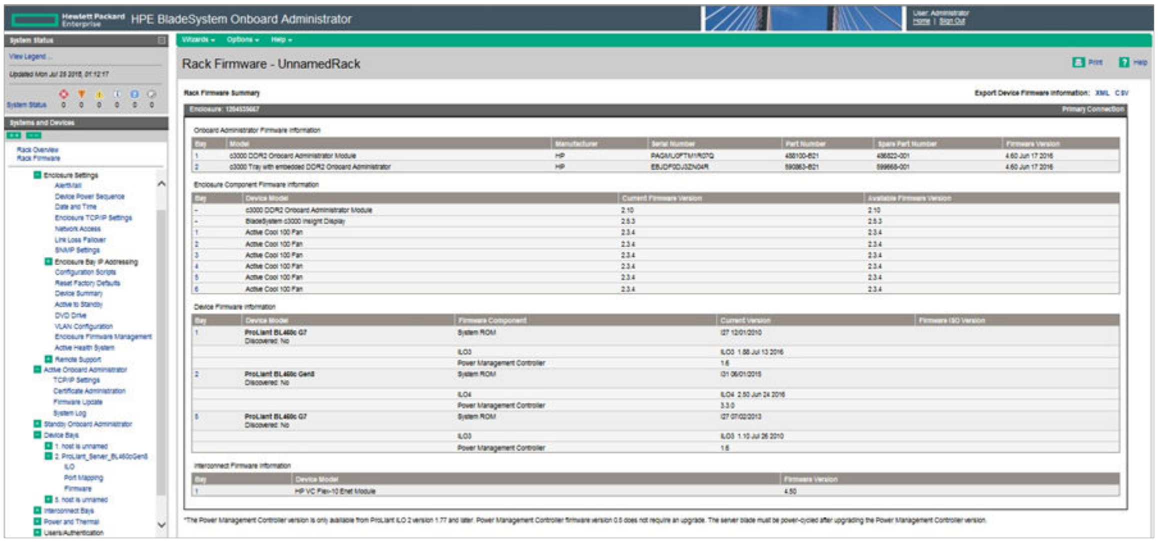
The table below displays firmware versions for the components in this blade. Extended firmware information, manual discovery, and manual update may not be available until Enclosure Firmware Management is enabled. For more information see the Enclosure Firmware Management configuration page under Enclosure Settings.

Bay	Device Model	Firmware Component	Current Version	Firmware ISO Version
2	ProLiant BL660c Gen8 Discovered: No	System ROM	I32 02/10/2014	
		iLO4	2.10 Oct 02 2014	
		Power Management Controller	3.3	

Rack firmware

Select **Rack Firmware** at the top of the left tree view pane.

The Onboard Administrator GUI or CLI provides a report of the current firmware inventory in each enclosure. For linked enclosures, the GUI provides the firmware across all linked enclosures. The report includes the current firmware version of the server BIOS, iLO, PMC, NIC, FC HBA, Smart Array, and each installed hard drive connected to the Smart Array. This information assists in the diagnosis of complex network or FC SAN issues caused by incorrect NIC or FC HBA firmware versions.



Rack Firmware - UnnamedRack

Rack Firmware Summary

Export Device Firmware Information: XML CSV

Enclosure: 1264533667 — Primary Connection

Onboard Administrator Firmware Information

Bay	Model	Manufacturer	Serial Number	Part Number	Spare Part Number	Firmware Version
1	c3000 DDR2 Onboard Administrator Module	HP	PAGMUOFTM1R07Q	456100-B21	456822-001	4.60 Jun 17 2016
2	c3000 Tray with embedded DDR2 Onboard Administrator	HP	EBJDF0DJ3ZN04R	590863-B21	599668-001	4.60 Jun 17 2016

Enclosure Component Firmware Information

Bay	Device Model	Current Firmware Version	Available Firmware Version
-	c3000 DDR2 Onboard Administrator Module	2.10	2.10
-	BladeSystem c3000 Insight Display	2.5.3	2.5.3
1	Active Cool 100 Fan	2.3.4	2.3.4
2	Active Cool 100 Fan	2.3.4	2.3.4
3	Active Cool 100 Fan	2.3.4	2.3.4
4	Active Cool 100 Fan	2.3.4	2.3.4
5	Active Cool 100 Fan	2.3.4	2.3.4
6	Active Cool 100 Fan	2.3.4	2.3.4

Device Firmware Information

Bay	Device Model	Firmware Component	Current Version	Firmware ISO Version
1	**ProLiant BL460c G7** Discovered: No	System ROM	I27 12/01/2010	
		iLO3	iLO3 1.88 Jul 13 2016	
		Power Management Controller	1.6	
2	**ProLiant BL460c Gen8** Discovered: No	System ROM	I31 06/01/2015	
		iLO4	iLO4 2.50 Jun 24 2016	
		Power Management Controller	3.3.0	
5	**ProLiant BL460c G7** Discovered: No	System ROM	I27 07/02/2013	
		iLO3	iLO3 1.10 Jul 26 2010	
		Power Management Controller	1.6	

Interconnect Firmware Information

Bay	Device Model	Firmware Version
1	HP VC Flex-10 Enet Module	4.50

*The Power Management Controller version is only available from ProLiant iLO 2 version 1.77 and later. Power Management Controller firmware version 0.5 does not require an upgrade. The server blade must be power-cycled after upgrading the Power Management Controller version.

Firmware version variations

The following scenarios might cause irregular firmware version or status information to appear:

- If a letter is included after the firmware version, this indicates a smart component release note revision. This is not a functional firmware update.
- If `No Component` appears as the Firmware ISO Version, this indicates that the SPP image does not contain firmware for that component. This scenario usually occurs with the Power Management Controller in ProLiant G7 servers.
- If the informational icon appears, the server blade firmware does not match the DVD ISO firmware after a server is discovered or updated.
- If the NIC, FC HBA, Smart Array, or installed hard drive connected to the Smart Array are flashed without using the Enclosure Firmware Management utility, then the Onboard Administrator cannot interpret this information and continues to report firmware information based on the most recent Enclosure Firmware Management operation.
- If firmware is not updated using the Enclosure Firmware Management utility, the utility's tracking and reporting will not reflect changes made using other tools.

  EFM tracking and reporting will not reflect the changes made using other tools such as HP SUM and SIM if firmware on a blade was not updated using EFM. Correct versions of firmware will be reported once EFM discovery or update is performed.

Storage blades

In the **Systems and Devices** menu, the Device Bays category lists server blades and storage blades. Selecting a storage blade menu item displays the status page of the storage blade (selecting the **+** symbol to the left of the menu item does not expand the storage blade). Three tabs are available that display specific information about the storage blade: **Status**, **Information**, and **Virtual Devices**.

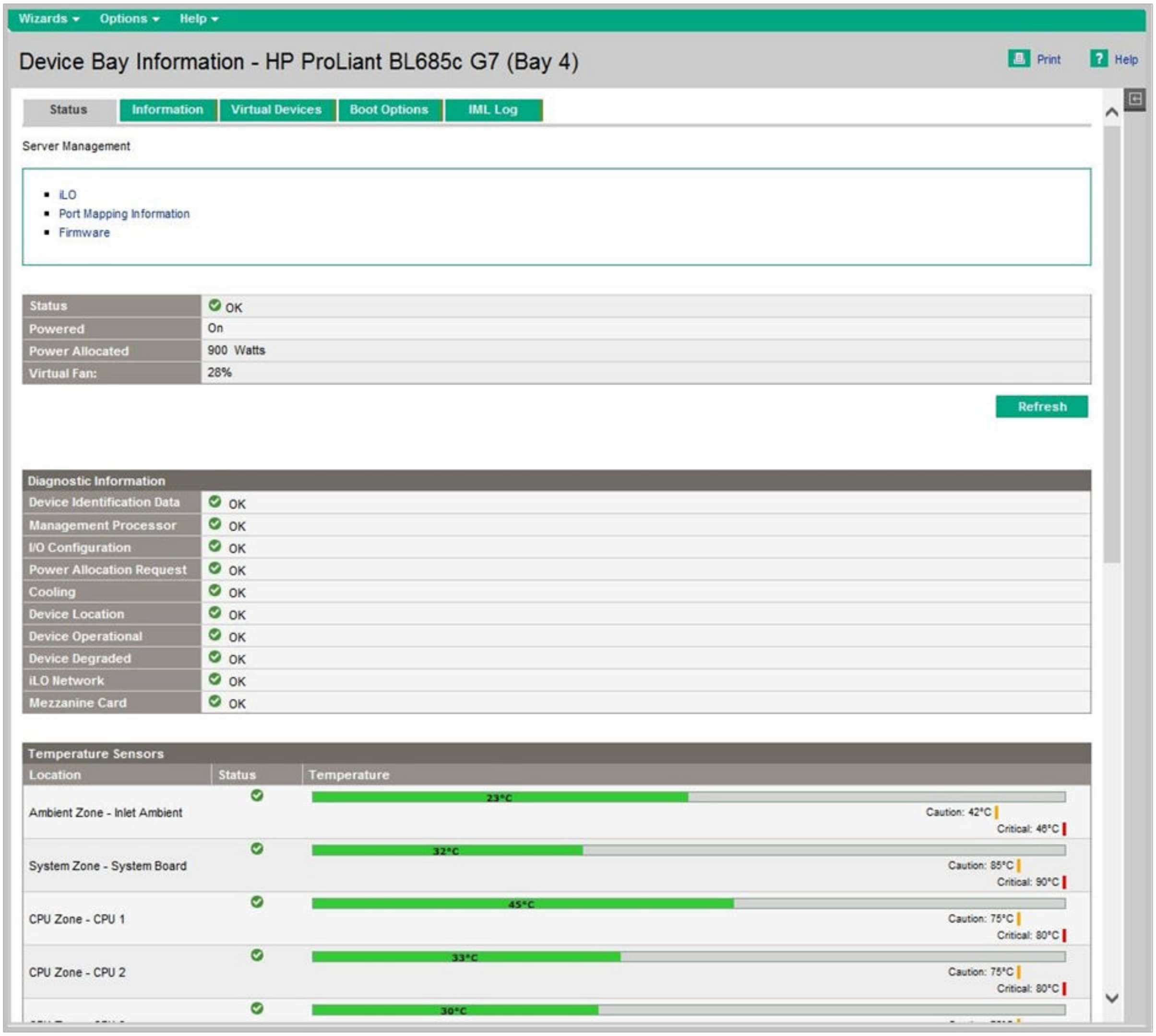
Storage blades are inserted into the enclosure adjacent to server blades following physical placement rules and ensuring the storage blade is not powered on before powering on and associating a server blade with it.

When using half-height server blades, the storage blade must be placed in the slot in the enclosure to the left of the server blade. For each server blade installed in the enclosure, an associated storage blade can be placed in the enclosure to the left of the server blade (maximum of eight server blades and eight storage blades).

When using full-height server blades, the storage blade must be placed into the lower slot in the enclosure to the left of the server blade. Placing the storage blade to the top left slot of the enclosure causes a partner device error. You can have a half-height server blade in the slot to the top-left of a full-height server blade while a storage blade is to the lower left of the full-height server blade.

Full-height server blades require a mezzanine card to communicate with the appropriate storage blade. If a storage blade is placed correctly next to a full-height server blade but the server blade is missing the proper mezzanine card, then a Configuration error (not a Partner Device Error) occurs.

If power to a server blade is disconnected, power to the associated storage blade is also disconnected.



Device Bay Information - HP ProLiant BL685c G7 (Bay 4)

Server Management

- iLO
- Port Mapping Information
- Firmware

Status	✓ OK
Powered	On
Power Allocated	900 Watts
Virtual Fan:	28%

Diagnostic Information	
Device Identification Data	✓ OK
Management Processor	✓ OK
I/O Configuration	✓ OK
Power Allocation Request	✓ OK
Cooling	✓ OK
Device Location	✓ OK
Device Operational	✓ OK
Device Degraded	✓ OK
iLO Network	✓ OK
Mezzanine Card	✓ OK

Temperature Sensors

Location	Status	Temperature
Ambient Zone - Inlet Ambient	✓	23°C Caution: 42°C Critical: 46°C
System Zone - System Board	✓	32°C Caution: 85°C Critical: 90°C
CPU Zone - CPU 1	✓	45°C Caution: 75°C Critical: 80°C
CPU Zone - CPU 2	✓	33°C Caution: 75°C Critical: 80°C
	✓	30°C

Row	Description
Status	The overall status of the storage blade. Possible values are Unknown, OK, Degraded, and Failed.
Powered	The power state of the storage blade. Possible values are On or Off.
Power Allocated	The amount of power allocated for use by the storage blade in watts.
Virtual Fan	The percentage of maximum RPM of the virtual fan.
Partner Device [1]	Displays the server blade and bay the storage blade is associated with.

[1] *Not shown*

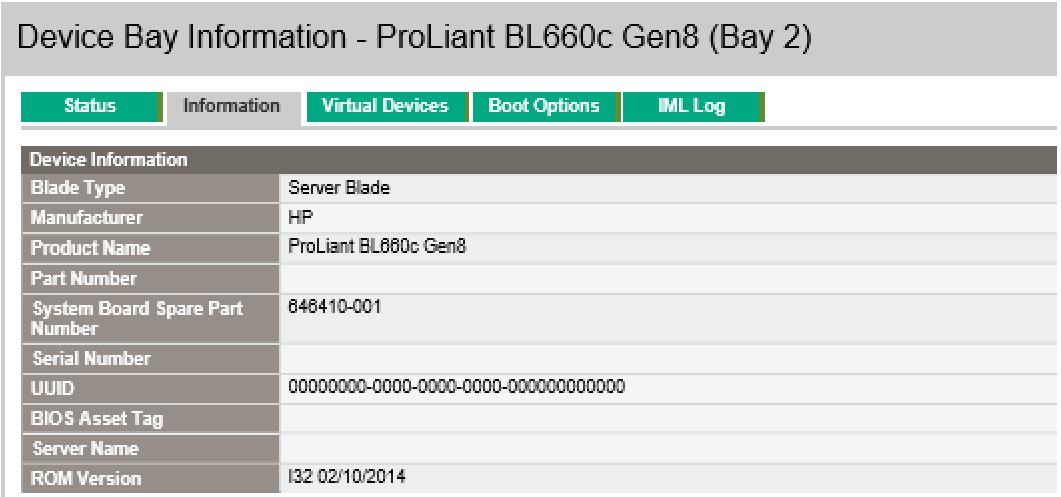
Diagnostic Information

Diagnostic information is gathered by polling a device microcontroller (resulting in a degraded status if a failure has occurred) or is sent by the device microcontroller, without being polled, to report a failure.

Row	Description
Device Identification Data	Information such as model name, part number, serial number, and other information used to identify the device is checked. This data is also referred to as FRU data. If the data is not present or not readable by the Onboard Administrator, a device identification data error displays. Possible values are OK or Error.
Management Processor	Status of the storage controller's management interface processor. Possible values are OK or Error.
Temperature	Temperature is above the warning threshold. Possible values are OK or Temperature Warning.
Overheat Check	Temperature is above the danger threshold. Possible values are OK or Critical temperature threshold reached.
Power Allocation Request	There is insufficient power to adequately power the storage blade. Possible values are OK or Insufficient enclosure power.
Cooling	There is an insufficient number of fans to properly cool this storage blade or the fan configuration is incorrect. Possible values are OK or Insufficient fans for enclosure cooling.
Device Location	Storage blade bay configuration status. Possible values are OK or Incorrect location for proper device cooling.
Device Operational	Status of the storage blade. Possible values are OK or Error
Device Degraded	Device has failed; status was requested by the Onboard Administrator. Possible values are OK or Error
Disk Tray	DVD Drive. Possible values are Disk Tray is OPEN or Disk Tray is CLOSED.
Partner Device Presence	The storage blade has a partner server. It must have a server next to it in the proper configuration. Possible values are OK or No adjacent partner found.
Power Sequence	The storage blade must always be powered up first. If a storage blade is inserted next to a server blade that is already powered up, it will be denied power. The server blade must be powered down, so that the storage blade will power up, and then the server blade can be powered up again. Possible values are OK or Potential partner device is already ON.
Partner Device Link	When degraded, two storage blades have been placed next to each other in the enclosure. Possible values are OK or Inappropriate device in adjacent bay.
Virtual Connect Configured	Possible values are Configured for Virtual Connect or Not configured for Virtual Connect.

Temperature sensors information

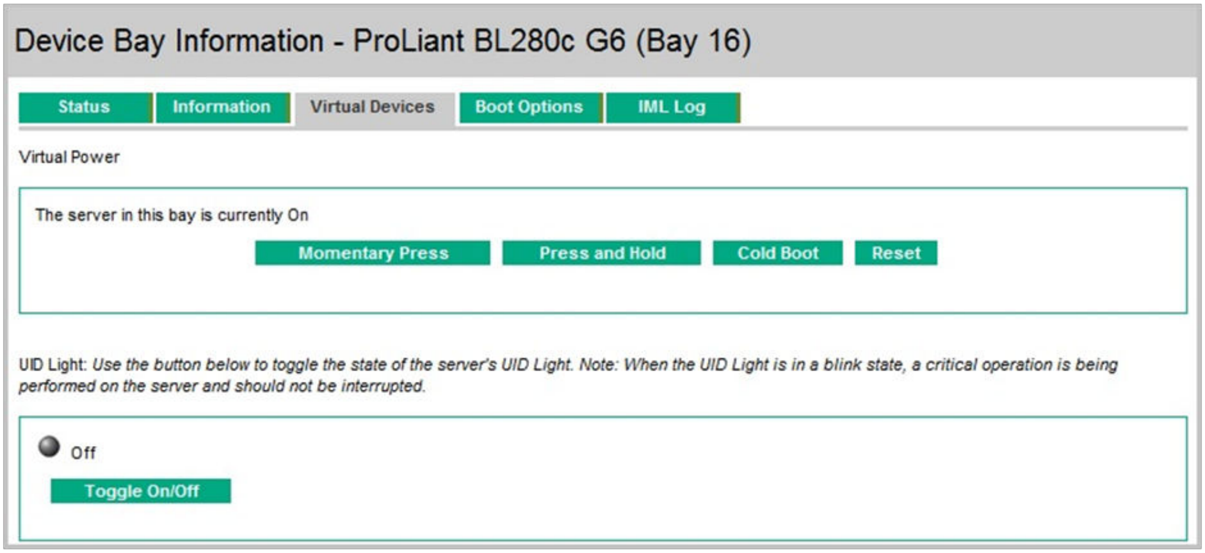
Column	Description
Location	Location of sensor in the device.
Status	This is the status of the temperature sensor. The status matches the graphic presentation of the temperature.
Temperature	Graphic presentation of temperature.



Device Bay Information - ProLiant BL660c Gen8 (Bay 2)

Device Information	
Blade Type	Server Blade
Manufacturer	HP
Product Name	ProLiant BL660c Gen8
Part Number	
System Board Spare Part Number	646410-001
Serial Number	
UUID	00000000-0000-0000-0000-000000000000
BIOS Asset Tag	
Server Name	
ROM Version	I32 02/10/2014

Row	Description
Blade Type	The type of device installed in the bay
Manufacturer	The manufacturer of the device installed in the bay
Product Name	The common descriptive name of the server blade
Part Number	The part number to be used when ordering an additional or replacement server blade of this type
System board spare part number	The part number to be used when ordering a replacement system board for this device
Serial Number	The unique serial number of the server blade
ROM Version	ROM version number



Device Bay Information - ProLiant BL280c G6 (Bay 16)

Virtual Power

The server in this bay is currently On

UID Light: *Use the button below to toggle the state of the server's UID Light. Note: When the UID Light is in a blink state, a critical operation is being performed on the server and should not be interrupted.*

● Off

The blade UID LED for the storage blade is toggled from this screen. To toggle the blade UID LED, click **Toggle On/Off**.

The icon directly above the Toggle On/Off button is gray when the blade UID LED is inactive and is blue when active.

I/O expansion blade information

Selecting a specific I/O expansion blade displays the Device Bay Information—Bay xx page, where xx is the bay selected. Information provided on this screen includes tabs for Status, Information, and Virtual Devices.

Status tab

Status information

Row	Description
Status	The overall status of the blade. Possible values are Unknown, OK, Degraded, or Failed
Powered	The power state of the blade. Possible values are On or Off
Power Allocated	The amount of power allocated to the blade in watts.
Partner Device	The server blade the I/O expansion blade is partnered with
Virtual Fan	The percentage of maximum RPM of the virtual fan.

The information in the status information table is current as of the last download. Click **Refresh** to update the status information.

Diagnostic information

Diagnostic information is gathered by polling a device microcontroller (resulting in a degraded status if a failure has occurred) or is sent by the device microcontroller, without being polled to report a failure.

Row	Description
Device Identification Data	Information such as model name, part number, serial number, and other information used to identify the device is checked. This data is also referred to as FRU data. If the data is not present or not readable by the Onboard Administrator, a device identification data error displays. Possible values are OK or Error.
Management Processor	Status of the iLO. Possible values are OK or Error.
I/O Configuration	Device bay configuration is incorrect. If a storage blade is partnered with a full-height server blade and the server blade does not have the correct mezzanine card, then an invalid I/O configuration results. Possible values are OK or I/O mismatch detected.
Power Allocation Request	There is insufficient power to adequately power this blade. Possible values are OK or Insufficient enclosure power.
Cooling	There is an insufficient number of fans to properly cool this server blade, or the fan configuration is incorrect. Possible values are OK or Insufficient fans for enclosure cooling.
Device Location	The I/O blade is in the wrong slot in the enclosure according to the current fan configuration. Possible values are OK or Incorrect location for proper device cooling.
Device Operational	Device has failed. Status was not requested by the Onboard Administrator. Possible values are OK or Error
Device Degraded	Device has failed. Status was requested by the Onboard Administrator. Possible values are OK or Error

Table Continued

Row	Description
Partner Device Presence	The I/O expansion blade has a partner server. It must have a server next to it in the proper configuration. Possible values are OK or No adjacent partner found.
Power Sequence	The I/O expansion blade must always be powered up first. If an I/O expansion blade is inserted next to a server blade that is already powered up, it is denied power. The server blade must be powered down so the I/O expansion blade can power up, and then the server blade can be powered up again. Possible values are OK or Potential partner device is already ON.
Partner Device Link	Possible values are OK or Inappropriate device in adjacent bay. This information does not display if the server blade is not partnered with a storage/expansion blade.

Temperature sensors

Column	Description
Sensor	The sensor number
Location	Location of sensor in the device
Status	This is the status of the temperature sensor. The status matches the graphic presentation of the temperature.
Temperature	Graphic presentation of temperature

I/O expansion blade virtual devices tab

UID Light

Clicking **Toggle On/Off** turns the UID light on the I/O expansion blade on (blue) or off (gray) for easy identification of the selected I/O expansion blade.

I/O expansion blade information tab

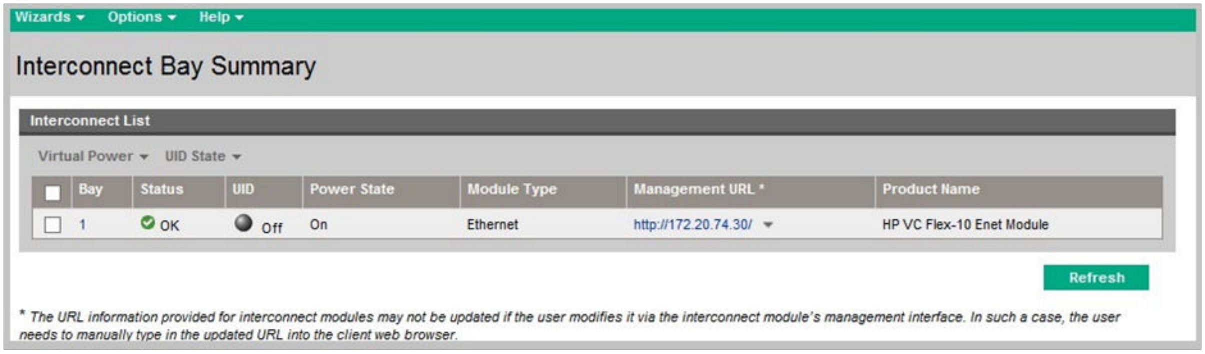
Device Information

Row	Description
Blade Type	I/O Expansion Blade
Manufacturer	Name of the company that manufactured the I/O expansion blade
Product Name	Common descriptive name for the I/O expansion blade
Part Number	Part number to be used when ordering an additional or replacement I/O expansion blade of this type
System Board Spare Part Number	Part number to be used when ordering an additional or replacement system board of this type
Serial Number	Unique serial number for the I/O expansion blade
ROM Version	ROM version number

Interconnect bays

Interconnect Bay Summary screen

In the Enclosure Information menu, the Interconnect Bays category lists all the interconnect devices within the enclosure. Selecting the interconnect bays menu item directly opens the interconnect device list with a grid that shows the status of each interconnect device within the enclosure as well as the UID status, power state, module type, management URL, and product name. These parameters are described in the table near the end of this section.



Interconnect Bay Summary

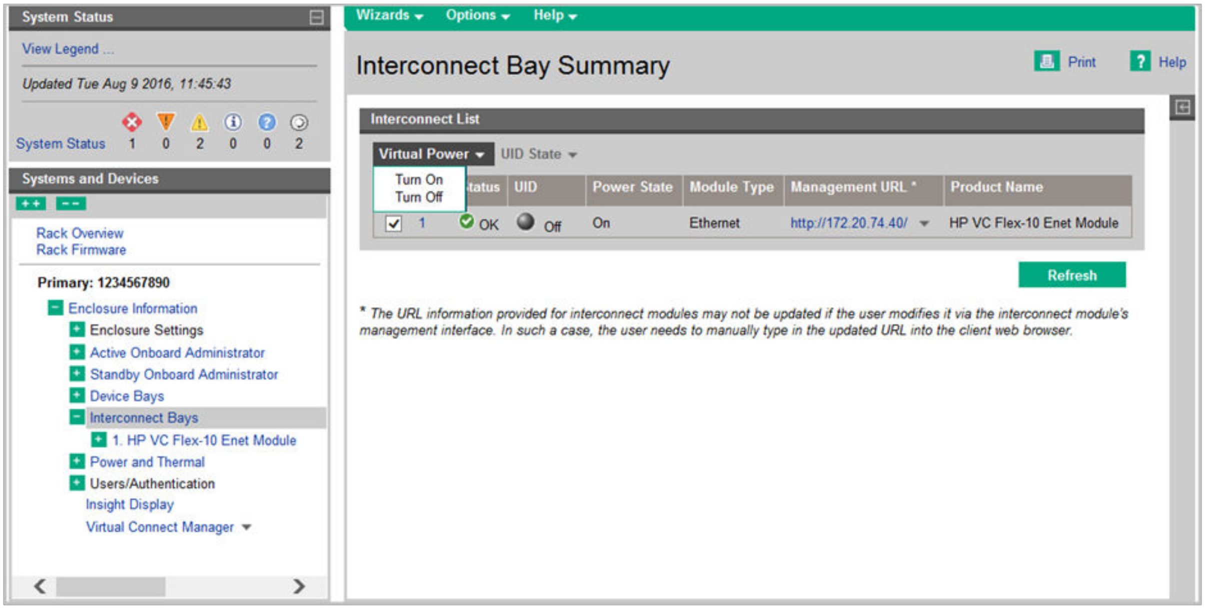
Interconnect List

□	Bay	Status	UID	Power State	Module Type	Management URL *	Product Name
□	1	✓ OK	● Off	On	Ethernet	http://172.20.74.30/ ▾	HP VC Flex-10 Enet Module

* *The URL information provided for interconnect modules may not be updated if the user modifies it via the interconnect module's management interface. In such a case, the user needs to manually type in the updated URL into the client web browser.*

The check box in the first column on the top row toggles all check boxes on or off for all interconnect devices. This feature is useful if, for example, you want to toggle the UID state for all interconnect devices at the same time. Otherwise, the first column contains check boxes that can be used to select individual interconnects. After the appropriate interconnects are selected, you can use the Virtual Power or UID State dropdown menus (click the corresponding down arrow) to perform the appropriate action.

The Virtual Power menu shown in the following figure enables you to turn an interconnect device on or off. Hewlett Packard Enterprise recommends that only one device be turned on or off at a time using this feature.



Updated Tue Aug 9 2016, 11:45:43

1	0	2	0	0	2

Primary: 1234567890

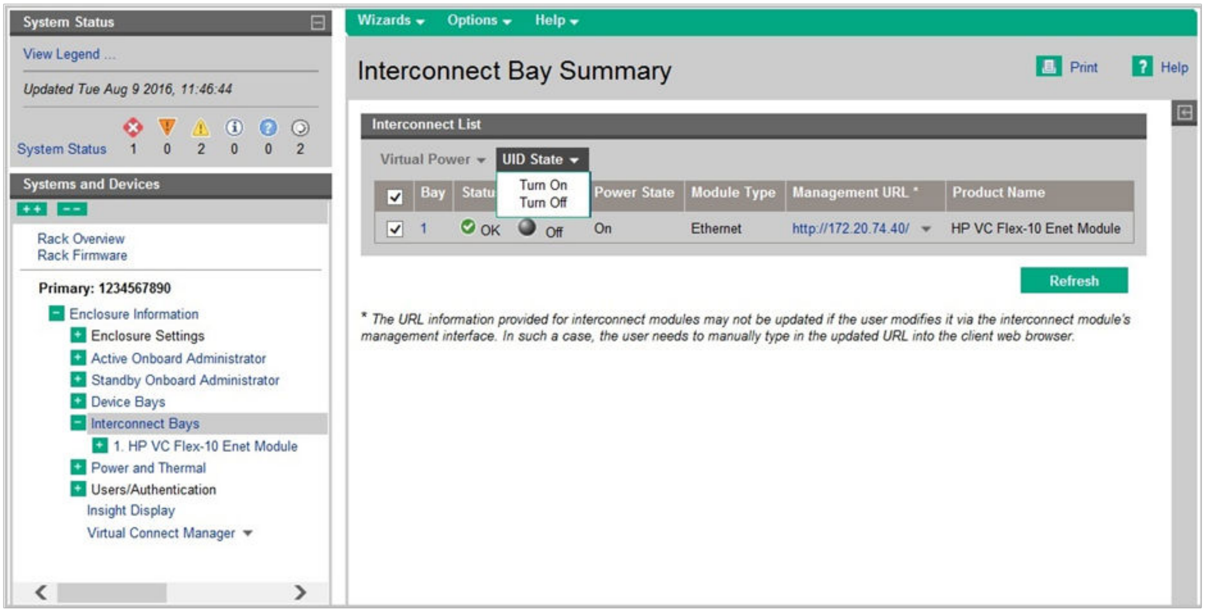
Interconnect Bay Summary

Interconnect List

		Status	UID	Power State	Module Type	Management URL *	Product Name
☑	1	✓ OK	● Off	On	Ethernet	http://172.20.74.40/ ▾	HP VC Flex-10 Enet Module

* *The URL information provided for interconnect modules may not be updated if the user modifies it via the interconnect module's management interface. In such a case, the user needs to manually type in the updated URL into the client web browser.*

The UID State menu shown in the following figure is used to set the UID LED on the interconnect device. Turning on the UID LED assists in locating a specific interconnect device within an enclosure. These LEDs can be turned on or off one at a time or as groups, depending on the check boxes selected.



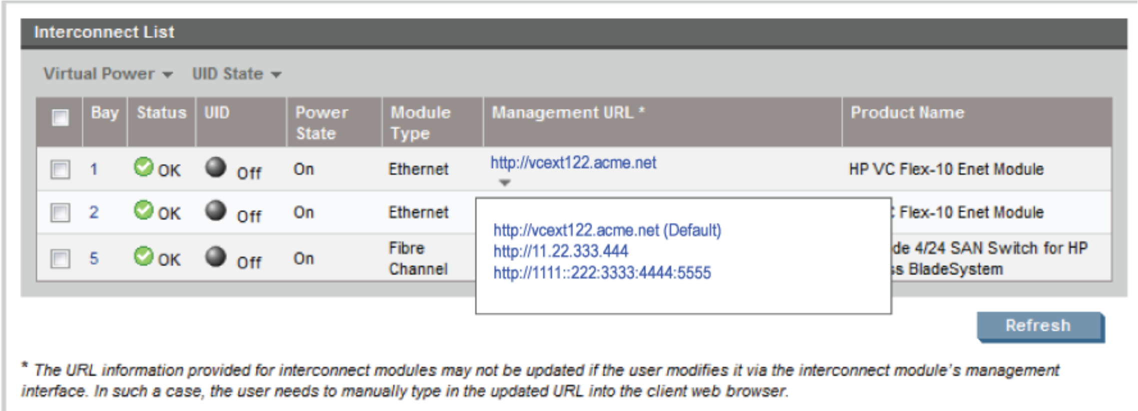
Interconnect Bay Summary

Interconnect List

☑	Bay	Status	UID	Power State	Module Type	Management URL *	Product Name
☑	1	OK	Off	On	Ethernet	http://172.20.74.40/	HP VC Flex-10 Enet Module

* The URL information provided for interconnect modules may not be updated if the user modifies it via the interconnect module's management interface. In such a case, the user needs to manually type in the updated URL into the client web browser.

To view available Management Console address links (IPv4 and IPv6), click the down arrow alongside the Management URL address. A popup appears, as in the following figure. When FQDN link support is enabled and certain DNS configuration requirements are met, an FQDN-based address displays as the default Management URL (as shown). For more information about enabling FQDN link support, see **Network Access**.



Interconnect List

□	Bay	Status	UID	Power State	Module Type	Management URL *	Product Name
□	1	OK	Off	On	Ethernet	http://vcext122.acme.net	HP VC Flex-10 Enet Module
□	2	OK	Off	On	Ethernet		: Flex-10 Enet Module
□	5	OK	Off	On	Fibre Channel		de 4/24 SAN Switch for HP s BladeSystem

http://vcext122.acme.net (Default)
http://11.22.333.444
http://1111::222:3333:4444:5555

* The URL information provided for interconnect modules may not be updated if the user modifies it via the interconnect module's management interface. In such a case, the user needs to manually type in the updated URL into the client web browser.

Column	Description
Check box	Click the check boxes next to the bay or bays where you want to apply the Virtual Power and UID State features.
Bay	Bay in the enclosure of the corresponding interconnect device. This field displays only populated bays. Empty bays are not displayed in this table.
Status	Overall status of the interconnect device. Possible values are Unknown, OK, Degraded, and Failed.
UID	Status of the UID on the interconnect device. Possible values are On (blue) or Off (gray).
Power State	Power state of the interconnect device. Possible values are On or Off.
Module Type	Network interface type for the interconnect device installed in this bay. Possible values are Ethernet or fiber.

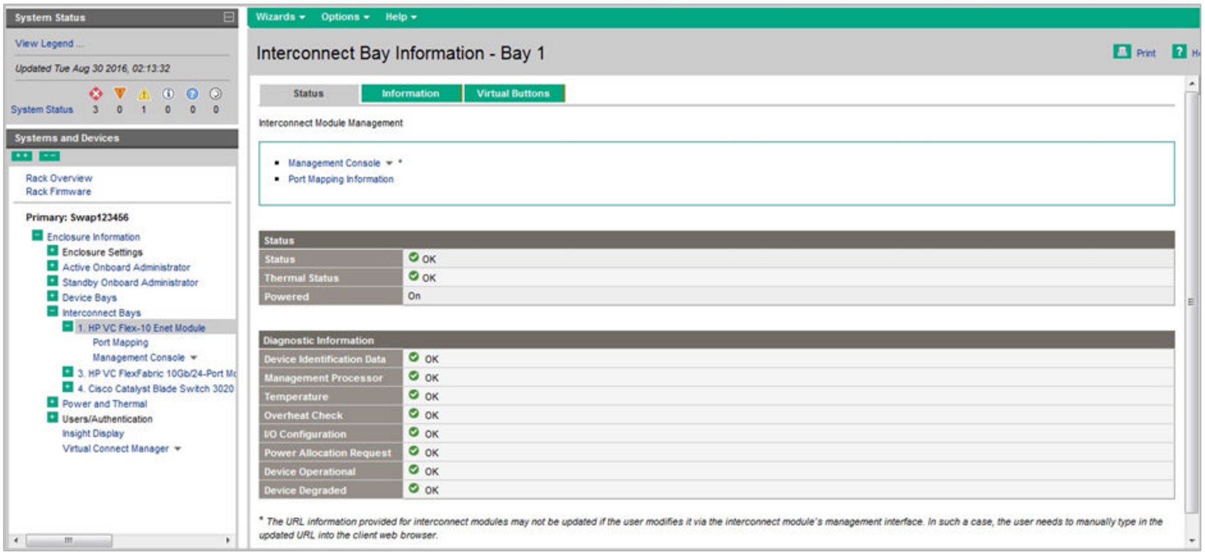
Table Continued

Column	Description
Management URL	IPv4 address where the interconnect device can be managed and configured for use in the network. To view available Management URL address links (IPv4 and IPv6), click the down arrow to display a dropdown menu. When FQDN link support is enabled and certain DNS configuration requirements are met, an FQDN-based address displays as the default Management URL. For more information about enabling FQDN link support, see **Network Access**.
Product Name	Common descriptive name for the interconnect device.

Information on this page is current as of the last download. To view updated information, click **Refresh**.

Interconnect Bay screen

The Interconnect Bay screen displays information about the bays where switches and routers can be placed. Also, you can view the Onboard Administrator modules.



Interconnect Bay Information - Bay 1

Interconnect Module Management

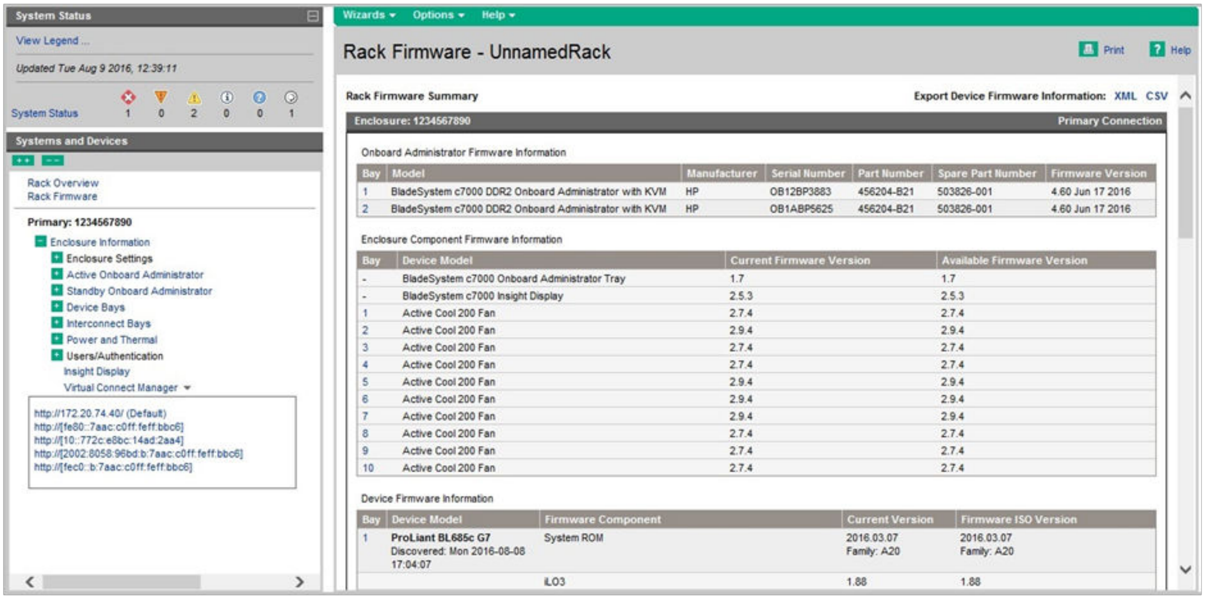
- Management Console *
- Port Mapping Information

Status	
Status	✓ OK
Thermal Status	✓ OK
Powered	On

Diagnostic Information	
Device Identification Data	✓ OK
Management Processor	✓ OK
Temperature	✓ OK
Overheat Check	✓ OK
I/O Configuration	✓ OK
Power Allocation Request	✓ OK
Device Operational	✓ OK
Device Degraded	✓ OK

** The URL information provided for interconnect modules may not be updated if the user modifies it via the interconnect module's management interface. In such a case, the user needs to manually type in the updated URL into the client web browser.*

To connect to the Management Console, click the **Management Console** link. To view available Management Console address links (IPv4 and IPv6), click the down arrow alongside the link. You can also connect to the Management Console from the navigation tree, as shown in the following figure. In either case, when FQDN link support is enabled and certain DNS configuration requirements are met, an FQDN-based address displays as the default link. For more information about enabling FQDN link support, see **Network Access**.



Updated Tue Aug 9 2016, 12:39:11

System Status 1 0 2 0 0 1

Rack Overview
Rack Firmware

Primary: 1234567890

- Enclosure Information
  - Enclosure Settings
  - Active Onboard Administrator
  - Standby Onboard Administrator
  - Device Bays
  - Interconnect Bays
  - Power and Thermal
  - Users/Authentication
  - Insight Display
  - Virtual Connect Manager

http://172.20.74.40/ (Default)
http://[fe80::7aac:c0ff:feff:bbc6]
http://[10::772c:e8bc:14ad:2aa4]
http://[2002:8058:96bd:b:7aac:c0ff:feff:bbc6]
http://[fec0::b:7aac:c0ff:feff:bbc6]

Rack Firmware - UnnamedRack

Rack Firmware Summary

Export Device Firmware Information: XML CSV

Enclosure: 1234567890 Primary Connection

Onboard Administrator Firmware Information

Bay	Model	Manufacturer	Serial Number	Part Number	Spare Part Number	Firmware Version
1	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB12BP3883	456204-B21	503826-001	4.60 Jun 17 2016
2	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB1ABP5625	456204-B21	503826-001	4.60 Jun 17 2016

Enclosure Component Firmware Information

Bay	Device Model	Current Firmware Version	Available Firmware Version
-	BladeSystem c7000 Onboard Administrator Tray	1.7	1.7
-	BladeSystem c7000 Insight Display	2.5.3	2.5.3
1	Active Cool 200 Fan	2.7.4	2.7.4
2	Active Cool 200 Fan	2.9.4	2.9.4
3	Active Cool 200 Fan	2.7.4	2.7.4
4	Active Cool 200 Fan	2.7.4	2.7.4
5	Active Cool 200 Fan	2.9.4	2.9.4
6	Active Cool 200 Fan	2.9.4	2.9.4
7	Active Cool 200 Fan	2.9.4	2.9.4
8	Active Cool 200 Fan	2.7.4	2.7.4
9	Active Cool 200 Fan	2.7.4	2.7.4
10	Active Cool 200 Fan	2.7.4	2.7.4

Device Firmware Information

Bay	Device Model	Firmware Component	Current Version	Firmware ISO Version
1	**ProLiant BL685c G7** Discovered: Mon 2016-08-08 17:04:07	System ROM	2016.03.07 Family: A20	2016.03.07 Family: A20
		iLO3	1.88	1.88

To display port mapping information on the interconnect bay you have selected, click the **Port Mapping Interconnect** link. The port mapping information can also be selected from the navigation tree.

Status information

Row	Description
Status	The overall status of the interconnect device. Possible values are Unknown, OK, Degraded, and Failed.
Thermal Status	The thermal status of the interconnect device. Possible values are Unknown, OK, Degraded, and Failed.
Powered	The power state of the blade. Possible values are On, Off, or Delayed.
Power Delay Remaining	The number of seconds remaining before the device powers on.

Diagnostic Information

Row	Description
Device Identification Data	Information such as model name, part number, serial number, and other information used to identify the device is checked. This data is also referred to as FRU data. If the data is not present or not readable by the Onboard Administrator, a device identification data error displays. Possible values are OK or Error.
Management Processor	Management processor is not responding. Possible values are OK or Error.
Temperature	Temperature is above the warning threshold. Possible values are OK or Temperature Warning.
Overheat Check	Temperature is above the danger threshold. Possible values are OK or Critical temperature threshold reached.
I/O Configuration	Interconnect bay configuration is incorrect. Possible values are OK or I/O mismatch.
Power Allocation Request	There is insufficient power to adequately power the interconnect. Possible values are OK or Insufficient enclosure power.

Table Continued

Row	Description
Device Operational	Device has failed; status was not requested by the Onboard Administrator. Possible values are OK or Error.
Device Degraded	Device has failed; status was requested by the Onboard Administrator. Possible values are OK or Error.
Device Informational	The device is operating normally but requires attention.
Duplicate IP Address	A check to verify if a duplicate IP address exists on the network during assignment. Possible values are OK or an informational message indicating there is a duplicate IP address on the network.

Interconnect Bay Information tab

Hardware Information

Row	Description
Product Name	The common descriptive name of the interconnect device.
Management IP Address	IP address of the interconnect management interface.
Management URL	Address where the interconnect device can be managed and configured for use in the network.
User Assigned Name	A name assigned to the interconnect by the user. If supported, the name is assigned using the interconnect Management Interface.
Part Number	The part number to be used when ordering an additional interconnect device of this type.
Spare Part Number	The part number to be used when ordering a replacement interconnect device of this type.
Serial Number	The unique serial number of the interconnect device.
Type	The interface type of the interconnect device. Possible values are Ethernet or fiber.
Manufacturer	The name of the company that manufactured the interconnect device.
Temperature Sensor	Indicates whether or not the interconnect device has a temperature sensor.
Firmware Version	The firmware version of the interconnect module.
VLAN ID (Name)	The VLAN ID number and name assigned to the interconnect bay.

IPv6 Information

Row	Description
Link Local Address	The link local IPv6 address of the interconnect interface.
EBIPA Address	The EBIPA IPv6 address of the interconnect interface.
DHCPv6 Address	The DHCP IPv6 address of the interconnect interface.
SLAAC Address	The SLAAC IPv6 address of the interconnect interface.
Link Local Management URL	The link local IPv6 management URL where the interconnect device can be managed and configured for use in the network.

Table Continued

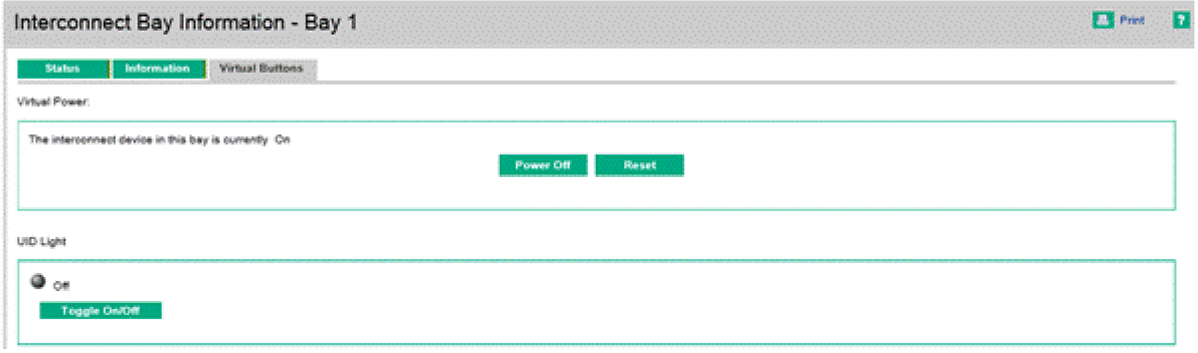
Row	Description
EBIPA Management URL	The EBIPA IPv6 management URL where the interconnect device can be managed and configured for use in the network.
DHCPv6 Management URL	The DHCP IPv6 management URL where the interconnect device can be managed and configured for use in the network.
SLAAC Management URL	The SLAAC IPv6 management URL where the interconnect device can be managed and configured for use in the network.

Connectivity Information

Row	Description
JS2 Connector	This field displays the presence or absence of the JS2 connector.
Internal Ethernet Interface to OA	This field displays the presence or absence of an internal Ethernet interface to the Onboard Administrator.
Internal Ethernet Route to OA	This field displays the status of an internal Ethernet route to the Onboard Administrator . Possible values are Enabled or Disabled.
Internal Serial Interface to OA	This field displays the presence or absence of an internal serial interface to the Onboard Administrator.
Internal Serial Route to OA	This field displays the status of an internal serial route to the Onboard Administrator. Possible values are Enabled or Disabled.
Serial Port Baud Rate	This field displays the serial port baud rate.
External Serial Port Interface	This field displays the presence or absence of an external serial port interface.
External Ethernet Interface	This field displays the presence or absence of an external Ethernet interface.

Interconnect Bay Virtual Buttons

Interconnect bay virtual buttons enable you to cycle power, reset, or toggle the UID on the device of your choice from the Onboard Administrator GUI.


Interconnect Bay Information - Bay 1

The interconnect device in this bay is currently On

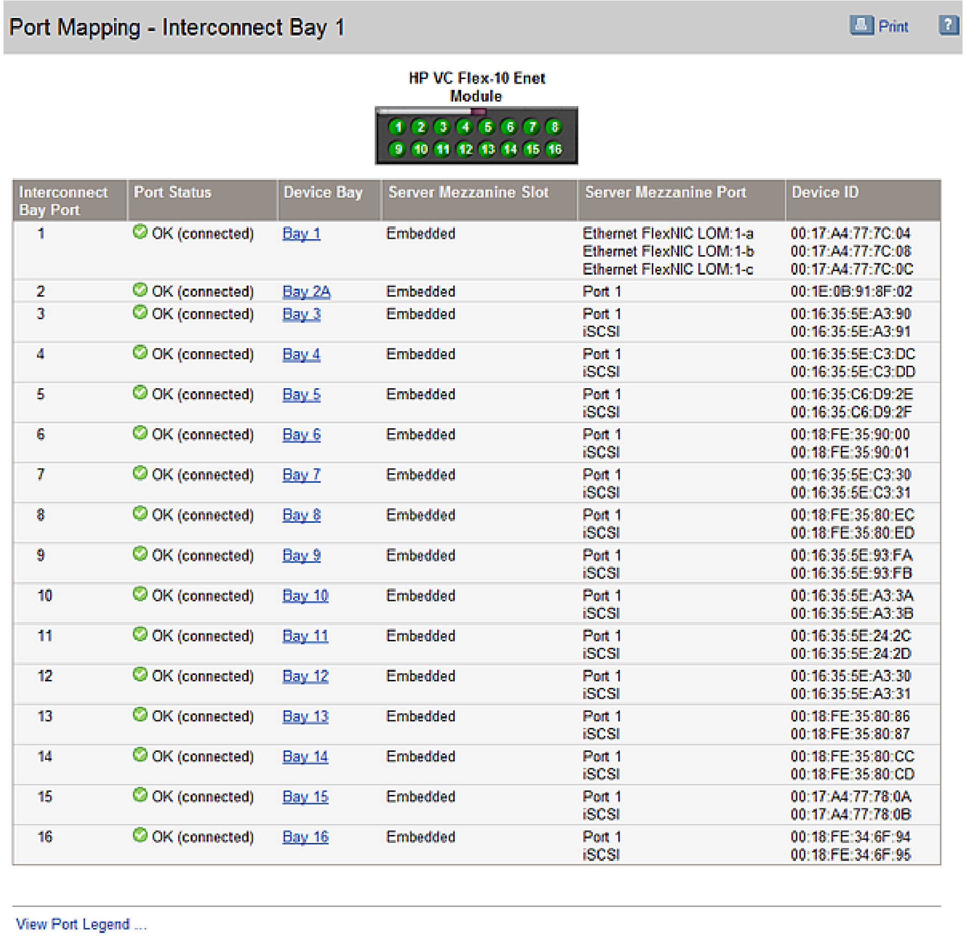
Button	Description
Power Off	Clicking this button shuts the power off on the interconnect device
Reset	Clicking this button forces the interconnect device to shut down and then power back up again, performing a reset
Toggle On/Off	Clicking this button turns the UID on the interconnect device on (blue) or off (gray) for easy identification of the selected interconnect device

NOTE:

If an interconnect module is powered off, the module will be powered on after an Onboard Administrator restart or the module will failover if sufficient enclosure power is available.

Interconnect Bay Port Mapping screen

The Interconnect Bay Port Mapping screen provides a graphical view and a table view of the interconnect bay port mapping.



Port Mapping - Interconnect Bay 1

Interconnect Bay Port	Port Status	Device Bay	Server Mezzanine Slot	Server Mezzanine Port	Device ID
1	✓ OK (connected)	Bay 1	Embedded	Ethernet FlexNIC LOM:1-a Ethernet FlexNIC LOM:1-b Ethernet FlexNIC LOM:1-c	00:17:A4:77:7C:04 00:17:A4:77:7C:08 00:17:A4:77:7C:0C
2	✓ OK (connected)	Bay 2A	Embedded	Port 1	00:1E:0B:91:8F:02
3	✓ OK (connected)	Bay 3	Embedded	Port 1 iSCSI	00:16:35:5E:A3:90 00:16:35:5E:A3:91
4	✓ OK (connected)	Bay 4	Embedded	Port 1 iSCSI	00:16:35:5E:C3:DC 00:16:35:5E:C3:DD
5	✓ OK (connected)	Bay 5	Embedded	Port 1 iSCSI	00:16:35:C6:D9:2E 00:16:35:C6:D9:2F
6	✓ OK (connected)	Bay 6	Embedded	Port 1 iSCSI	00:18:FE:35:90:00 00:18:FE:35:90:01
7	✓ OK (connected)	Bay 7	Embedded	Port 1 iSCSI	00:16:35:5E:C3:30 00:16:35:5E:C3:31
8	✓ OK (connected)	Bay 8	Embedded	Port 1 iSCSI	00:18:FE:35:80:EC 00:18:FE:35:80:ED
9	✓ OK (connected)	Bay 9	Embedded	Port 1 iSCSI	00:16:35:5E:93:FA 00:16:35:5E:93:FB
10	✓ OK (connected)	Bay 10	Embedded	Port 1 iSCSI	00:16:35:5E:A3:3A 00:16:35:5E:A3:3B
11	✓ OK (connected)	Bay 11	Embedded	Port 1 iSCSI	00:16:35:5E:24:2C 00:16:35:5E:24:2D
12	✓ OK (connected)	Bay 12	Embedded	Port 1 iSCSI	00:16:35:5E:A3:30 00:16:35:5E:A3:31
13	✓ OK (connected)	Bay 13	Embedded	Port 1 iSCSI	00:18:FE:35:80:86 00:18:FE:35:80:87
14	✓ OK (connected)	Bay 14	Embedded	Port 1 iSCSI	00:18:FE:35:80:CC 00:18:FE:35:80:CD
15	✓ OK (connected)	Bay 15	Embedded	Port 1 iSCSI	00:17:A4:77:78:0A 00:17:A4:77:78:0B
16	✓ OK (connected)	Bay 16	Embedded	Port 1 iSCSI	00:18:FE:34:6F:94 00:18:FE:34:6F:95

View Port Legend ...

Graphical view

When you mouse over the port on the interconnect, the graphical view provides the same information that appears in the table view.

Table view

Column	Description
Interconnect Bay Port	The number of the interconnect bay port in order from 1 to 16
Port Status	Current status of the port
Device Bay	The device bay corresponding with the interconnect port mapping
Server Mezzanine Slot	The type of device placed into the mezzanine of the server blade

Table Continued

Column	Description
Server Mezzanine Port	The physical port of the mezzanine device
Device ID	The MAC address of the interconnect bay port

Enclosure power management

Power management planning

The power enclosures each contain six power supplies, which are monitored directly by Onboard Administrator. Up to two power supply enclosures can be connected to a single enclosure.

Onboard Administrator is responsible for calculating the redundancy status, total available power, and total power consumed. This information is displayed to the user and is used to manage power resources. The Onboard Administrator power subsystem displays include status and information for each power supply, as well as the power enclosure itself.

Also included in the power fault realm is control of the electronic fuses between the power backplane and the server or switch bays. The Onboard Administrator will alert on fuse trips to enable you to reset fuses manually.

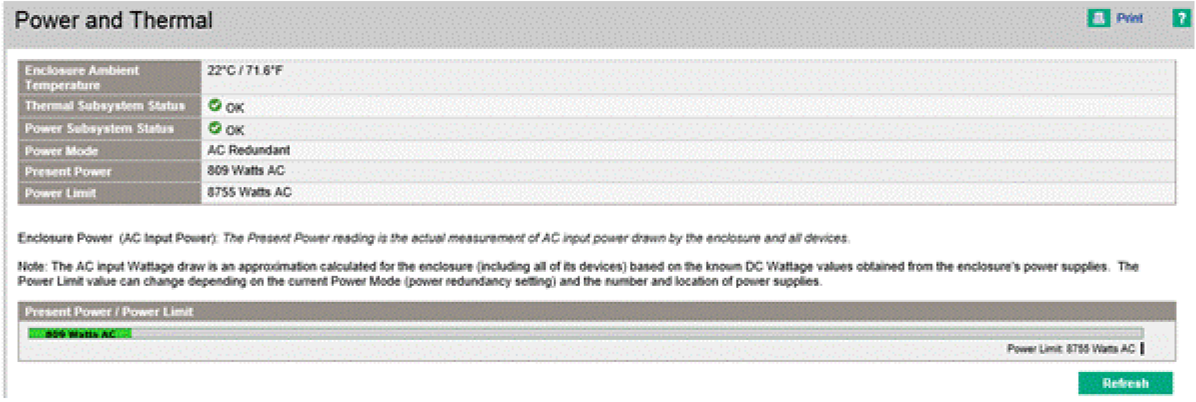
When installing additional power supplies into the enclosure, different power supply part numbers are not supported in the same enclosure. Onboard Administrator warns which power supplies must be replaced with a caution icon.

NOTE:

HPE 1200W Common Slot Silver Hot Plug Power Supplies, spare part numbers 441830-001 and 498152-001 can be combined in an enclosure and are treated as equivalent for the purposes of power supply mixing.

For proper installation of the power supplies into the enclosure, see the appropriate BladeSystem c7000 Enclosure Setup and Installation guide.

Power and thermal screen



Power and Thermal

Enclosure Ambient Temperature	22°C / 71.6°F
Thermal Subsystem Status	✓ OK
Power Subsystem Status	✓ OK
Power Mode	AC Redundant
Present Power	809 Watts AC
Power Limit	8755 Watts AC

Enclosure Power (AC Input Power): *The Present Power reading is the actual measurement of AC input power drawn by the enclosure and all devices.*

Note: The AC input Wattage draw is an approximation calculated for the enclosure (including all of its devices) based on the known DC Wattage values obtained from the enclosure's power supplies. The Power Limit value can change depending on the current Power Mode (power redundancy setting) and the number and location of power supplies.

Present Power / Power Limit

809 Watts AC

Power Limit: 8755 Watts AC

Row	Description
Enclosure Ambient Temperature	This field displays the highest ambient temperature being reported by the installed blade devices. If no blade devices are installed, then this field displays the temperature of the Onboard Administrator module as an approximation of the ambient temperature.
Thermal Subsystem Status	The overall thermal status of the enclosure. Possible values are Unknown, OK, Degraded, or Critical Error.
Power Subsystem Status	The overall power status of the enclosure. Possible values are Unknown, OK, Degraded, or Critical Error.
Power Mode	A user setting to configure the enclosure DC power capacity and the input power redundancy mode of the enclosure. See Power Management for possible values.
Present Power	The amount of watts being consumed by all devices in the enclosure.
Power Limit	The maximum amount of power available for consumption by the enclosure measured in watts.
Enclosure Dynamic Power Cap	A power cap on a group of servers in the enclosure. As the servers run, the demand for power varies for each server. A power cap for each server is set to provide the server with enough power to meet its workload demands while still conforming to the Enclosure Dynamic Power Cap. Continuous monitoring of power demands and automatic adjustments to server power caps ensure there is minimal performance degradation. Information for the Enclosure Dynamic Power Cap appears only if a cap has been defined.

Present Power/Enclosure Dynamic Power Cap/Power Limit

The Present Power is the number of watts being consumed by all the devices in the enclosure. The Enclosure Dynamic Power Cap automatically adjusts power caps on servers in the enclosure to meet workload demands on the servers while still conforming to the Enclosure Dynamic Power Cap. The Power Limit is the maximum amount of input power available for consumption by the enclosure. The Power Limit is dependent on the enclosure power redundancy setting and the number and location of the power supplies in the enclosure. If a Static Power Limit has been specified, the Power Limit displays that limit.

Power management

To set the power management options in Onboard Administrator, go to the menu on the left and select the enclosure to be managed. Click **Power and Thermal** > **Power Management**. The main Power Management page appears and displays the following choices:

- AC Redundant
- Power Supply Redundant
- Not DC Redundant

Beneath the main power management choices is the Enable Dynamic Power check box which allows you to enable or disable Dynamic Power mode.

The AC Input VA Limit field enables you to set a VA limit for the enclosure. After this limit is met by the enclosure, it will not allow any further blades, power supplies, fans, or switches to power on. If a value is entered into the VA Limit field that is lower than the currently used VA for the enclosure, the enclosure will not power off any devices within the enclosure. However, if a device is powered off, it cannot power on because of the VA limit rule set in the Onboard Administrator power management settings.

IMPORTANT:

If redundancy mode is set to DC Redundant, AC Redundant, or Power Supply Redundant, and power redundancy is lost, then you must either add additional power supplies or change the redundancy mode setting in the Onboard Administrator to restore Power Subsystem status. See the Insight Display for corrective steps.

To change the power redundancy mode, you must disable EDPC. After changing the power redundancy mode, reset EDPC based on the new ranges.

Power management options

The HPE BladeSystem c3000 and c7000 Enclosure power management systems enable you to configure the enclosure to meet your needs. You can choose from the different power management options on the Onboard Administrator Power Management screen. These power management options are explained in the following table.

Power management option	Insight Displayname	Description
Power mode (power redundancy mode)		
DC Redundant or AC Redundant	DC Redundant or AC Redundant	The OA detects the type of power supplies present, automatically adapts the power mode behavior accordingly, and displays the corresponding mode name: • If DC power supplies are present: DC Redundant mode • If AC power supplies are present: AC Redundant mode Also known as N+N redundancy or grid redundancy. N power supplies are used to provide power and N are used to provide redundancy (where N can equal 1, 2, or 3). Up to three power supplies can fail without causing the enclosure to fail. When correctly wired with redundant AC or DC line feeds, this configuration also ensures that an AC or DC line feed failure does not cause the enclosure to power off. In the unlikely event that the entire power bank is unable to provide power because of multiple power supply failures or a power grid failure, the system might power down. The system powers down when the surviving power supplies do not have enough power to meet the system's power requirements. AC Redundant or DC Redundant mode requires a minimum of two power supplies. In either mode, Hewlett Packard Enterprise recommends operating with an even number of power supplies (2, 4, or 6). In this case, N power supplies are used to provide power, and N are used to provide redundancy (where N equals 1, 2, or 3). When using an odd number of power supplies (3 or 5), N are used for providing power, and N+1 are used for redundancy (where N equals 1 or 2). AC Redundant or DC Redundant mode also protects a system from a power grid failure when using redundant AC or DC power feeds (if wired correctly). In AC Redundant mode, if using a c7000 Enclosure 3-phase power input module, Hewlett Packard Enterprise recommends six active power supplies (3+3) for proper phase balancing.

Table Continued

Power management option	**Insight Displayname**	**Description**
Power Supply Redundant	Power Supply	For all power supplies. This mode supports two to six power supplies. Also known as N+1 redundancy. With this power mode, N power supplies are used to provide power and 1 is used to provide redundancy (where N can equal 1, 2, 3, 4, or 5). If using a c7000 Enclosure 3-phase power input module, Hewlett Packard Enterprise recommends 3 or 6 active power supplies (2+1 or 5+1) for proper phase balancing. This power mode is designed to protect the system from one power supply failing. In the unlikely event that more than one power supply is unable to provide power because of multiple power supply failures or a power grid failure, the system might power down. The system powers down when the surviving power supplies do not have enough power to meet the system's power requirements.
Not Redundant	None	For all power supplies. This mode supports 1 to 6 power supplies. With this power mode, N power supplies are used to provide power and none are used to provide redundancy (where N can equal 1, 2, 3, 4, 5, or 6). If using a c7000 Enclosure 3-phase power input module, Hewlett Packard Enterprise recommends 3 or 6 active power supplies for proper phase balancing. There is no power redundancy, and no power redundancy warnings are given. If a power supply is unable to provide power because of a power supply failure or a grid failure, the system might power down. It will power down if the surviving power supplies do not have enough power to meet the system's power requirements. This power mode is not recommended for deployed systems in production environments.
Dynamic Power mode (enabled or disabled)		
Dynamic Power	Dynamic Power	If enabled, Dynamic Power automatically places unused power supplies in standby mode to increase enclosure power supply efficiency, thereby minimizing enclosure power consumption during lower power demand. Increased power demands automatically return standby power supplies to full performance. More information about Dynamic Power follows this table.
Power Limit mode		

Table Continued

Power management option	Insight Displayname	Description
Enclosure Dynamic Power Cap	None	Allows specifying a limit for the enclosure power consumption. The power draw is limited by dynamically managing server blade power caps to stay under the overall enclosure power cap. For more information, see the Power Limit table that follows.
Static Power Limit	Power Limit	An optional setting to limit power. Whenever you attempt to power on a device, the total power demands of the new device and of the devices already on are compared against this Static Power Limit. If the total power demands exceed the limit, the new device is prevented from powering on. For more information about the Static Power Limit and how it compares to the Enclosure Dynamic Power Cap, see the Power Limit table that follows.

NOTE:

Independent of the redundancy mode enabled, all operational power supplies present in the enclosure are typically active and share in delivering the enclosure power needs. If Dynamic Power mode is enabled, some power supplies might automatically be placed on standby to increase overall enclosure power efficiency. For more information, see the discussion of Dynamic Power mode that follows.

The Onboard Administrator allows you to change the power (redundancy) mode setting after the enclosure and devices are powered up. If the power mode is changed, the Onboard Administrator updates the redundancy status as needed, reporting degraded/failed redundancy if applicable. For example, the original power mode was Power Supply Redundant (N+1) when all blades powered on and then was changed to AC Redundant (N+N) reducing the Power Capacity as seen by the Onboard Administrator. As long as enough power is available, all blades will remain operational. However, under some circumstances a blade will not be powered on, such as when it is replacing another server blade. Additional information is provided in the table and sections that follow.

Dynamic Power—The default setting is Disabled. The following selections are valid:

- Enabled—Some power supplies can be automatically placed on standby to increase overall enclosure power subsystem efficiency.
- Disabled—All power supplies share the load. The power subsystem efficiency varies based on load.

NOTE:

Dynamic Power is supported with all c3000 power supplies. It is supported with all c7000 power supplies except those operating with low-line input voltage (nominal 100-120V AC).

For OA v4.01 and later, the factory default value associated with the Dynamic Power setting was changed from enabled to disabled. The operating efficiency of the currently available HPE Gold (92% efficient) and HPE Platinum (94% efficient) enclosure power supplies makes this firmware-based power management strategy unnecessary. The Dynamic Power setting is recommended only for enclosure power supplies with an efficiency value less than 92%. When upgrading to OA v4.01 or later, the current Dynamic Power setting is retained after the upgrade. For more information, see the **Customer Advisory c03957955**.

Power Limit

Do not set a Static Power Limit or Enclosure Dynamic Power Cap on an empty enclosure.

Mode	Insight Display name	Description
Enclosure Dynamic Power Cap	None	An optional feature that enables you to cap the servers in an enclosure as a group. As the servers run, the demand for power varies for each server. A power cap for each server is automatically adjusted to provide the server with enough power to meet workload demands while still conforming to the Enclosure Dynamic Power Cap. A redundant OA board is required for setting the Dynamic Power Cap feature. The feature is enabled with three configuration parameters: • Dynamic Power Cap—Total enclosure average power will not exceed Dynamic Power Cap. • Derated Circuit Capacity—Average power on a single circuit will not exceed Derated Circuit Capacity. • Rated Circuit Capacity—Peak power on a single circuit will not exceed Rated Circuit Capacity. When configuring these parameters, the Derated Circuit Capacity must be at least as large as the Dynamic Power Cap and no larger than the Rated Circuit Capacity. The Dynamic Power Cap is used to limit the enclosure power consumption based on a cooling constraint that might be lower than the Derated Circuit Capacity. The Derated Circuit Capacity is used to limit the enclosure average power consumption on a circuit. The Rated Circuit Capacity is used to limit the enclosure peak power consumption on a circuit. If you need to restrict an enclosure electrical load and thermal output, an Enclosure Dynamic Power Cap is better than a Static Power Limit. Enclosure Dynamic Power Cap enables more blades to power on than a Static Power Limit.
Static Power Limit	Power Limit	An optional setting to limit power. Whenever you attempt to power on a device, the total power demands of the new device and of the devices already on are compared against this Static Power Limit. If the total power demands exceed the limit, the new device is prevented from powering on. A Static Power Limit is better when:

Table Continued

Mode	Insight Display name	Description
		• You do not want caps dynamically adjusted on your blades. • You prefer to not power on a server blade if it cannot be allocated full power (even if it typically consumes less). • More than 1/4 of the blades in the enclosure do not meet hardware or firmware requirements for the Enclosure Dynamic Power Cap.
None	None	The enclosure power usage is not managed or capped.

Understanding power capping varieties

Hewlett Packard Enterprise delivers three varieties of power management that enable users to limit the server power consumption. All three power capping varieties work to limit your consumption to a specified Watt or Btu/hr goal. The three technologies are Power Capping, Dynamic Power Capping, and Enclosure Dynamic Power Capping.

Power Capping

In May 2007, Hewlett Packard Enterprise launched Power Capping technology with iLO 2 version 1.30. This firmware-based technology limits the average power consumption of the server to a user-defined Watt or Btu/hr goal. Because this technology runs in firmware, it cannot limit power consumption rapidly enough to ensure protection of PDU-level circuit breakers. Power Capping does limit power consumption rapidly enough to protect cooling infrastructure, so it is an effective solution for data centers experiencing cooling capacity constraints. Power Capping is supported on any ProLiant server or blade that has an iLO management processor and power measurement capabilities. Using Power Capping requires iLO 2 version 1.30 (or later) firmware and an updated system ROM/BIOS.

Dynamic Power Capping

Dynamic Power Capping is a hardware-based technology that limits power consumption fast enough to protect circuit breakers and cooling infrastructure. Hewlett Packard Enterprise launched Dynamic Power Capping in December of 2008 with iLO 2 version 1.70. Supported servers contain an internal hardware circuit that monitors server power consumption on a sub-second basis. If server power consumption approaches the power cap limit set in iLO, the internal hardware circuit limits power consumption rapidly enough to protect PDU-level circuits from over-subscription and prevent power-related server outages.

Dynamic Power Capping requires specific hardware on the system board. Dynamic Power Capping also requires iLO 2 version 1.70 (or later) firmware and a system ROM/BIOS dated 10/1/2008 (or later). iLO automatically updates firmware in the Dynamic Power Capping hardware power circuit.

Dynamic Power Capping is supported on the following BladeSystem server blades:

- BL260c G5 (Notes: 2)
- BL2x220 G5 (Notes: 2)
- BL460c G1 (Notes: 1 and 2)
- BL460c G5 (Notes: 2)
- BL465c G5 (Notes: 2)
- BL495c G5 (Notes: 2)
- BL685c G5 (Notes: 2)
- All G6 server blades
- All G7 server blades
- All G8 server blades

Additional information

- These systems require Quad-Core capable system boards to support Dynamic Power Capping.
- When implementing power capping for BladeSystem, Hewlett Packard Enterprise recommends using Enclosure Dynamic Power Capping set through the Onboard Administrator. To use Enclosure Dynamic Power Capping, you must upgrade iLO 2 firmware to version 1.70 or later and are encouraged to update system ROM to version 10/1/2008 or later. For some older BL460c Servers, the iLO firmware might not be able to automatically update the Dynamic Power Capping hardware circuit. In these instances, Onboard Administrator compensates for the absence of the internal hardware circuit and continues to guarantee circuit protection.

Enclosure Dynamic Power Capping

Enclosure Dynamic Power Capping combines the power capping technology of the BladeSystem server with a power balancing control algorithm in the Onboard Administrator to maximize the aggregate performance of the enclosure. Enclosure Dynamic Power Capping protects your circuit breakers and maximizes your performance.

Using Enclosure Dynamic Power Capping, you set a power cap for the entire enclosure. The Onboard Administrator allocates individual limits to each participating server blade. The server blades manage consumption to that limit. The Onboard Administrator continuously monitors power consumption requirements for each server blade and continuously rebalances the individual limits to ensure that busy server blades receive more power than idle server blades. This power allocation improves aggregate enclosure performance.

BladeSystem server power caps are set in the Onboard Administrator. Enclosure Dynamic Power Capping protects both cooling and electrical infrastructures. Enclosure Dynamic Power Capping works with either firmware-based power capping technology on the server or with the fast, hardware-based technology. The Enclosure Dynamic Power Capping solution performs better if the server blades that support the fast, hardware-based capping technology are upgraded.

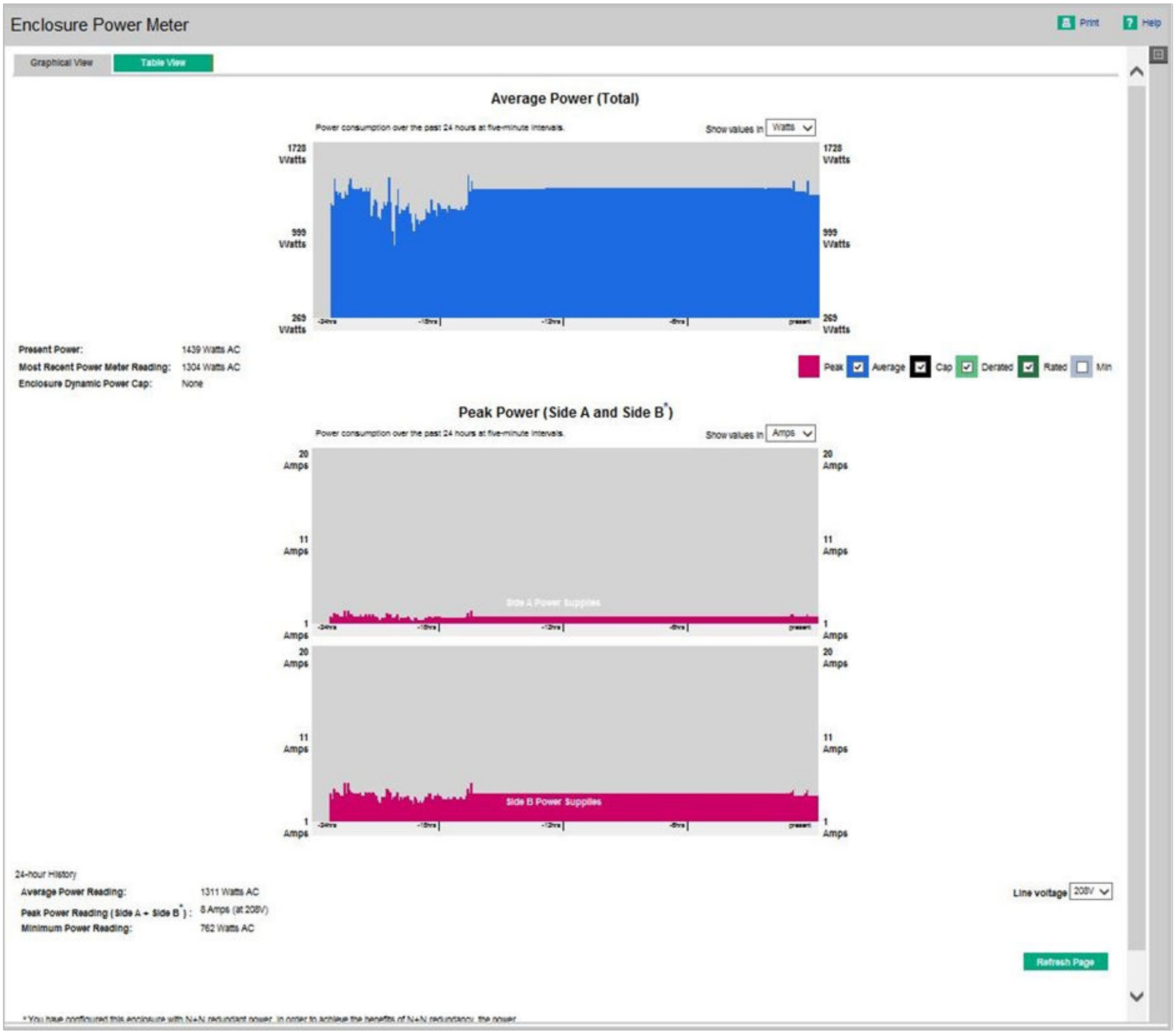
Enclosure Dynamic Power Capping requires Onboard Administrator 2.30 (or later), iLO 2 version 1.70 (or later), and System ROM/BIOS dated 10/1/2008 (or later).

NOTE:

Power caps set for less than 50% of the difference between maximum power and idle power might become unreachable due to changes in the server. Power caps set for less than 20% are not recommended, and might cause the server to reboot or the server operating system to stop responding.

Enclosure Power Meter screen

The Enclosure Power Meter screen displays peak power use, average power use, and allocated power available in a graph, which enables fast and easy interpretation of the power situation for the enclosure. The power meter is useful for showing trends in power consumption and can assist in troubleshooting the power subsystem.



Present Power: 1439 Watts AC

Most Recent Power Meter Reading: 1304 Watts AC

Enclosure Dynamic Power Cap: None

24-hour History

Average Power Reading: 1311 Watts AC

Peak Power Reading (Side A + Side B*): 8 Amps (at 208V)

Minimum Power Reading: 762 Watts AC

* You have configured this enclosure with N+N redundant power. In order to achieve the benefits of N+N redundancy, the power

Graphical View tab

This screen enables you to see a graphical view of the power readings for the enclosure.

To toggle between Watts, Btu/hr, and Amps, click **Show Values.**

The **Line Voltage** value is used to provide conversion to Amps. The default value is based on the power supply hardware model, not the actual line voltage. Select the actual line voltage for the enclosure for a more accurate Amps conversion.

To view updated power meter information, click **Refresh Page.**

Average Power data graph

This graph displays the power usage of the enclosure over the previous 24 hours. The Onboard Administrator collects power usage and Enclosure Dynamic Power Cap information from the enclosure every 5 minutes. For each 5 minute time period, the peak and average power usage and the cap for that time period are stored in a circular buffer. These values appear in the form of a bar graph, with the average value in blue, the peak value in red, and the cap value in black. This data is reset when the enclosure is reset. You can choose what appears on the bar graph by selecting or clearing the **Average, Cap, Derated, Rated,** and **Min** check boxes.

Present Power

This value represents the number of watts being consumed by all devices in the enclosure.

Most Recent Power Meter Reading

This value represents the most recent power reading from the enclosure.

Peak Power data graph

This graph displays the peak power usage and the Enclosure Dynamic Power Cap over the previous 24 hours.

The label Peak Power becomes Peak Power (Side A + Side B) when N+N redundant power is in place, indicating that the peak is divided across two circuits. Also, two graphs appear: one for Side A and one for Side B.

The power distribution between Side A and Side B is estimated from the number of active power supplies on each side. If redundancy is lost, the lost side displays peak power of zero.

Enclosure Dynamic Power Cap

This value represents the most recent Enclosure Dynamic Power Cap reading from the enclosure.

Average Power Reading

This value represents the average of the power readings from the enclosure over the last 24-hour period. If the enclosure has not been running for 24 hours, then the value is the average of all the readings since the enclosure was powered up.

Peak Power Reading

This value represents the peak power readings from the enclosure over the last 24-hour period. If the enclosure has not been running for 24 hours, then the value is the maximum of all the readings since the enclosure was powered up or the Onboard Administrator was reset.

The label Peak Power Reading becomes Peak Power Reading (Side A + Side B) when N+N redundant power is in place, indicating that the peak is divided across two circuits.

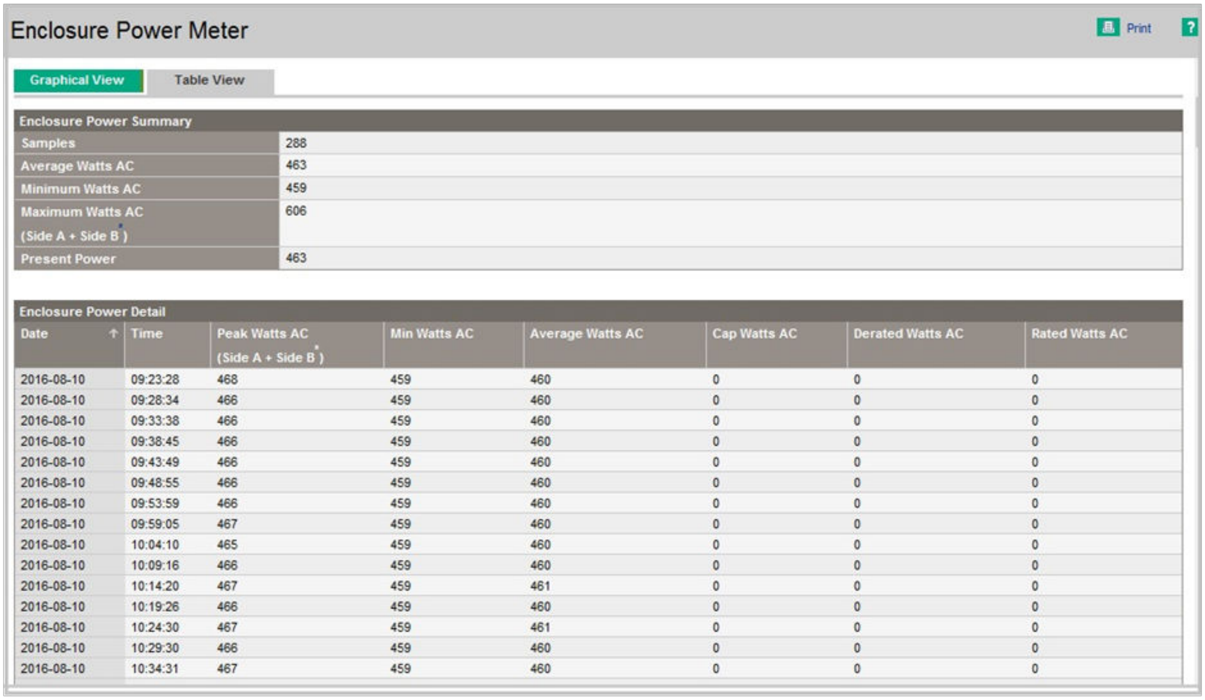
Minimum Power Reading

This value represents the minimum power readings from the enclosure over the last 24-hour period. If the enclosure has not been running for 24 hours, then the value is the minimum of all the readings since the enclosure was powered up.

Refresh Page

When you restart an enclosure, Hewlett Packard Enterprise recommends waiting five minutes and then click **Refresh Page,** because the Power Meter does not dynamically update.

Table View tab



Enclosure Power Meter

Enclosure Power Summary	
Samples	288
Average Watts AC	463
Minimum Watts AC	459
Maximum Watts AC (Side A + Side B*)	606
Present Power	463

Enclosure Power Detail

Date ↑	Time	Peak Watts AC (Side A + Side B*)	Min Watts AC	Average Watts AC	Cap Watts AC	Derated Watts AC	Rated Watts AC
2016-08-10	09:23:28	468	459	460	0	0	0
2016-08-10	09:28:34	466	459	460	0	0	0
2016-08-10	09:33:38	466	459	460	0	0	0
2016-08-10	09:38:45	466	459	460	0	0	0
2016-08-10	09:43:49	466	459	460	0	0	0
2016-08-10	09:48:55	466	459	460	0	0	0
2016-08-10	09:53:59	466	459	460	0	0	0
2016-08-10	09:59:05	467	459	460	0	0	0
2016-08-10	10:04:10	465	459	460	0	0	0
2016-08-10	10:09:16	466	459	460	0	0	0
2016-08-10	10:14:20	467	459	461	0	0	0
2016-08-10	10:19:26	466	459	460	0	0	0
2016-08-10	10:24:30	467	459	461	0	0	0
2016-08-10	10:29:30	466	459	460	0	0	0
2016-08-10	10:34:31	467	459	460	0	0	0

Select the appropriate line voltage from the menu.

Row	Description
Samples	Number of samples taken.
Average (Watts, Btu/hr, or Amps)	This value shows the average of the power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the average of all the readings since the enclosure was powered up.
Minimum (Watts, Btu/hr, or Amps)	This value shows the minimum power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the minimum of all the readings since the enclosure was powered up.
Maximum (Watts, Btu/hr, or Amps) (Side A + Side B)	This value shows the maximum power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the maximum of all the readings since the enclosure was powered up.
Present Power	This value shows the power being consumed by all devices in the enclosure.

This screen enables you to view the power readings for the enclosure in a table format.

Enclosure Power Summary

Row	Description
Samples	Number of samples taken.
Average (Watts, Btu/hr, or Amps)	This value shows the average of the power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the average of all the readings since the enclosure was powered up.
Minimum (Watts, Btu/hr, or Amps)	This value shows the minimum power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the minimum of all the readings since the enclosure was powered up.
Maximum (Watts, Btu/hr, or Amps) (Side A + Side B)	This value shows the maximum power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the maximum of all the readings since the enclosure was powered up.
Present Power	This value shows the power being consumed by all devices in the enclosure.

Enclosure Power Detail

The Enclosure Power Detail table provides detailed information for each five minute sample period. Click **Date** in the table heading to arrange the order of the detailed enclosure power information from present date to oldest date or oldest date to present date.

Column	Description
Date	Date the power reading sample was taken.
Time	Time the power reading sample was taken.
Peak (Watts, Btu/hr, or Amps) (Side A + Side B)	This value shows the maximum power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the maximum of all the readings since the enclosure was powered up.
Min (Watts, Btu/hr, or Amps)	This value shows the minimum power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the minimum of all the readings since the enclosure was powered up.
Average (Watts, Btu/hr, or Amps)	This value shows the average of the power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the average of all the readings since the enclosure was powered up.
Cap (Watts, Btu/hr, or Amps)	This value shows the maximum dynamic power cap readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the maximum of all the readings since the enclosure was powered up.

Table Continued

Column	Description
Derated (Watts, Btu/hr, or Amps)	This value shows the derated power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the maximum of all the readings since the enclosure was powered up.
Rated (Watts, Btu/hr, or Amps)	This value shows the rated power readings (Watts, Btu/hr, or Amps depending on what you have selected) from the enclosure over the last 24 hour period. If the enclosure has not been running for 24 hours, the value is the maximum of all the readings since the enclosure was powered up.

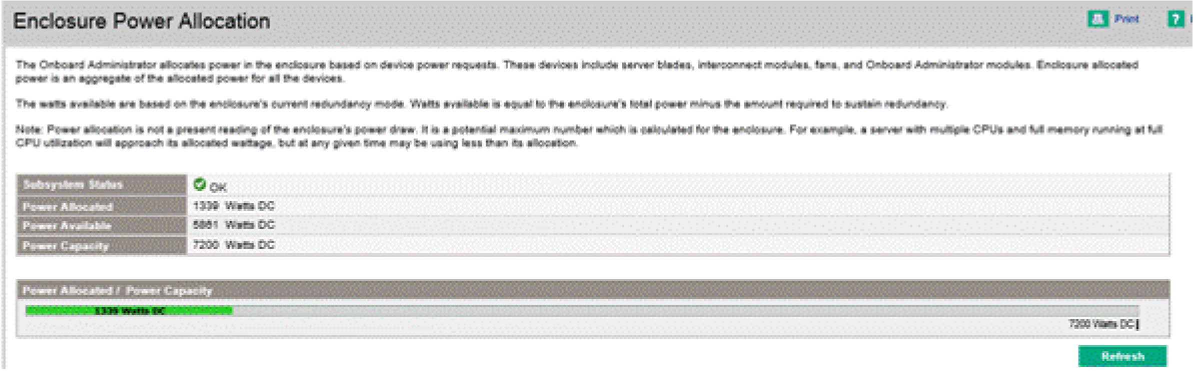
Power units

Select the appropriate value in which to display the power date from the menu.

Line voltage

Select the appropriate line voltage from the menu.

Enclosure power allocation



Enclosure Power Allocation

The Onboard Administrator allocates power in the enclosure based on device power requests. These devices include server blades, interconnect modules, fans, and Onboard Administrator modules. Enclosure allocated power is an aggregate of the allocated power for all the devices.

The watts available are based on the enclosure's current redundancy mode. Watts available is equal to the enclosure's total power minus the amount required to sustain redundancy.

Note: Power allocation is not a present reading of the enclosure's power draw. It is a potential maximum number which is calculated for the enclosure. For example, a server with multiple CPUs and full memory running at full CPU utilization will approach its allocated wattage, but at any given time may be using less than its allocation.

Subsystem Status	✓ OK
Power Allocated	1339 Watts DC
Power Available	5861 Watts DC
Power Capacity	7200 Watts DC

The Power Allocation screen displays basic information regarding the power subsystem's total capacity, redundant capacity, and the allocated power in watts. The Enclosure Internal Power graph displays the watts that are allocated in green against a gray background, which represents the total redundant capacity of the power supplies.

If you change the enclosure redundancy mode after power is allocated to the devices, then the power subsystem might become degraded. Power is still allocated to the devices, but redundancy might not function properly. If zero watts are available and the power graph displays degraded, check your power subsystem and redundancy configurations. You can resolve the degraded condition by changing your redundancy mode or by adding more power supplies to the enclosure.

Power Capacity will equal Power Allocated in the case where redundancy is lost.

Enclosure power summary

Enclosure Input Power Summary

Present Power is the input watts to the enclosure and is measured in Watts AC for power supplies with AC inputs and is measured in Watts DC for power supplies with DC inputs. Max Input Power is the highest expected input watts. If the Power Limit is set, then the Max Input Power is equal to the Power Limit. If the Enclosure Dynamic Power Cap is set and EDPC is enabled, then the Max Input Power is equal to the Enclosure Dynamic Power Cap. If neither Enclosure Dynamic Power Cap nor Power Limit is set, then the Max Input Power of the enclosure is the expected input power for the enclosure to operate at maximum DC output capacity.

Enclosure Output Power Summary

When EDPC is disabled, Power Capacity is based on the number of installed and operational power supplies, their DC output capacities, and the redundant Power Mode setting. Power Allocated is the total enclosure power output allocated for Device Bays, Interconnect Bays, and Fans. Power Available is Power Capacity minus Power Allocated.

When EDPC is enabled, Power Capacity is the Enclosure Dynamic Power Cap in Watts DC. Power Allocated is the minimum power the enclosure can be capped to in Watts DC. Power Available is Power Capacity minus Power Allocated. The total power allocated for Device Bays, Interconnect Bays, and Fans might not be equal to the Power Allocated for the enclosure because the power cap on each server is controlled dynamically.

Enclosure Bay Output Power Allocation

Power Allocated in the enclosure is the total of the power allocations for all Device Bays, Interconnect Bays, and Fans.

Device Bay Power Summary

Each populated device bay is listed with the power allocated. If EDPC is enabled, additional columns indicate compatible ProLiant server Power Cap, % Power Cap, and Present Power. The % Power Cap is computed based on current Power Cap Watts divided by the Power Allocated Watts. If EDPC is enabled, a server blade requesting power is only permitted to turn on if the Power Available supports the request or the Onboard Administrator can change the power cap for other servers to support the request.

Interconnect Bay Power Summary

Each populated interconnect bay is listed with the power allocated.

Fan Power Summary

Fan power is allocated based on a fan-rule. Fan-rule is determined according to the enclosure type (c3000 or c7000) and occupied device bays. Both the power allocation for the fans and the total Present Power consumption of all the fans are listed.

To update power summary information, click **Refresh.**

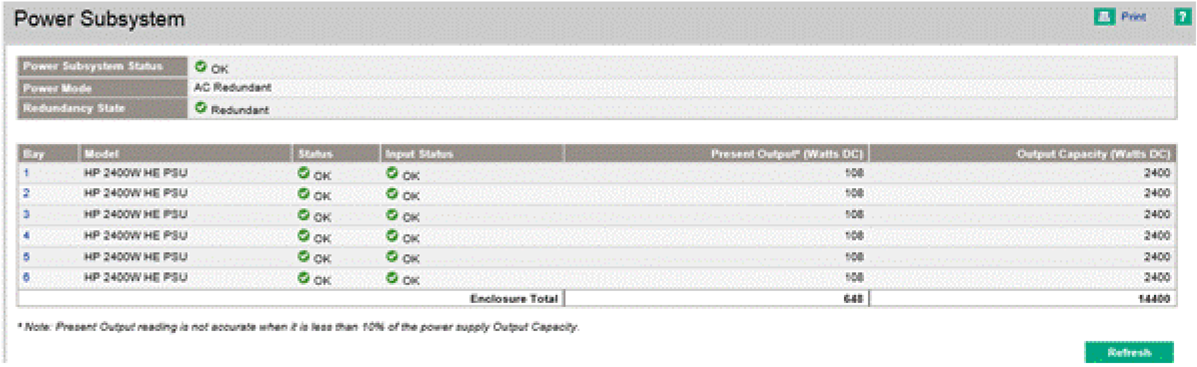
Power Subsystem screen

Power supplies available for use in BladeSystem enclosures

All power supplies in one enclosure must have the same part number. Onboard Administrator warns which power supplies must be replaced with a caution icon.

Power Supply summary

The Power Subsystem screen provides status on the power subsystem, on each individual power supply, and fault conditions.



Power Subsystem Status	✓ OK
Power Mode	AC Redundant
Redundancy State	✓ Redundant

Bay	Model	Status	Input Status	Present Output* (Watts DC)	Output Capacity (Watts DC)
1	HP 2400W HE PSU	✓ OK	✓ OK	108	2400
2	HP 2400W HE PSU	✓ OK	✓ OK	108	2400
3	HP 2400W HE PSU	✓ OK	✓ OK	108	2400
4	HP 2400W HE PSU	✓ OK	✓ OK	108	2400
5	HP 2400W HE PSU	✓ OK	✓ OK	108	2400
6	HP 2400W HE PSU	✓ OK	✓ OK	108	2400
			Enclosure Total	648	14400

* *Note: Present Output reading is not accurate when it is less than 10% of the power supply Output Capacity.*

Power subsystem

Row	Description
Power Subsystem Status	The status of the power subsystem. Possible values are Unknown, OK, Degraded, or Critical Error.
Power Mode	A user setting to configure the enclosure DC power capacity and the input power redundancy mode of the enclosure. Possible values are Redundant, AC Redundant, Power Supply Redundant, Not Redundant, or Unknown.
Redundancy State	Indicates the redundancy status of the power subsystem. Possible values are Redundant, Not Redundant, or Redundancy Lost.

Power supply status

Column	Description
Bay	The bay in the enclosure of the corresponding power supply. This field displays only populated bays. Empty bays do not appear in this table.
Model	The power supply model name.
Status	The overall status of the power supply. Possible values are Unknown, OK, Degraded, and Critical Error.
Input Status	The input status of the power supply. Possible values are Unknown, OK, Degraded, and Critical Error.
Present Output (Watts)	This value is a measure of the present output of the power supply in watts.
Output Capacity (Watts)	The amount of power provided by the power supply displayed in watts. This is a measure of the output in DC watts generated by the power supply.

Click **Refresh** to update the power subsystem information.

Power Supply Information

Selecting a specific power supply opens the Power Supply Information—Bay x page, where x is the bay of the selected power supply. This screen provides status information on the selected power supply.

Status information

Row	Description
Status	The overall status of the power supply. Possible values are Unknown, OK, Degraded, and Critical Error.
Input Status	The input status of the power supply. Possible values are Unknown, OK, Degraded, and Critical Error.
Present Output	The amount of power provided by the power supply in AC or DC mode. This value is displayed in watts
Output Capacity	The maximum amount of power that can be provided by the power supply in AC or DC mode. This value is displayed in watts.
Model	The power supply model name.
Serial Number	The unique serial number of the power supply.

Table Continued

Row	Description
Part Number	The part number to be used when ordering an additional or replacement power supply of this type.
Spare Part Number	The spare part number to be used when ordering an additional or replacement power supply.

Diagnostic Information

Diagnostic information is gathered by polling a device microcontroller (resulting in a degraded status if a failure has occurred) or is sent by the device microcontroller, without being polled to report a failure.

Row	Description
Device Identification Data	The device identification data checked is information such as model name, part number, serial number, and other information used to identify the device. This data is also referred to as FRU data. A device identification data error appears if the data is not present or not readable by the Onboard Administrator. Possible values are OK or Error.
Device Location	Incorrect power supply location. Possible values are OK or Incorrect location for proper device cooling.
Device Operational	Device has failed; status was not requested by the Onboard Administrator. Possible values are OK and Error.
Device Degraded	Device has failed; status was requested by the Onboard Administrator. Possible values are OK and Error.
Power Cord	Input power status. Possible values are OK and Error.
Device Mismatch	This field indicates different power supply models are installed in the same enclosure and you need to install the same power supply models in each bay.
Service Action	Recommended service action required to correct a power supply error.

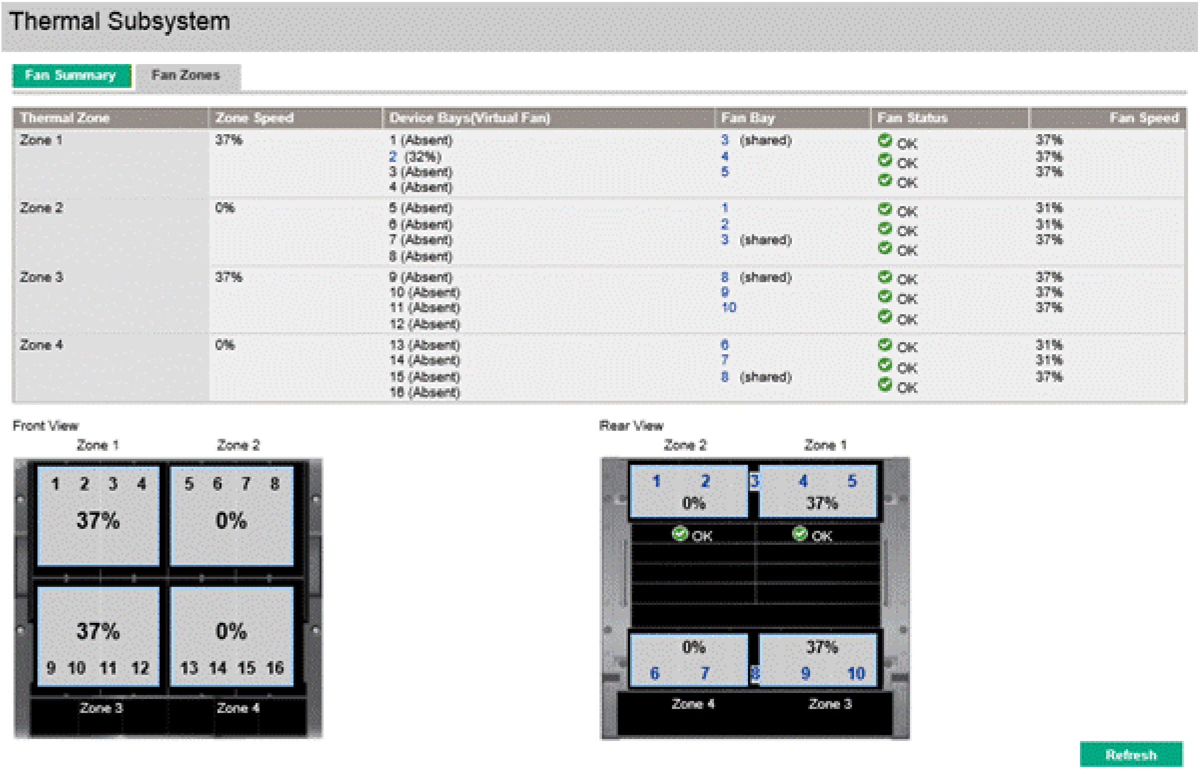
Click **Refresh** to update the power supply information.

Fans and cooling management

Fan zones

Fan zones monitor the bay cooling efficiency and the status of the bays the fans are configured to cool. Zone speeds reported are targeted speeds. These values change with time as the fans speed and slow in response to cooling needs of the zone. The Fan Zones screen does not dynamically update. To update information on this screen, click **Refresh**.

Fan speeds appear in percentage of total capacity, and fans operating in a zone without any blades run at a minimum RPM of 30% to maintain proper cooling for the entire enclosure.



Thermal Subsystem

Thermal Zone	Zone Speed	Device Bays(Virtual Fan)	Fan Bay	Fan Status	Fan Speed
Zone 1	37%	1 (Absent) 2 (32%) 3 (Absent) 4 (Absent)	3 (shared) 4 5	✓ OK ✓ OK ✓ OK	37% 37% 37%
Zone 2	0%	5 (Absent) 6 (Absent) 7 (Absent) 8 (Absent)	1 2 3 (shared)	✓ OK ✓ OK ✓ OK	31% 31% 37%
Zone 3	37%	9 (Absent) 10 (Absent) 11 (Absent) 12 (Absent)	8 (shared) 9 10	✓ OK ✓ OK ✓ OK	37% 37% 37%
Zone 4	0%	13 (Absent) 14 (Absent) 15 (Absent) 16 (Absent)	6 7 8 (shared)	✓ OK ✓ OK ✓ OK	31% 31% 37%

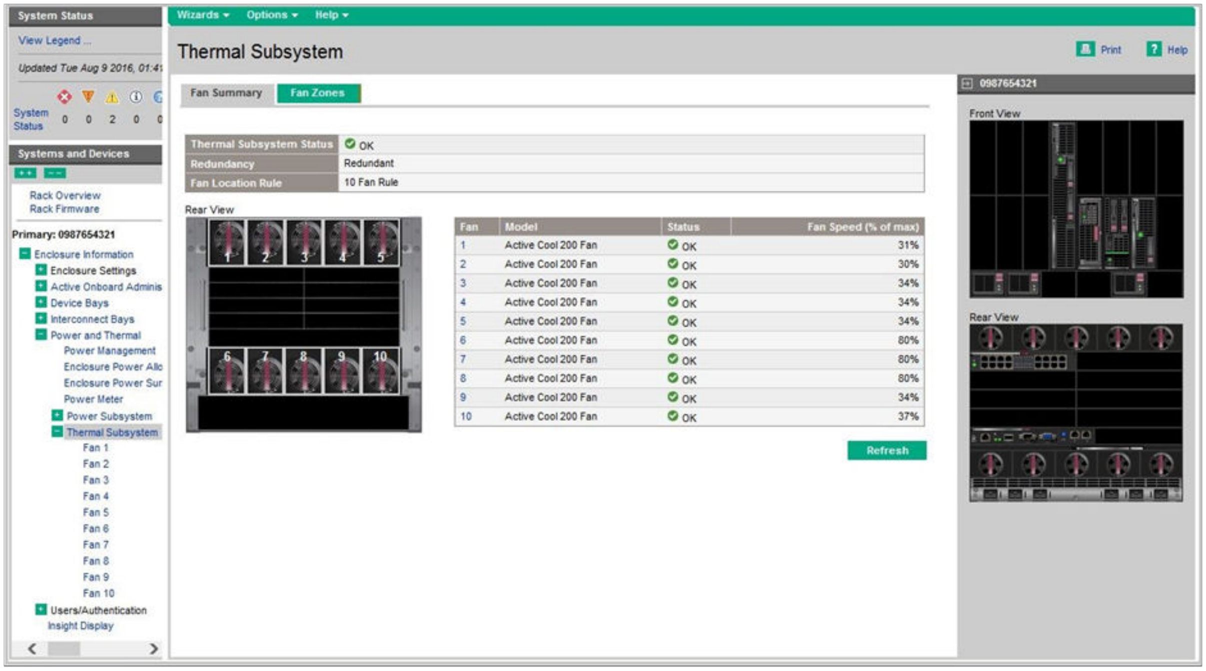
Column	Description
Thermal Zone	The four cooling zones in the enclosure: top left, top right, bottom left and bottom right
Zone Speed	The computed fan speed required based on the highest device need in the zone.
Device Bays	The number of the device bays in a particular thermal zone.
Fan Bay	The fan bay number. Fans in bays 3 and 8 are shared between thermal zones.
Fan Status	The overall status of each fan. Possible values are Unknown, OK, Degraded, Failed, and Absent.
Fan Speed	The fan speed is displayed as a percentage of maximum RPM.

Thermal subsystem

Onboard Administrator monitors up to 10 fans in the enclosure and adjusts fan speeds as necessary, based on thermal and power measurements. The speed of individual fans can be adjusted to reduce noise and power consumption, and to compensate for airflow differences within the enclosure. The performance of each fan is monitored, and Onboard Administrator reports any failures or warnings to the system log and SIM (when SNMP is enabled).

Monitoring fan zones is only available on the c7000 Enclosure. All other thermal subsystem features and functions are the same for c3000 and c7000 Enclosures, except where noted.

The following screen shows the Fan Summary page for a c7000 Enclosure.



Thermal Subsystem

Thermal Subsystem Status	✓ OK
Redundancy	Redundant
Fan Location Rule	10 Fan Rule

Fan	Model	Status	Fan Speed (% of max)
1	Active Cool 200 Fan	✓ OK	31%
2	Active Cool 200 Fan	✓ OK	30%
3	Active Cool 200 Fan	✓ OK	34%
4	Active Cool 200 Fan	✓ OK	34%
5	Active Cool 200 Fan	✓ OK	34%
6	Active Cool 200 Fan	✓ OK	80%
7	Active Cool 200 Fan	✓ OK	80%
8	Active Cool 200 Fan	✓ OK	80%
9	Active Cool 200 Fan	✓ OK	34%
10	Active Cool 200 Fan	✓ OK	37%

Fan Summary

This screen provides status on the thermal subsystem and each individual fan.

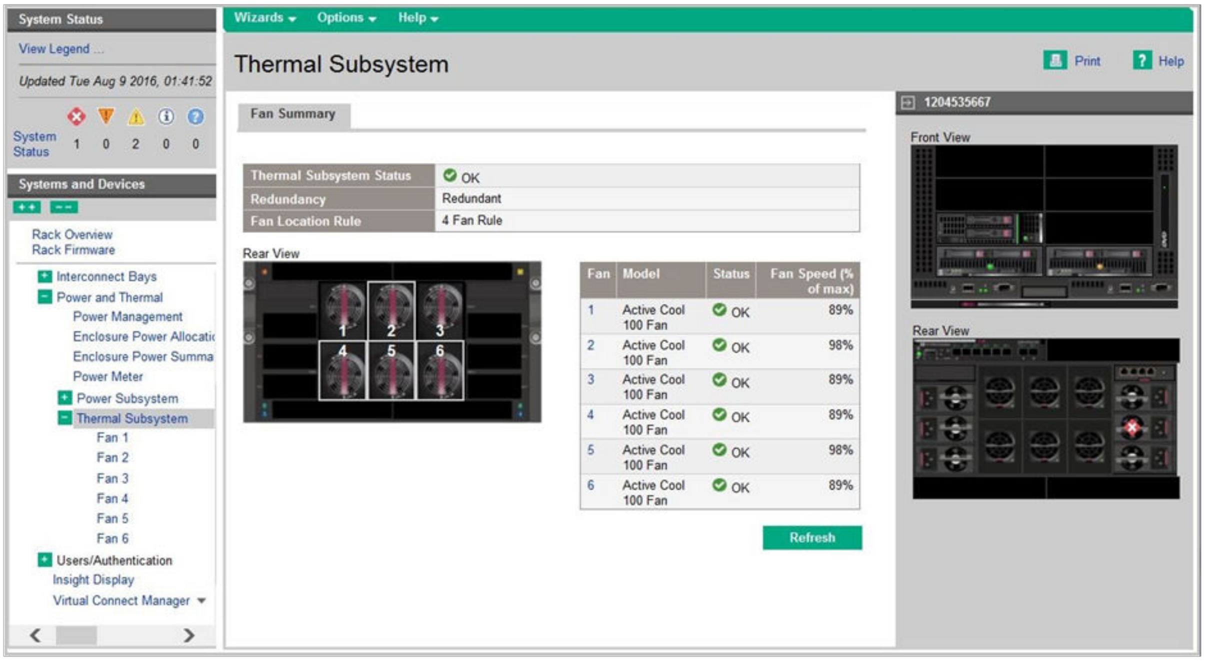
Fan subsystem status

Row	Description
Thermal Subsystem Status	Indicates the overall status of the fan subsystem. Possible values are Unknown, OK, Degraded, or Critical Error.
Redundancy	Indicates the redundancy status of the fans. Possible values are Redundant or Not Redundant
Fan Location Rule	The fan location rule indicates the proper location of the fans and the device bays that are supported.

Fan status

Row	Description
Thermal Subsystem Status	Indicates the overall status of the fan subsystem. Possible values are Unknown, OK, Degraded, or Critical Error.
Redundancy	Indicates the redundancy status of the fans. Possible values are Redundant or Not Redundant
Fan Location Rule	The fan location rule indicates the proper location of the fans and the device bays that are supported.

The following screen shows the Fan Summary page for the c3000 Enclosure.



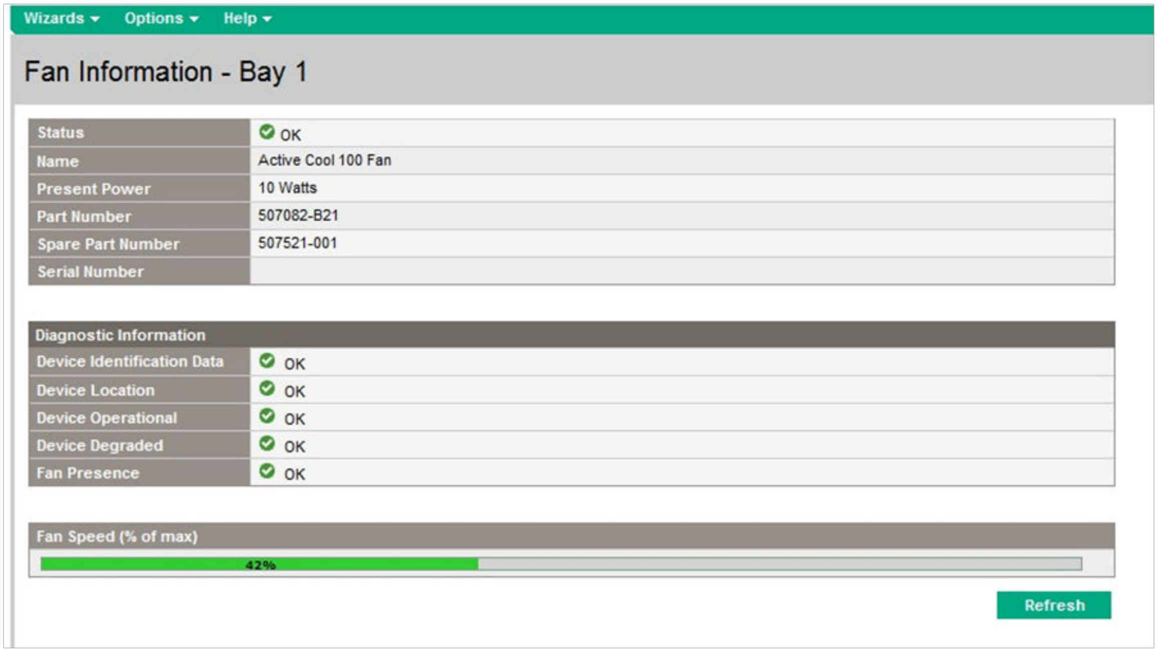
Thermal Subsystem

Thermal Subsystem Status	✓ OK
Redundancy	Redundant
Fan Location Rule	4 Fan Rule

Fan	Model	Status	Fan Speed (% of max)
1	Active Cool 100 Fan	✓ OK	89%
2	Active Cool 100 Fan	✓ OK	98%
3	Active Cool 100 Fan	✓ OK	89%
4	Active Cool 100 Fan	✓ OK	89%
5	Active Cool 100 Fan	✓ OK	98%
6	Active Cool 100 Fan	✓ OK	89%

When a fan module fails, the remaining fans automatically compensate by adjusting fan speeds.

You can view the status of each fan by selecting from either tree navigation or graphical navigation. The Fan Information screen provides information about the overall status, the name, the amount of power consumed in watts, the part number, the spare part number, and the serial number. The Fan Information screen also includes diagnostic information such as internal data errors, location errors, device failures, device degradation, and device mismatch. Fan speeds appear in RPMs. To update information on this page, click the **Refresh** button.



Fan Information - Bay 1

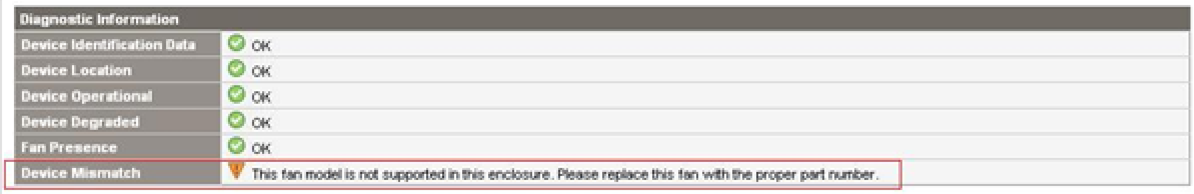
Status	✓ OK
Name	Active Cool 100 Fan
Present Power	10 Watts
Part Number	507082-B21
Spare Part Number	507521-001
Serial Number	

Diagnostic Information	
Device Identification Data	✓ OK
Device Location	✓ OK
Device Operational	✓ OK
Device Degraded	✓ OK
Fan Presence	✓ OK

Fan Speed (% of max)

42%

This screen shows a fan mismatch error.



Diagnostic Information	
Device Identification Data	✓ OK
Device Location	✓ OK
Device Operational	✓ OK
Device Degraded	✓ OK
Fan Presence	✓ OK
Device Mismatch	! This fan model is not supported in this enclosure. Please replace this fan with the proper part number.

Selecting a specific fan opens the Fan Information, Bay x page, where x is the bay of the selected fan. This screen provides status information on the selected fan.

Status information

Row	Description
Status	The overall status of the fan. Possible values are Unknown, OK, Degraded, Failed, and Other.
Name	The common descriptive name of the fan.
Present Power	The amount of power consumed by the fan.
Part Number	The part number to be used when ordering an additional or replacement fan of this type.
Spare Part Number	The spare part number to be used when ordering an additional or replacement fan.
Serial Number	The unique serial number of the fan.

Diagnostic Information

Diagnostic information is gathered by polling a device microcontroller (resulting in a degraded status if a failure has occurred) or is sent by the device microcontroller, without being polled to report a failure.

Row	Description
Device Identification Data	Information such as model name, part number, serial number, and other information used to identify the device is checked. This data is also referred to as FRU data. If the data is not present or not readable by the Onboard Administrator, a device identification data error displays. Possible values are OK or Error.
Device Location	Incorrect fan location. Possible values are OK or Incorrect location for proper device cooling.
Device Operational	Device has failed; status was not requested by the Onboard Administrator.
Device Degraded	Device has failed; status was requested by the Onboard Administrator.
Fan Presence	This field indicates whether a fan is required to support the current fan rule.
Device Mismatch	This field indicates different fan models are installed in the same enclosure and you need to install the same fan models in each bay.

Fan models

The c3000 Enclosure supports Active Cool 100 Fan and Active Cool 200 Fan models. The c7000 Enclosure only supports the Active Cool 200 Fan model. You cannot mix fan models in the c3000 Enclosure. If you mix fan models or you put the wrong fan model in the enclosure you see a **Device Mismatch** error in the Diagnostic Information table.

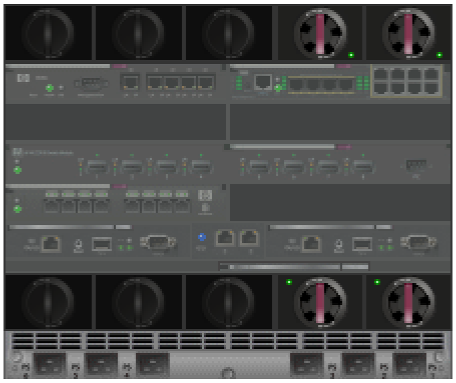
To update the fan information, click **Refresh**.

For proper installation of the fans into the enclosure, see the appropriate BladeSystem c7000 Enclosure Setup and Installation guide.

c7000 Enclosure fan location rules

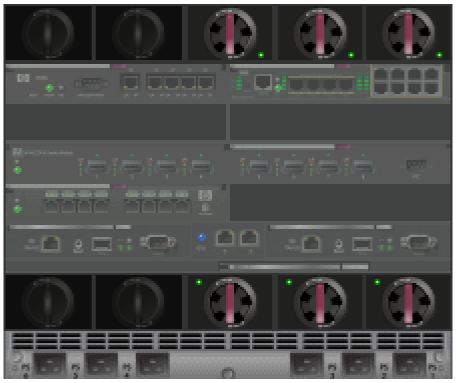
The BladeSystem c7000 Enclosure ships with at least four HPE Active Cool 200 fans and supports up to 10 fans. You must install fans in even-numbered groups, based on the total number of server blades installed in the enclosure. Install fan blanks in unused fan bays.

Four fan rule



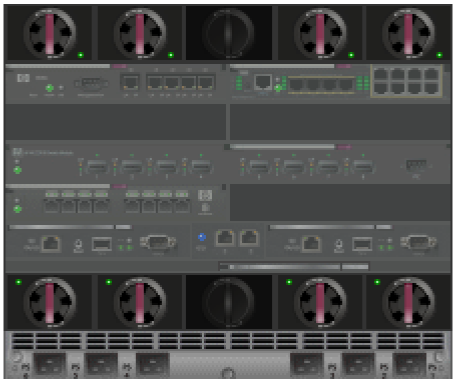
Fan bays 4, 5, 9, and 10 are used for any supported combination of server blades occupying a maximum of two device bays located in device bays 1, 2, 9, or 10.

Six fan rule



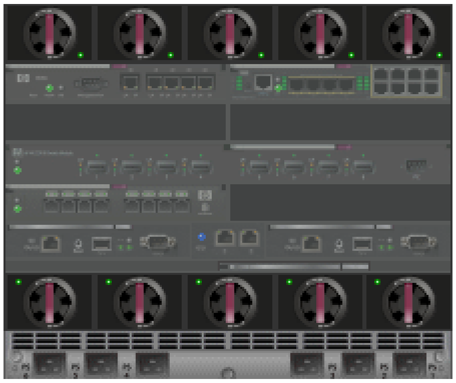
Fan bays 3, 4, 5, 8, 9, and 10 are used for any supported combination of server blades occupying a maximum of eight device bays located in device bays 1, 2, 3, 4, 9, 10, 11, or 12.

Eight fan rule



Fan bays 1, 2, 4, 5, 6, 7, 9, and 10 are used for any supported combination of server blades in all device bays.

Ten fan rule



All fan bays are used for any supported combination of server blades in all device bays.

General fan rules

- A minimum of 6 fans are required for any enclosure configured with a three-phase power input module.
- A minimum of 8 fans are required if at least one switch module is installed in interconnect bay 1, 3, 5, or 7 and at least one switch module is installed in interconnect bay 2, 4, 6, or 8. This does not apply to pass-thru modules.
- Ten fans are required for a configuration with:
  - One or more Virtual Connect FlexFabric-20/40 F8 Modules
  - One or more D2220sb Storage Blades
  - More than half of the enclosure device bays occupied and any quantity of D2200sb Storage Blades present
  - Nine or more HPE BL460c G1 and/or HPE BL460c G5 Server Blades

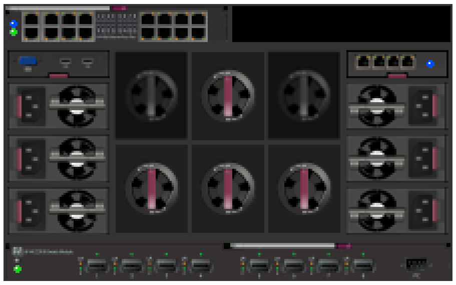
NOTE:

To provide maximum cooling efficiency and redundancy, reduced power consumption, and reduced noise, Hewlett Packard Enterprise strongly recommends ten fans for all configurations.

c3000 Enclosure fan location rules

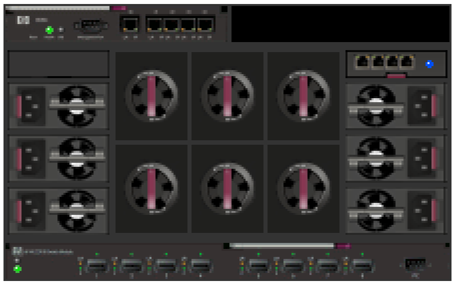
The BladeSystem c3000 enclosure ships with four HPE Active Cool 100 fans and supports up to six fans. You must install fans in even-numbered groups based on the total number of server blades installed in the enclosure. Install fan blanks in unused fan bays.

Four fan rule



For one to four half-height storage or server blades, or one to two full-height storage or server blades, use fan bays 2, 4, 5, and 6 to support a maximum of four device bays located in device bays 1, 2, 5 or 6.

Six fan rule



For additional storage or server blades, install six fans using all device bays.

> **NOTE:**
>
> You cannot install Active Cool 100 fans and Active Cool 200 fans in the same enclosure. The Onboard Administrator sends an error message, and you must remove the type of fan with the least number of units installed.

Managing users

Users/Authentication

This section explains the levels of user rights recognized by the Onboard Administrator and provides detailed procedures to configure the management functionalities provided by the Onboard Administrator.

The Users/Authentication menu item cannot be selected and does not display overview information for user accounts or settings. Instead, select any of the sublevel menu items for specific settings.

Role-based user accounts

Role-based user accounts on Onboard Administrator serve two purposes:

- To control the functions a user has access to on Onboard Administrator.
- To control permissions a temporary user account adopts on iLO when autologin is used.

There are two major aspects of role-based user accounts on Onboard Administrator: bay permissions and a user privilege level. Bay permissions determine which bays the user is allowed to access. Bay permissions are selected during user account creation and allow access to specific device bays, interconnect bays, or Onboard Administrator bays. The privilege level determines which administrative functions the user is allowed to perform. A user's privilege level can be administrator, operator, or user.

A user with an administrator privilege level and with permission to the OA bays in the enclosure is automatically given full access to all bays and can perform any function on the enclosure or bays including managing user accounts and configuring the enclosure. An operator with permission to only the OA bays can configure the enclosure, but the operator cannot manage users or any security settings, nor access any other bays. A user with permission to the OA bays can view only configuration settings, but the user cannot change the settings. The user accounts can be created with multiple bay permissions, but the same privilege level, across those bays.

User accounts configured to permit access to device bays can be created for server administrators. If the user logs into the Onboard Administrator, the user is given information on the permitted server bays. If the user selects the iLO from the Onboard Administrator web GUI, the user is automatically logged into that iLO using a temporary user account with their privilege level. iLO users with administrator privilege level have complete control including modifying user accounts. Operators have full control over the server power and consoles. Users have minimum read-only access to server information. Using this single-sign on feature greatly simplifies managing multiple servers from the Onboard Administrator web GUI.

Permissions for interconnect modules are slightly different. Autologin is not supported for interconnect modules, and all user levels have access to the Management Console link for interconnect bays to which they have permission. Administrators and operators can use the virtual buttons from Onboard Administrator to control power and the UID light on the interconnect module. Users can view only status and information about the interconnect module.

Examples

The following are examples of management scenarios in a c-Class environment and the user accounts that can be created to provide the appropriate level of security.

Scenario 1

A member of an organization needs to have full access to the servers in bays 1-8 to view logs, control power, and use the remote console. The user does not have clearance to manage any settings on Onboard Administrator. The user account to accomplish this security level has an administrator access level and permission to server bays 1-8. Thus, the user does not have permission to Onboard Administrator bays or any interconnect bay.

Scenario 2

A member of an organization needs to manage ports on two interconnect modules in bays 3 and 4. This person needs to know which ports on the switch map to certain servers, but this person must not be able to manage any of the servers. The user account to accomplish this security level has a user access level, permission to all server bays, and permission to interconnect bays 3 and 4. However, this user is not able to control the power or UID LED for the interconnect modules or blades. To control the power or UID to the interconnect modules the user privilege would have to be an operator. To restrict this user from performing server operations such as power control or consoles, the account is restricted to just bay permissions for interconnect bays 3 and 4.

User roles and privilege levels

Within the Users/Authentication category of Onboard Administrator, you can access the Local Users subcategory. In this subcategory, you can create user accounts that individuals use to log in to the Onboard Administrator, and have a username, password, and typically contact information. Users can have one of three privilege levels:

- **ADMINISTRATOR** allows access to all aspects of the Onboard Administrator including configuration, firmware updates, user management, and resetting default settings.
- **OPERATOR** allows access to all information, but only certain configuration settings can be changed. This account is used for individuals who might be required to periodically change configuration settings.
- **USER** allows access to all information, but no changes can be made within Onboard Administrator. This account is used for individuals who need to see the configuration of the Onboard Administrator but do not need the ability to change settings.

The privilege level approach of Onboard Administrator to user permissions facilitates the maintenance of server blade bays. This approach operates according to the following principles:

- Users are assigned privilege levels in User Management.
- A user can have access to any combination of device bays, interconnect bays, and Onboard Administrator bays.

Access to a server blade by a user depends on the privilege level assigned to the user account. If you select a user with Administrator ACL or OA permission, the page will grey out and disable access to the blade and interconnect permissions and select them all.

In cases where SIM is used, Onboard Administrator can integrate with SIM and use SIM users to facilitate a single login from SIM into Onboard Administrator. For more information, see SIM integration.

Local Users

New—To add a new user to the selected enclosure, click **New**. The Add Local User screen appears.

NOTE:

A maximum of 30 user accounts can be configured in FIPS Mode OFF, while a maximum of 21 user accounts can be configured in FIPS Mode ON or Top-Secret.

The maximum user account limit includes reserved accounts such as the Administrator and Virtual Connect accounts.

Edit—Select a user (only one can be selected) by selecting the check box next to the name of the user. To change the settings on the Edit Local User screen, click **Edit**.

Delete—Select a user or users to be deleted by selecting the check box next to the name of each user. To remove the accounts, click **Delete**. If an attempt is made to delete the last remaining Administrator account, you will receive an alert warning that one Administrator account must remain and the delete action will be canceled.

Add Local User

Field	Possible value	Description
Username	1 to 40 characters, including all alphanumeric characters, the dash (-), and the underscore (_)	A maximum of 30 user accounts can be configured in FIPS Mode OFF, while a maximum of 21 user accounts can be configured in FIPS Mode ON or Top-secret. The maximum user account limit includes reserved accounts such as the Administrator and Virtual Connect accounts. The user names ALL (case-insensitive), ADMINISTRATOR (case-insensitive), switch1, switch2, switch3, switch4, switch5, switch6, switch7, switch8, ldapuser, nobody, tbmuser_, vcmuser, and vcmuser_ are reserved and cannot be used. The user name must begin with a letter and is case-sensitive.
Password	When in FIPS Mode ON/Top-secret, or in FIPS Mode OFF with strong passwords enabled, the password must contain at least one character from three of the four types of characters. The four types are uppercase, lowercase, numeric, and non-alphanumeric. The password length must be between 8 and 40 characters. When in FIPS Mode OFF, the password may include any printable character, and the password length must be from 3 to 40 characters.	The password associated with the user.
Password Confirm	Password characters and length must conform to the password rules described in the preceding row.	The password associated with the user. This value must match the Password value.

To save the settings, click **Add User**. The Edit Local User screen appears.

NOTE:

Duplicate users with the same name and different case can be added. Be sure you select the appropriate user when assigning or editing user authorization.

Edit Local User

User information

Field	Possible value	Description
Password	When in FIPS Mode ON/Top-secret, or FIPS Mode OFF with strong passwords enabled, the password must contain at least one character from three of the four types of characters. The four types are uppercase, lowercase, numeric, and non-alphanumeric. The password length must be between 8 and 40 characters. When in FIPS Mode OFF with strong passwords disabled, the password may include any printable character, and the password length must be from 3 to 40 characters.	The password associated with the user.
Password Confirm	Password characters and length must conform to the password rules described in the preceding row.	The password associated with the user. This value must match the Password value.
Full Name	0 to 20 characters, including all alphanumeric characters, the dash (-), the underscore (_), and the space	The user's full name. All users can modify their own full name.
Contact	0 to 20 characters, including all alphanumeric characters, the dash (-), the underscore (_), and the space	Contact information for the user account. The contact information can be the name of an individual, a telephone number, or other useful information. All users can modify their own contact information.

The Username field cannot be modified on the Edit Local User screen.

Privilege level

Account classification	Capabilities	Account name / Privilege level	Bays selected for this account
Administrator	• All commands • Local account, not LDAP • Only account remaining after a reset Onboard Administrator to factory defaults (account retains configured Administrator password) • Administrator account password can be reset to factory default through the Onboard Administrator serial port using `L` lost password recovery option • Can download, add, and clear SSHKey. This key only works with the Administrator account.	Administrator / administrator	All
OA administrator	• All commands • Allows access to all aspects of the BladeSystem Enclosure and Onboard Administrator including configuration, firmware updates, user management, and resetting default settings.	username / administrator	OA bays (all bays automatically selected)
administrator	• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access • administrator permission on device iLO	username / administrator	No OA bays and only selected device bays and interconnect bays
OA operator	Allows access to all aspects of the BladeSystem Enclosure and Onboard Administrator, with the exception of user management	username / operator	OA bays and can have other bays selected, but the capabilities for the other bays are defined in operator [1]
operator	• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access • operator permission on device iLO	username / operator	Selected device bays and interconnect bays

Table Continued

Account classification	Capabilities	Account name / Privilege level	Bays selected for this account
OA user	• Can view status and information of enclosure • Can view CLI history	username / user	OA bays and can have other bays selected, but the capabilities for the other bays are defined in user
user	• Can view status and information of selected bays • Can view CLI history • Can set password for own account • Can set user contact information for own account • Can show CLI commands	username / user	No OA bays and some device bays and interconnect bays

[1] *EBIPA and VLAN features allow access to all bays for an OA operator.*

User Enabled must be selected to enable the user account. If a user account is disabled, then all open sessions for that account are terminated (signed out).

Privilege level change

If a user account privilege level is changed, then all open sessions for that user account are terminated (signed out). The user must sign in again after the privilege level change.

Check boxes

Selecting the device base bay check box does not give the user permission to a double dense server without also checking A and B for that bay. Select only A or B for a device bay if restricting permission to a single server in a double dense server blade.

User Permissions

Check box	Description
Onboard Administrator Bays	Gives the user permissions for the Onboard Administrator bays. If the user privilege level is Administrator, then All Device Bays and All Interconnect Bays are automatically selected when Onboard Administrator Bays is selected and all the check boxes are grayed out.
All Device Bays	Gives the user permissions for all the device bays.
Selected Device Bays	Gives the user permissions for only the selected device bays.
All Interconnect Bays	Gives the user permissions for all the interconnect bays.
Selected Interconnect Bays	Gives the user permissions for only the selected interconnect bays.

To save changes, click **Update User**.

Edit Local User Certificate Information tab

When Two-Factor or CAC Authentication is enabled, you must have a user certificate to sign in to the Onboard Administrator. Users with administrator privileges can upload or map a valid certificate to a selected user.

NOTE:

When the Onboard Administrator is operating in FIPS Mode ON, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. In FIPS Top-Secret Mode - certificates must have a minimum RSA key length of 3072 bits or ECDSA 384 bits, and the signature hash algorithm must be SHA-384.

There are two methods for uploading certificates for use in Onboard Administrator:

- Paste certificate contents into the text field and click **Upload**.
- Paste the URL of the certificate into the URL field and click **Apply**.

When the certificate is successfully uploaded, the SHA1 fingerprint of the user certificate appears.

If you already have a certificate mapped to an account, the SHA1 fingerprint of the certificate appears. Any user with administrator privileges can delete their certificate and upload a new user certificate. When your certificate expires and is renewed, as long as the renewed certificate has the same subject name as the expired one, you do not need to upload the renewed certificate to the Onboard Administrator.

Password settings

This screen enables you to enforce strong password features. Only Administrators with Onboard Administrator permission are allowed to manage strong passwords.

To enable this feature, select **Enable Strong Passwords**. To save the setting, click **Apply**.

NOTE:

This option cannot be disabled while in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug.

With FIPS Mode ON/Top-Secret or strong passwords enabled, the user password must contain three of the four character types listed in the following table.

Character type	Description
Uppercase	An upper-case character from the character set A to Z.
Lowercase	A lower-case character from the character set a to z.
Numeric	A numeric character from the character set 0 to 9.
Non-alphanumeric	Any printable character that is not a space or an alphanumeric character.

With FIPS Mode ON/Top-Secret, or with FIPS Mode OFF, the minimum password length can be from 3 to 40 characters. If the minimum password length is not configured, the default is three characters. With FIPS Mode ON/Top-Secret, or with FIPS Mode OFF and strong passwords enabled, the minimum password length (and default) is eight characters. To save the minimum password length setting, click **Apply**.

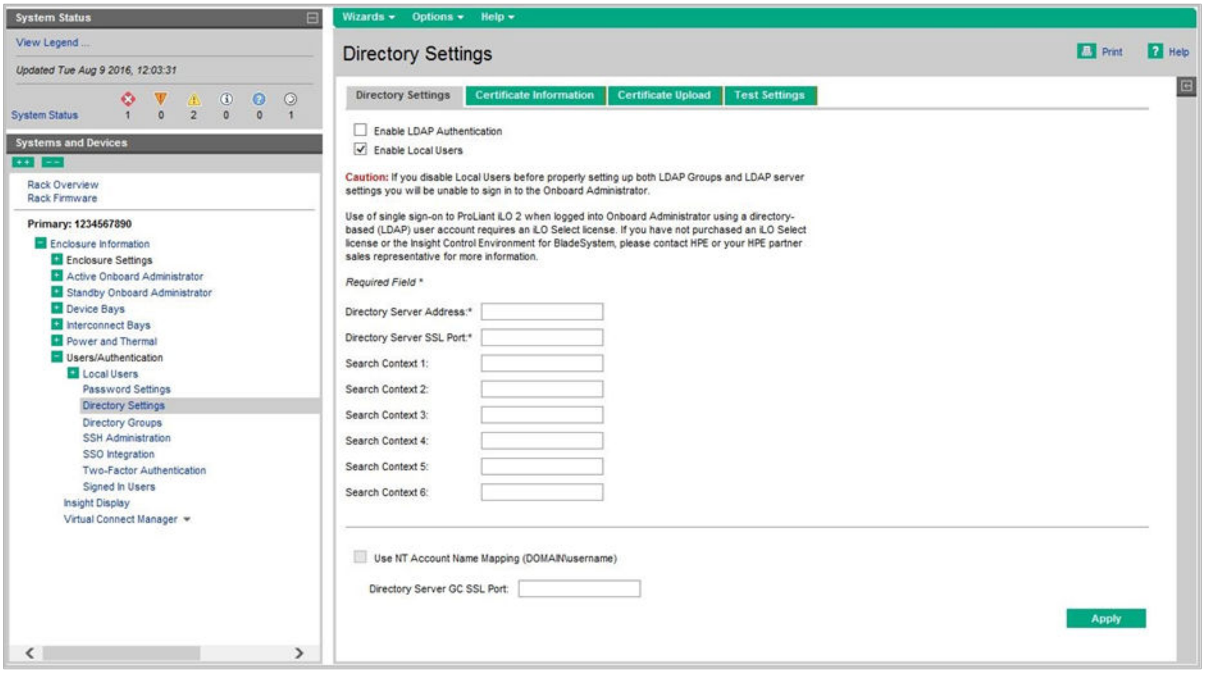
Directory Settings screen

LDAP is a protocol for accessing information directories. While LDAP is based on the X.500 standard, it is significantly simpler than this standard. LDAP also supports TCP/IP and is an open protocol.

NOTE:

The Onboard Administrator LDAP feature supports Microsoft® Active Directory using the `memberOf` attribute. Novell eDirectory is also supported with the `groupMembership` attribute. OpenLDAP is not supported.

Use the Directory Settings screen to set directory access for the currently selected enclosure.



Directory Settings

□ Enable LDAP Authentication

☑ Enable Local Users

Caution: If you disable Local Users before properly setting up both LDAP Groups and LDAP server settings you will be unable to sign in to the Onboard Administrator.

Use of single sign-on to ProLiant iLO 2 when logged into Onboard Administrator using a directory-based (LDAP) user account requires an iLO Select license. If you have not purchased an iLO Select license or the Insight Control Environment for BladeSystem, please contact HPE or your HPE partner sales representative for more information.

*Required Field **

Directory Server Address:*

Directory Server SSL Port:*

Search Context 1:

Search Context 2:

Search Context 3:

Search Context 4:

Search Context 5:

Search Context 6:

□ Use NT Account Name Mapping (DOMAIN\username)

Directory Server GC SSL Port:

- **Enable LDAP Authentication**

  Select this check box to enable a directory server to authenticate a user sign in.
- **Enable Local Users**

  Select this check box to enable a user to sign in using a local user account instead of a directory account.
- **Search Context**

  Specify one to six search contexts. A search context is a search filter or shortcut to a common directory, defining the directory user search to start at the specified path. By specifying a search context, users do not have to specify their full DNs at login. A DN might be long, and users might not be familiar with their DN or might have accounts in different directory contexts. The Onboard Administrator attempts to contact the directory service by DN, and then applies the search contexts in order, beginning with `Search Context 1` and continuing through any subsequent search contexts until successful.

  - **Example 1**:

    Assume that you are `user1`. If you enter the search context `ou=OU1,dc=hp,dc=com`, you can log in as `user1` instead of `cn=user1,ou=OU1,dc=hp,dc=com`.
  - **Example 2**:

    Assume that the following search contexts are defined:

    - Search Context 1: `ou=OU1,dc=hp,dc=com`
    - Search Context 2: `ou=OU2,ou=OU1,dc=hp,dc=com`

    If two users have the same common name, `user1`, in both search contexts, and their passwords are the same, when either user attempts to log in, the Onboard Administrator contacts `cn=user1,ou=OU1,dc=hp,dc=com`.

    If their passwords are different, and a user provides the password for the user in `OU2`, the Onboard Administrator uses DN `cn=user1,ou=OU1,dc=hp,dc=com`, but that will be rejected because the password does not match. The next login will be attempted using `cn=user1,ou=OU2,ou=OU1,dc=hp,dc=com`, which will succeed.

  Search context is also applicable to LDAP directory groups, which are useful when LDAP nested groups are configured. When specifying the search context for an LDAP directory group, the exact context is not required. For example, if a group's location is ou=OU2,ou=OU1,dc=hp,dc=com, the higher-level search context ou=OU1,dc=hp,dc=com can be used to locate that group. This feature helps circumvent the length limit of search contexts. For more information about nested groups, see **Directory Groups**.

Field	Possible value	Description
Directory Server Address	IPv4 Address: ###.###.###.### where ### ranges from 0 to 255 or DNS name of the directory server or the name of the domain. IPv6 Address: ####:####:####:####:####:####:####:####, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.	The IP address or the DNS name or the name of the domain of the directory service. This field is required.
Directory Server SSL Port	1 to 65535	The port used for LDAP communications. Port 636 is the standard SSL LDAP port. This field is required.
Search Context 1	All characters except " (quotes), not to exceed 127 characters	First searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 2	All characters except " (quotes), not to exceed 127 characters	Second searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 3	All characters except " (quotes), not to exceed 127 characters	Third searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 4	All characters except " (quotes), not to exceed 127 characters	Fourth searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 5	All characters except " (quotes), not to exceed 127 characters	Fifth searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.
Search Context 6	All characters except " (quotes), not to exceed 127 characters	Sixth searchable path used to locate the user when the user is trying to authenticate using directory services. The path is also used to search for a nesting LDAP group.

- **Use NT Account Name Mapping (DOMAIN\username)**

Select this check box to enable NT name mapping. This field enables users to log in by using the NT `domain\username` format. The Onboard Administrator may be optionally configured to search the Directory Server Global Catalog and locate the authenticated user information and associated authorized groups. The standard Directory Server GC SSL Port is 3269. This field is optional, and if left blank, the global catalog is not used.

IMPORTANT:

If NT Account Name Mapping is used with the global catalog, and the search context is not restrictive enough, or the domain name is not specified, the Onboard Administrator may associate the authenticated user with a user account that has the same name in a different domain. The authenticated user would then receive the authorization of the user in the other domain. To avoid ambiguity when logging on LDAP user, select search contexts or provide the domain name.

NOTE:

If NT Account Name Mapping is used with the global catalog, and cannot be resolved to a single user, then the user is not authorized to access the Onboard Administrator. This may occur with search contexts that are not restrictive enough and if multiple accounts with the same name exist in different domains. To avoid ambiguity, select search contexts.

Click **Apply** to save settings.

NOTE:

Password rules enforced on LDAP servers might be different than password rules enforced for local user accounts. Make sure both sets of rules adhere to security policies.

Directory Certificate Information tab

This screen displays the detailed information for all LDAP certificates that are currently in effect on the Onboard Administrator.

Row	Description
Issued to	The entity to whom the certificate was issued
Issued by	The certificate authority that issued the certificate
Valid from	The date from which the certificate is valid
Valid until	The date the certificate expires
Serial Number	The serial number assigned to the certificate by the certificate authority
Version	Version number of current certificate
MD5 Fingerprint	Validation of authenticity and is embedded in the certificate
SHA1 Fingerprint	Validation of authenticity and is embedded in the certificate
Public Key	The name of the public key

Click **Remove** below the LDAP certificate you want to remove from the enclosure.

Uploading a certificate

Certificates protect user credentials from "man-in-the-middle" attacks. If certificates are not loaded onto the Onboard Administrator, it is possible for a man-in-the-middle to view LDAP credentials for anyone who logs into the Onboard Administrator. The Onboard Administrator accepts multiple domain controller certificates, which can be uploaded using the Certificate Upload tab under Directory Settings.

To upload a certificate:

1. Obtain the certificate from the domain controller by opening a browser and entering the following address: https://<domain controller>:636

   Where domain controller is the IP address for your network domain controller
2. When prompted to accept a certificate:
   - If you are using Internet Explorer 6, click **View Certificate**.
   - If you are using Internet Explorer 7 or later, click **Continue to this website (not recommended)**, and then click **Certificate Error** in the top address bar. Click **View Certificate.**
3. Click the **Details** tab, and then click the **Copy to File** button.
4. From the list of export options, select Base-64 encoded x.509 (.CER). Provide a name and location for the file, and finish the upload a certificate wizard.
5. Locate the exported certificate file, and then rename it with a .txt extension (for example, dccert.txt). Open the file in a text editor, and then copy the entire contents to the clipboard. The following is an example of an exported certificate file:

   ```
   -----BEGIN CERTIFICATE-----
   MIIFxDCCBKygAwIBAgIKJWUSwAAAAAAAAjANBgkqhkiG9w0BAQUFADBVMRMwEQYK
   CZImiZPyLGQBGRYDY29tMRIwEAYKCZImiZPyLGQBGRYCaHAxFzAVBgoJkiaJk/Is
   ZAEZFgdhdGxkZW1vMREwDwYDVQQDEwh3aW5kb3pDQTAeFw0wNjA4MjIyMDIzMTFa
   Fw0wNzA4MjIyMDIzMTFaMCAxHjAcBgNVBAMTFXdpbmRvei5hdGxkZW1vLmhwLmNv
   bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAy4zeh3iXydUAWKVHIDsxLJ6B
   aRuVT9ZhkL5NQHIDeRjumsgc/jHSERDmHuyoY/qbF7JMhJ9Lh9QQHUg8QfEYsC1y
   qTvgisrZeHtvmrmecvSxZm27b4Bj5XYN0VYcrwqKnH7X/tVhmwqGls7/YZyahNU1
   lGB2OjoCq5eJxX+Ybx0CAwEAAaOCA00wggNJMAsGA1UdDwQEAwIFoDBEBgkqhkiG
   9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4D
   …output truncated…
   -----END CERTIFICATE-----
   ```
6. Return to the Onboard Administrator, paste the certificate contents into the window, and then click **Upload**.

Directory Certificate Upload tab

This screen enables you to upload an LDAP certificate to the Onboard Administrator to establish a trusted relationship with the LDAP server. You can upload a maximum of four certificates.

There are two methods for uploading certificates for use in Onboard Administrator:

- Paste certificate contents into the text field and click **Upload**.
- Paste the URL of the certificate into the URL field and click **Apply**.

Directory Test Settings tab

The **Test Settings** tab enables Onboard Administrator administrators to ensure that the configuration information provided allows the directory user access to the Onboard Administrator and to the resources in the enclosure. The **Test Settings** tab applies only to the current settings. Therefore, after making changes to the **Directory Settings** tab, you must click **Apply**, and then select the **Test Settings** tab.

Use the **Test Settings** tab to run and report the tests. When the tab page initially appears, it contains a list of tests with the current status of `Not Run`. To run the tests, click **Test Settings**. The tests are run in the order that they appear. The tests terminate when an error occurs. To perform the User Authentication and User Authorization tests, you must enter a user name and password in **Directory Test Controls**.

The following tests are performed in the order listed.

- **Overall Test Status**

The Overall Test Status is an aggregation of all the tests run. The value will either be `Not Run`, `Passed`, or `Failed`. If any of the individual tests fail, the status is `Failed`.

- **Ping Directory Server**

  A simple ping test is performed after a valid IP address or domain name is verified for the directory server. The ping test sends a maximum of four ping packets to the directory server and reports success or failure.

  - A successful test reports that Onboard Administrator can establish a network path to the directory server.
  - A failed test reports that Onboard Administrator cannot establish a network path to the directory server. The administrator should verify the host name or IP address.
- **Directory Server IP Address**

  If the LDAP configuration specifies an IP address instead of a DNS, then this test validates that the IP address is a valid IPv4 address. Otherwise, the test reports the `Not Run` status.

  - A successful test reports that the IP address stored for the directory server is a valid IPv4 address.
  - A failed test reports that the IP address stored for the directory server is not a valid IPv4 address. The administrator must verify the IP address entered and correct the IP address.
- **Directory Server DNS Name**

  The DNS lookup test determines if Onboard Administrator can resolve the domain name of the LDAP server. If the LDAP server configuration uses IP addresses instead of a DNS name, then this test reports the `Not Run` status.

  - A successful test reports that Onboard Administrator is able to resolve the Directory Server host name using domain name.
  - A failed test reports that Onboard Administrator is unable to resolve the Directory Server host name. The administrator must verify that the directory server host name is correct and that the host name is correct for the directory server.
- **Connect to Directory Server**

  This test attempts to connect to the specified directory server IP address and service port.

  - A successful test reports that Onboard Administrator can establish a connection to the directory server at the specified host name or address and at the specified port number. The successful test indicates that network service is available; the directory service is running and available at the specified directory server and port.
  - A failed test reports that Onboard Administrator cannot establish a connection to the directory server. The unsuccessful test reports that the network service is not available. The administrator must verify the host name or address and port number.
- **Connect using SSL**

  This test verifies that the directory server is providing the directory service over an SSL connection.

  - A successful test reports that Onboard Administrator can establish an SSL connection to the directory server host name or IP address and port. The network service is available as a secure SSL connection.
  - A failed test reports that the network service is not available as a secure SSL connection and the Onboard Administrator does not allow this type of connection. The administrator must identify a directory server that supports SSL connections or reconfigure the directory server to use SSL connections.
- **Certificate of Directory Server**

  If the directory server SSL certificate has been loaded onto Onboard Administrator, use this test to verify that the certificate provided by the directory server matches the current certificate stored on Onboard Administrator. If the directory server SSL certificate has not been loaded, then this test does not run.

    - A successful test reports that Onboard Administrator was able to validate the directory server certificate against the certificates stored on Onboard Administrator for the specified directory server.
    - A failed test reports that the directory server certificate stored on Onboard Administrator does not match the certificate provided on the SSL connection.
- **User Authentication**

  This test attempts to log in the user to the directory by using the user name and password provided in **Directory Test Controls**. If user authentication fails using the provided user name and password, then each search context is attempted. If a search context begins with the character @, then the DN used to log in is the search name concatenated to the user name entered. Otherwise, the search DN used to log in is constructed as follows: `cn=<username>,<search context>`. The result from this test identifies the search context that was successful in authenticating the user.
- **User Authorization**

  After a user has successfully authenticated and logged into Onboard Administrator, the configured directory group to which the user belongs is identified. A user might belong to multiple directory groups, so the directory group that gives the user the most privileges is identified.

    - A successful test reports the directory group with the highest privilege levels for the authenticated user.
    - A failed test reports the authenticated user does not have any authorization on Onboard Administrator because the user does not belong to any of the configured directory groups.

Test Log

This is a running log of the details associated with the tests that have run and the results of those tests.

Directory Test Controls

The user name and password are sent to the LDAP server for authentication before the User Authentication and User Authorization tests are performed. The Onboard Administrator limits the length of the user name and password as indicated. Authentication requirements are defined by the LDAP server; the length limits imposed by the LDAP server might be more restricted than the limits imposed by the Onboard Administrator .

- User Name—Accepts 0 to 256 characters.
- Password—Accepts 0 to 1024 characters.

Directory Groups

Access to the enclosure can be granted using LDAP. To use the LDAP server, you must create directory accounts.

The Directory Groups screen displays current directory groups that have been added to the Primary Connection enclosure. You may add user groups to all enclosures. You may edit and delete user groups from the Primary Connection enclosure only. To use LDAP services, you must add at least one directory group.

Column	Description
Check box	Used to select Directory Group for editing or deleting
Group Name	1 to 255 characters and contains the same characters as search contexts. The group name is used to determine LDAP users' group membership. The group name must match one of the following five properties of a directory group: the name, distinguished name, common name, Display Name, or SAM Account Name. For nested groups, matching is based on `objectSid` (an attribute that specifies the security ID of the group). The distinguished name is recommended to uniquely specify the LDAP group. If the Onboard Administrator is configured to search the GC port and a distinguished name is not used, then an incorrect match in multiple domains may occur which could result in unintended authorization.

Table Continued

Column	Description
Privilege Level	Used to determine which administrative functions the user is allowed to perform. A user's privilege level can be administrator, operator, or user.
Description	0 to 58 characters, containing alphanumeric characters, the dash (-), the underscore (_), and the space. The description of the LDAP group, a more readable version of the group name, or other useful information.

- **New**—To add a new Directory Group to the selected enclosure, click **New**. You can add a maximum of 30 Directory Groups. The Add LDAP Group screen appears.
- **Edit**—Select a Directory Group to be edited by selecting the check box next to the name of the group. To change the settings on the Edit LDAP Group screen, click **Edit**.
- **Delete**—Select the Directory Group to be deleted by selecting the check box next to the name of the group. To remove the group, click **Delete**.

Nested LDAP group support

When using Microsoft Active Directory, you can place one or more groups in another group. Groups that are contained within another group are called nested groups. The group that contains nested groups is called a nesting group. The advantage of nested groups is that users of a nested group can log in to the Onboard Administrator if their nesting group is configured appropriately. For example, assume `group2` is nested in `group1`. Users in `group2` are allowed to log in to the Onboard Administrator if the parent LDAP group (`group1`) is added to the Onboard Administrator and can be found using one of the search contexts. The search context is not restricted to the exact location: if the search context path is high in the LDAP directory tree, subtree searching is used. The Onboard Administrator supports the security group type only. Distribution group type is not supported.

Add an LDAP Group

Group information

NOTE:

A maximum of 30 Directory Groups can be added.

Field	Possible value	Description
Group Name	1 to 255 characters; all characters except quotation marks ("). The first character of the group name must be an alpha character.	The group name is used to determine LDAP users' group membership. The group name must match one of the following five properties of a directory group: the name, distinguished name, common name, Display Name, or SAM Account Name. The distinguished name is recommended to uniquely specify the LDAP group. If the Onboard Administrator is configured to search the GC port and a distinguished name is not used, then an incorrect match in multiple domains may occur which could result in unintended authorization.
Description	0 to 58 characters, including all alphanumeric characters, the dash (-), the underscore (_), and the space	Can contain a more readable version of the group name, as well as other useful information

Privilege level

Account classification	Capabilities	Account name / Privilege level	Bays selected for this account
Administrator	• All commands • Local account, not LDAP • Only account remaining after a reset Onboard Administrator to factory defaults (account retains configured Administrator password) • Administrator account password can be reset to factory default through the Onboard Administrator serial port using `L` lost password recovery option • Can download, add, and clear SSHKey. This key only works with the Administrator account.	Administrator / administrator	All
OA administrator	• All commands • Allows access to all aspects of the BladeSystem Enclosure and Onboard Administrator including configuration, firmware updates, user management, and resetting default settings.	username / administrator	OA bays (all bays automatically selected)
administrator	• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access • administrator permission on device iLO	username / administrator	No OA bays and only selected device bays and interconnect bays
OA operator	Allows access to all aspects of the BladeSystem Enclosure and Onboard Administrator, with the exception of user management	username / operator	OA bays and can have other bays selected, but the capabilities for the other bays are defined in operator [1]
operator	• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access • operator permission on device iLO	username / operator	Selected device bays and interconnect bays

Table Continued

Account classification	Capabilities	Account name / Privilege level	Bays selected for this account
OA user	• Can view status and information of enclosure • Can view CLI history	username / user	OA bays and can have other bays selected, but the capabilities for the other bays are defined in user
user	• Can view status and information of selected bays • Can view CLI history • Can set password for own account • Can set user contact information for own account • Can show CLI commands	username / user	No OA bays and some device bays and interconnect bays

[1] EBIPA and VLAN features allow access to all bays for an OA operator.

Group permissions

Check box	Description
Onboard Administrator Bays	Gives the user permissions for the Onboard Administrator bays. If the user privilege level is Administrator, then All Device Bays and All Interconnect Bays are automatically selected when Onboard Administrator Bays is selected and all the check boxes are grayed out.
All Device Bays	Gives the user permissions for all the device bays.
Selected Device Bays	Gives the user permissions for only the selected device bays.
All Interconnect Bays	Gives the user permissions for all the interconnect bays.
Selected Interconnect Bays	Gives the user permissions for only the selected interconnect bays.

To save settings, click **Add Group**.

Edit an LDAP Group

Group information

Field	Possible value	Description
Group Name	1 to 255 characters; all characters except quotation marks ("). The first character of the group name must be an alpha character.	The group name is used to determine LDAP users' group membership. The group name must match one of the following five properties of a directory group: the name, distinguished name, common name, Display Name, or SAM Account Name. The distinguished name is recommended to uniquely specify the LDAP group. If the Onboard Administrator is configured to search the GC port and a distinguished name is not used, then an incorrect match in multiple domains may occur which could result in unintended authorization.
Description	0 to 58 characters, including all alphanumeric characters, the dash (-), the underscore (_), and the space	Can contain a more readable version of the group name, as well as other useful information

Privilege level

Account classification	Capabilities	Account name / Privilege level	Bays selected for this account
Administrator	• All commands • Local account, not LDAP • Only account remaining after a reset Onboard Administrator to factory defaults (account retains configured Administrator password) • Administrator account password can be reset to factory default through the Onboard Administrator serial port using `L` lost password recovery option • Can download, add, and clear SSHKey. This key only works with the Administrator account.	Administrator / administrator	All
OA administrator	• All commands • Allows access to all aspects of the BladeSystem Enclosure and Onboard Administrator including configuration, firmware updates, user management, and resetting default settings.	username / administrator	OA bays (all bays automatically selected)
administrator	• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access • administrator permission on device iLO	username / administrator	No OA bays and only selected device bays and interconnect bays

Table Continued

Account classification	Capabilities	Account name / Privilege level	Bays selected for this account
OA operator	Allows access to all aspects of the BladeSystem Enclosure and Onboard Administrator, with the exception of user management	username / operator	OA bays and can have other bays selected, but the capabilities for the other bays are defined in operator [1]
operator	• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access • operator permission on device iLO	username / operator	Selected device bays and interconnect bays
OA user	• Can view status and information of enclosure • Can view CLI history	username / user	OA bays and can have other bays selected, but the capabilities for the other bays are defined in user
user	• Can view status and information of selected bays • Can view CLI history • Can set password for own account • Can set user contact information for own account • Can show CLI commands	username / user	No OA bays and some device bays and interconnect bays

[1] *EBIPA and VLAN features allow access to all bays for an OA operator.*

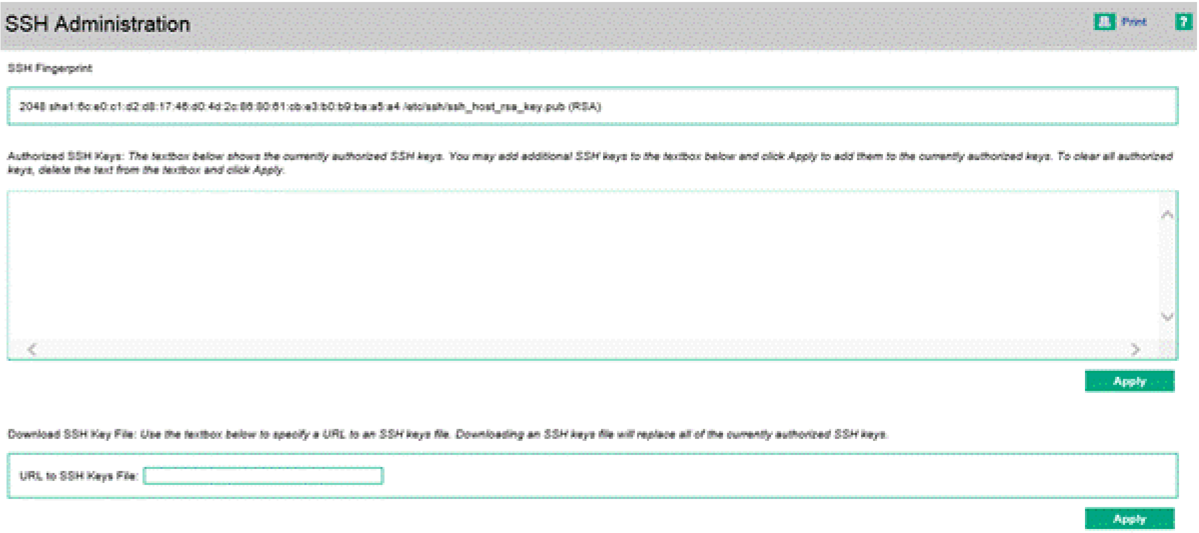
Group permissions

Check box	Description
Onboard Administrator Bays	Gives the user permissions for the Onboard Administrator bays. If the user privilege level is Administrator, then All Device Bays and All Interconnect Bays are automatically selected when Onboard Administrator Bays is selected and all the check boxes are grayed out.
All Device Bays	Gives the user permissions for all the device bays.
Selected Device Bays	Gives the user permissions for only the selected device bays.
All Interconnect Bays	Gives the user permissions for all the interconnect bays.
Selected Interconnect Bays	Gives the user permissions for only the selected interconnect bays.

To save settings, click **Update Group**.

SSH Administration

The SSH Administration page lists the owner of each authorized SSH key and enables the adding of new keys.



SSH Fingerprint

2048 sha1:6c:e0:c1:d2:d8:17:46:d0:4d:2c:86:80:61:cb:e3:b0:b9:ba:a5:a4 /etc/ssh/ssh_host_rsa_key.pub (RSA)

Authorized SSH Keys: The textbox below shows the currently authorized SSH keys. You may add additional SSH keys to the textbox below and click Apply to add them to the currently authorized keys. To clear all authorized keys, delete the text from the textbox and click Apply.

Download SSH Key File: Use the textbox below to specify a URL to an SSH keys file. Downloading an SSH keys file will replace all of the currently authorized SSH keys.

URL to SSH Keys File:

SSH Fingerprint—Lists the public key portion of a public/private key pair.

Authorized SSH Keys—Lists the authorized SSH key data. The owner is always the Administrator. To add additional Authorized SSH Keys, enter the SSH key in the text box and click **Apply**. To clear all Authorized SSH Keys, delete all the text in the text box and click **Apply**.

Download SSH Key File—In the **URL to SSH Keys File** field, enter the location of the public key file, and click **Apply** to download. All currently authorized SSH keys are replaced when the SSH key file is downloaded. Each key is associated with the Administrator account.

NOTE:

When the Onboard Administrator is operating in FIPS Mode ON, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. In FIPS Top-Secret Mode - certificates must have a minimum RSA key length of 3072 bits or ECDSA 384 bits, and the signature hash algorithm must be SHA-384.

Supported SSH and SSL versions

Onboard Administrator version	SSL version	SSH version
v1.20	openssl – 0.9.7k	openssh – 4.2p1
v2.00	openssl – 0.9.7l	openssh – 4.2p1
v2.30 - v2.60	openssl – 0.9.7m	openssh – 4.4p1
v3.00	openssl – fips-1.2 openssl – 0.9.8j	openssh – 5.1p1
v3.10	openssl – fips-1.2 openssl – 0.9.8n	openssh – 5.1p1
v 3.20	openssl – fips-1.2 openssl – 0.9.8n	openssh – 5.1p1
v3.50 - v3.55	openssl – 0.9.8r	openssh – 5.8p2

Table Continued

Onboard Administrator version	SSL version	SSH version
v3.56 - v3.71	openssl – 0.9.8w	openssh – 5.8p2
v4.01 - 4.02	openssl – 0.9.8y	openssh – 5.8p2
v4.11 - v4.22	openssl – fips-2.0.5 openssl – 1.0.1e	openssh – 6.2p2
v4.30	openssl – fips-2.0.5 openssl – 1.0.1f	openssh – 6.2p2
v4.40 - v4.60	openssl – fips 2.0.5 openssl – 1.0.1h	openssh – 6.2p2
v4.70	openssl – fips 2.0.5 openssl – 1.0.2h	openssh – 6.2p2

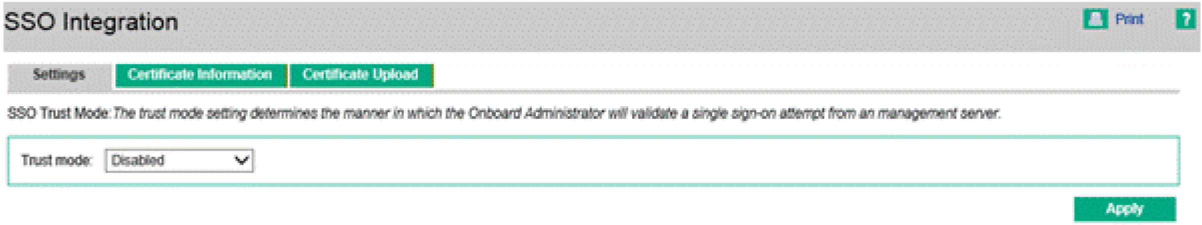
HPE SSO Integration

HPE BladeSystem Onboard Administrator supports SSO with trusted applications, such as HPE OneView or HPE SIM. The SSO feature enables you to log in to a trusted management application and then be able to access automatically any managed devices where the SSO certificate is installed. To configure SSO to work through SSO:

1. Set the SSO trust mode to ON. On the SSO Integration screen, select **Trust by Certificate** from the **Trust mode** dropdown menu.

   NOTE:

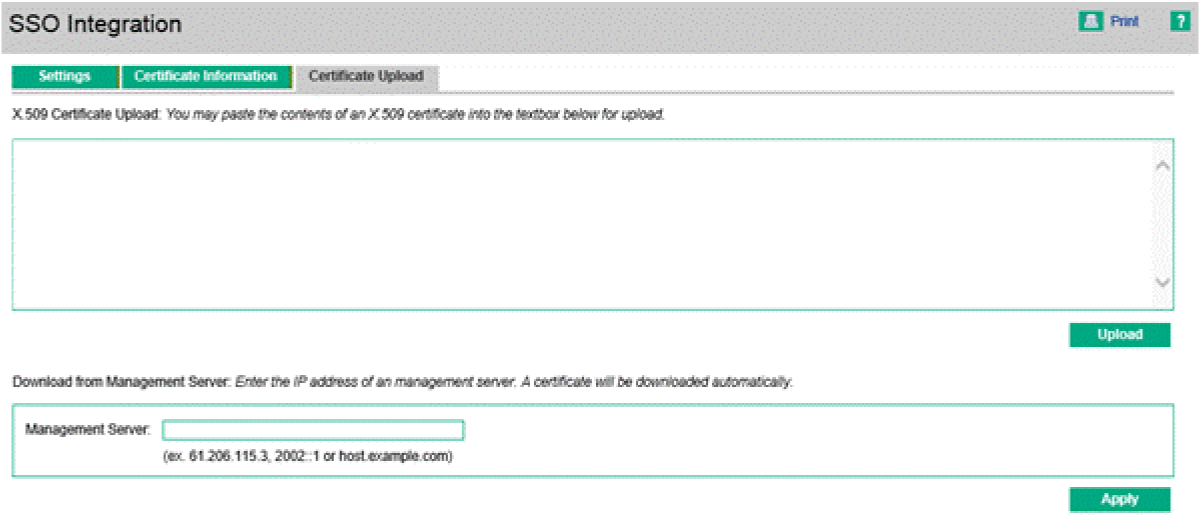
   When trust mode is disabled, the HPE SSO single sign-on attempt fails, and you must enter Onboard Administrator credentials to log on.



SSO Trust Mode: *The trust mode setting determines the manner in which the Onboard Administrator will validate a single sign-on attempt from an management server.*

Trust mode: Disabled

2. On the HPE SSO Integration screen, select the **Certificate Upload** tab.
3. To upload a certificate, use one of the following methods:
   - Paste the contents of the certificate into the text box, and click **Upload**.
   - Enter the IP address of the SSO system that will be managing the enclosure, and click **Apply**.



X.509 Certificate Upload: *You may paste the contents of an X.509 certificate into the textbox below for upload.*

Download from Management Server: *Enter the IP address of an management server. A certificate will be downloaded automatically.*

Management Server:
(ex. 61.206.115.3, 2002::1 or host.example.com)

NOTE:

Onboard Administrator 4.12 and later contains SSO application support for determining the minimum SSO certificate requirements.

Two-Factor Authentication

Two-Factor Authentication Settings tab

IMPORTANT:

Onboard Administrator must be configured in Virtual Connect mode before enabling Two-Factor Authentication when using Virtual Connect Manager and Two-Factor Authentication.

When Two-Factor Authentication is enabled, only users with a valid user certificate are allowed to sign in to Onboard Administrator. A valid user certificate is signed by a trusted Certificate Authority and is mapped to the respective user on the Onboard Administrator.

To enable Two-Factor Authentication for user authentication during sign in, select **Enable Two-Factor Authentication**. When Two-Factor Authentication is enabled, SSH and Telnet access is disabled by default. Disabling Two-Factor Authentication does not automatically re-enable SSH and Telnet. You must go to the Network Access screen, and then select **Enable Secure Shell** and **Enable Telnet**.

To enable the Onboard Administrator to verify with the Certifying Authority that the certificate being used has been added to the certificate revocation list (CRL), select **Check for Certificate Revocation**. If the certificate is on the CRL, the sign in is denied.

Certificate Owner field

You can configure the Onboard Administrator to use the user principle name in the SAN by selecting SAN or to use the certificate subject name by selecting Subject when authenticating directory users with a directory server.

To save settings, click **Apply**.

For information about configuring Two-Factor Authentication for local user and LDAP group accounts, see **Creating CAs and configuring Two-Factor Authentication for local user and LDAP group accounts**.

Two-Factor Authentication Certificate Information tab

This screen displays all Insight Remote Control server certificates trusted by the Onboard Administrator. A maximum of 12 certificates can be uploaded to the Onboard Administrator.

Row	Description
Certificate Version	Version number of current certificate
Issuer Organization	Name of the organization that issued the certificate
Issuer Organization Unit	Name of the organizational unit that issued the certificate
Issued By	The certificate authority that issued the certificate
Subject Organization	Subject name
Issued To	Organization to whom the certificate was issued
Valid From	The date from which the certificate is valid
Valid Upto	The date the certificate expires
Serial Number	The serial number assigned to the certificate by the certificate authority
Extension Count	Number of extensions in the certificate
MD5 Fingerprint	This field can be used to validate the authenticity of the certificate
SHA1 Fingerprint	This field can be used to validate the authenticity of the certificate.

To remove an existing certificate, click **Remove**.

Two-Factor Authentication Certificate Upload tab

To enable Two-Factor Authentication, upload at least one valid certificate belonging to a CA to the Onboard Administrator.

There are two methods for uploading certificates for use in Onboard Administrator:

- Paste certificate contents into the text field and click **Upload**.
- Paste the URL of the certificate into the URL field and click **Apply**.

Authenticating OA with the Common Access Card

The Common Access Card is the standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel in the United States. It is used to enable physical access to buildings and controlled spaces, and provides access to DoD computer networks and systems. The Common Access Card (CAC) can be used for access into computers and networks that are equipped with various smart card readers. When it is inserted into the reader, the device asks the user for a PIN to access the certificate loaded in the card.

By using a combination of PIN and Certificate , a CAC satisfies the requirement for two-factor authentication: something the user knows combined with something the user has. The CAC also satisfies the requirements for digital signature and data encryption technologies: authentication, integrity and non-repudiation.

CAC feature in Onboard Administrator (OA) 4.71 supports integration of c3000 & c7000 enclosures with DoD environments leveraging CAC authentication.

The request for and presentation of the client certificate happens during initial SSL session establishment. Below are the core elements in the process of a user gaining access to Onboard Administrator enabled for CAC:

- Authentication occurs during SSL session establishment and entails:

    - Verifying the certificate date.
    - Verifying the revocation status using Online Certificate Status Protocol (OCSP) or Online Certificate Revocation List (CRL).
    - Verifying the full chain to the Certificate Authority (CA).
- Authorization occurs after SSL session establishment and the matching of the Certificate Subject Alternate Name (SAN) or Subject against the User Principal Name (UPN) of the appropriate principal in Active Directory.

CAC Authentication Settings tab

To enable CAC Authentication for user authentication during sign in, select **Enable CAC Authentication**.When CAC Authentication is enabled, SSH, Telnet, and XML Reply are disabled by default. However SSH and Telnet can be enabled by the user while XML Reply cannot be enabled in CAC Authentication mode.

When CAC Authentication mode is disabled both SSH and XML Reply mechanisms are automatically enabled. However Telnet interface needs to be enabled manually in the **network access** screen by selecting **Enable Telnet** option.

The Onboard Administrator can be configured to validate the certificates using two methods.

- **Using Certificate Revocation List (CRL)**

  Select **Check for Certificate Revocation using CRL** . If the certificate is revoked, then the sign in is denied.
- **Using Online Certificate Status Protocol (OCSP)**

  Select **Check for Certificate Revocation using OCSP**. If OCSP is enabled, the certificate presented for CAC sign in should have OCSP responder link in it. An OCSP responder (a server typically run by the certificate issuer) may return a signed response signifying that the certificate specified in the request is 'good', 'revoked', or 'unknown'. Sign in is successful for users whose certificate gets 'good' response from the responder.

  NOTE: In case OCSP responder is not reachable, sign in will be allowed based on the result of CRL verification.

Certificate Owner field

Onboard Administrator can be configured to use one of the two fields of the user certificate to authenticate the user.

- User Principal Name (UPN) in the Subject Alternate Name (SAN) - this can be enabled by selecting "SAN" option.
- Certificate Subject Name - This can be enabled by selecting "Subject " option. When Subject is selected, the first Common Name (CN) field of the certificate subject name will be used.

For information about configuring CAC Authentication for local user and LDAP group accounts, see section:

Creating CAs and configuring Two-Factor Authentication for local user and LDAP group accounts

CAC Authentication Certificate Information tab

This screen displays all Insight Remote Control server certificates trusted by the Onboard Administrator. A maximum of 12 certificates can be uploaded to the Onboard Administrator .

Certificate Fields and Descriptions:

ROW	DESCRIPTION
Certificate Version	Version number of current certificate
Issuer Organization	Name of the organization that issued the certificate
Issuer Organizational Unit	Name of the organizational unit that issued the certificate
Issued By	The certificate authority that issued the certificate
Subject	Organization Subject Name
Issued To	Organization to whom the certificate was issued
Valid From	The date from which the certificate was valid
Valid Upto	The date the certificate expires
Serial Number	The serial number assigned to the certificate by the certificate authority
Extension Court	Number of extensions in the certificate
MD5 Fingerprint	The field can be used to validate the authenticity of the certificate
SHA1 Fingerprint	The field can be used to validate the authenticity of the certificate

To remove an existing certificate, select the certificate and click **Remove**.

CAC Authentication Certificate Upload tab

To enable CAC Authentication, upload at least one valid certificate belonging to a CA .

There are two methods for uploading certificates for use in Onboard Administrator:

- Paste certificate contents into the text field and click **Upload**.
- Paste the URL of the certificate into the URL field and click **Apply**.

Signed In Users

This screen displays all the current sessions signed in to the Onboard Administrator. This screen is only available to Administrators with Onboard Administrator access. The Administrator can terminate sessions, disable users, and delete users from this screen.

Current Session—This table lists the session created when you signed in to the Onboard Administrator.

Other Sessions—This table lists the other users signed in to the Onboard Administrator.

Column	Description
Check box	Used to select a user or all users.
Username	The name of the user signed in to the enclosure.
IP Address	The user account IP address. The IP address of the session can be an enclosure linked address if it looks like "169.254.1.x". These sessions are created by other linked enclosures. Performing a delete, disable, or terminate session on a user with a linked enclosure IP address might end the enclosure link sessions of other users. For KVM and Serial logins the IP address field displays Local.
Age	The length of time, measured in days, hours, minutes and seconds, the user account has been signed in.

Table Continued

Column	Description
Idle Time	The length of time, measured in days, hours, minutes and seconds, the signed in account has been idle.
User Type	The type of user signed in to the enclosure. Possible values are Local, LDAP, or SSO.
Session Type	The type of session of the signed in user. Possible values are Web, SSH, Telnet, KVM, Serial, and Factory Diagnostics.
OA Module	The Onboard Administrator module the user is signed into. Possible values are Active or Standby.

Delete Users—Select a user or users to be deleted by selecting the check box next to the name of the user, and click **Delete Users**. You cannot delete your own account or the built-in Administrator account.

Disable Users—Select a user or users to be disabled by selecting the check box next to the name of the user, and click **Disable Users**. You cannot disable your own account or the built-in Administrator account.

Terminate Sessions—Select a user or users whose sessions you want to terminate by selecting the check box next to the name of the user, and click **Terminate Sessions**. You cannot terminate your own session.

Session Options tab

This screen enables you to specify the length of time a user session is valid if there is no activity. Sessions are checked every five minutes to see if they have been inactive for the amount of time specified by the system administrator. If any sessions have been inactive for the specified amount of time, they are removed from the system.

Session Timeout—The number of minutes before an inactive session becomes invalid. Session Timeout can be any value between 10 and 1440 (24 hours). To disable Session Timeout, set it to 0. The default value for Session Timeout is 1440. After entering a Session Timeout value, click **Apply**.

Insight Display

All Onboard Administrator GUI users can access the Insight Display screens by selecting Insight Display from the Tree View or Rack Overview.

The Security tab can lock the Insight Display buttons, set a PIN code, and enable PIN protection.

NOTE:

When Onboard Administrator is operating in FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug, the PIN protection cannot be disabled.

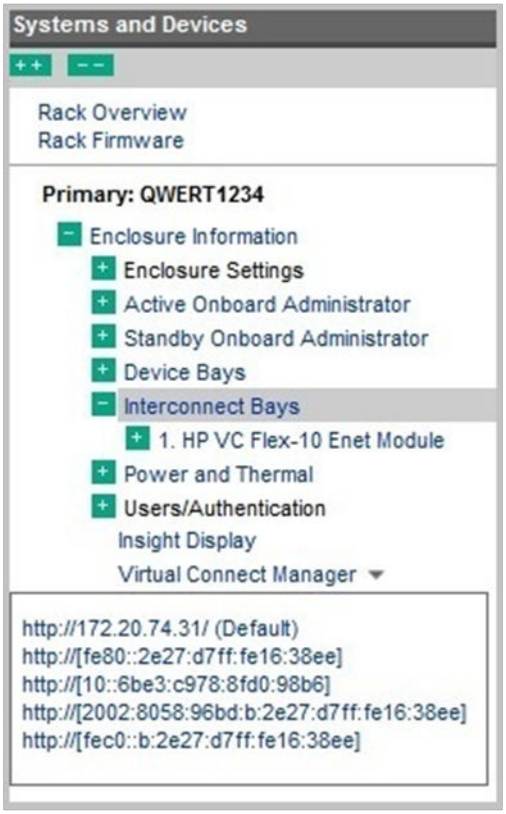
The User Note tab enables note text to be edited.

The Background tab enables a 320x240 px Windows bitmap to be uploaded as the user note background image.

The Chat Mode tab enables an administrator to initiate a chat with a user at the enclosure using the Insight Display.

Virtual Connect Manager

The Virtual Connect Manager link in the tree menu launches the Virtual Connect Manager in a new window. To view available VCM address links (IPv4 and IPv6), click the down arrow alongside the link. When FQDN link support is enabled and certain DNS configuration requirements are met, an FQDN-based address displays as the default, as shown in the following figure. For more information about enabling FQDN link support, see **Network Access**.


Systems and Devices
++
−−
Rack Overview
Rack Firmware
Primary: QWERT1234
Enclosure Information
Enclosure Settings
Active Onboard Administrator
Standby Onboard Administrator
Device Bays
Interconnect Bays
1. HP VC Flex-10 Enet Module
Power and Thermal
Users/Authentication
Insight Display
Virtual Connect Manager
http://172.20.74.31/ (Default)
http://[fe80::2e27:d7ff:fe16:38ee]
http://[10::6be3:c978:8fd0:98b6]
http://[2002:8058:96bd:b:2e27:d7ff:fe16:38ee]
http://[fec0::b:2e27:d7ff:fe16:38ee]

For more information on using the Virtual Connect Manager, see the Virtual Connect Manager User Guide.

iLO Integration

HPE BladeSystem Onboard Administrator integrates with each server blade's iLO and enables for pass-through authentication from Onboard Administrator. Like the CLI, HPE BladeSystem Onboard Administrator only supports a maximum of 4 users connected to the iLO at one time using pass-through authentication. To connect to the server blade iLO port, click the **iLO** link. If the user account is set up on the iLO and matches the user account on the Onboard Administrator, then the user will have access to the iLO GUI which will be displayed in the same screen.

Management network IP dependencies

Onboard Administrators management port allows external clients to connect through Onboard Administrator to iLOs and interconnect management processors that are configured to use Onboard Administrators internal management network.

Onboard Administrator firmware bridges the client traffic to the enclosure from the management port to the internal enclosure management network if the destination IP address is not Onboard Administrator. Onboard Administrator creates a route table entry for each server iLO IP address in an enclosure. This allows Onboard Administrator to conduct IP communications with that iLO. These iLO route table entries enable you to configure each iLO network in a different subnet than Onboard Administrator. Each iLO is configured with a valid gateway on its subnet that is accessible through Onboard Administrators external management port connection. Routers are needed on the network connected to Onboard Administrator management port in order to provide the multiple subnets and gateways on the management network. Use of different subnets to attempt to isolate iLOs and Onboard Administrator management is not complete isolation of those networks.

Using the command line interface

Command line overview

The Onboard Administrator CLI is available from the Onboard Administrator serial port, management port, service port or c3000 KVM Module option and provides access to all Onboard Administrator commands and information.

The CLI user must provide a valid username/password to log into Onboard Administrator. The CLI is available for both local user accounts and LDAP users. Two-factor and CAC Authentication are not available for the CLI.

Access to the Onboard Administrator CLI from either the Onboard Administrator Ethernet management port or service port requires that telnet or SSH protocols are enabled on Onboard Administrator.

Access to the Onboard Administrator CLI from the c3000 KVM Module or Onboard Administrator serial port is always available independent of the telnet or SSH protocol setting.

The Onboard Administrator serial port must be used for Onboard Administrator firmware flash recovery or Administrator lost password recovery.

The Onboard Administrator serial port speed is fixed at 9600, N, 8, 1.

For more information about the Command Line Interface, see the Onboard Administrator Command Line Interface User Guide.

Setting up Onboard Administrator using the CLI

1. Connect to the Onboard Administrator CLI using the serial port, management port, service port, or c3000 KVM Module option.
2. Log in to the Onboard Administrator with the "Administrator" user account and the OA dogtag password.
3. Set Onboard Administrator name: "SET OA NAME 1 <name>".
4. If a redundant Onboard Administrator is present, set the name to: "SET OA NAME 2 <name>".
5. Configure Onboard Administrator IP address
   a. Select whether to use either the OA1/OA2 IP address or Enclosure IP address.
   b. Configure OA1 IP address as static or DHCP. Example for static: "SET IPCONFIG STATIC 1 <ipaddress><netmask>"
6. If a redundant Onboard Administrator is present: "SET IPCONFIG STATIC 2 <ip address> <netmask>".
7. Set Onboard Administrator gateway: "SET OA GATEWAY 1 <ip address>.
8. If a redundant Onboard Administrator is present: "SET OA GATEWAY 2 <ip address>.
9. Set the iLO IP address: "SET EBIPA SERVER <ip address> <netmask>. Allocate each IP address needed (up to 32) consecutive static IP addresses.
10. If a gateway exists on the management network, set the iLO gateway to the IP address: SET EBIPA SERVER GATEWAY <ip address>.
11. Start EBIPA FOR iLO: "ENABLE EBIPA SERVER".
12. Complete the remainder of the settings as required.

    The CLI User Guide indicates the enclosure defaults for each setting.

Configuring c-Class iLO IP addresses

Each c-Class iLO factory default configuration enables DHCP network settings. To use the iLO with a DHCP network, connect the Onboard Administrator management port to a network with a DHCP server and Onboard

Administrator and all iLO management processors and supporting interconnect modules such as Virtual Connect obtain IP addresses from the DHCP server.

To configure each iLO for static IP addresses there are five alternatives. Use Onboard Administrator to setup an IP address for each iLO using EBIPA. This enables iLO to be addressed using TCP/IP so that the network settings can be reconfigured. The client PC must be configured to access these iLO IP addresses temporarily for Alternatives 2-4.

Alternative 1 using EBIPA:

Configuring each iLO with an IP address using EBIPA provides a fixed network configuration including IP address, netmask and gateway that is based on the enclosure bay where the server is installed. The new iLO obtains the IP address for that bay without further configuration needed.

Alternative 2 using the OA GUI:

Log in to the OA GUI with an account having administrator privilege and bay permissions to the corresponding iLO. Select the **iLO** link on the desired server to single-sign-on to the iLO web GUI. Select **Administration | Network Settings.** Change iLO to DHCP disabled and enter the desired IP address, subnet mask and gateway. Select **Apply** and the iLO that has been configured for a static IP address. Repeat these steps for each iLO. When all iLOs in the enclosure have static IP addresses configured, turn off the EBIPA setting for the servers.

Alternative 3 using the OA CLI:

Login to the OA CLI with an account having administrator privilege and bay permissions to the corresponding iLO. Perform the `connect server X` command where X is the bay number containing the iLO to be configured. Use iLO SMASH/CLP interface to set the iLO to the desired IP address subnet mask and gateway. This resets the iLO network settings to the configured values. Repeat these steps for each iLO. When all iLOs in the enclosure have static IP addresses configured, turn off the EBIPA setting for the servers.

Alternative 4 using iLO RIBCL scripts:

Create a unique RIBCL xml script to configure the iLO network settings to the desired values for each iLO. Copy these scripts to an HTTP, FTP, or TFTP server that can be accessed by the Onboard Administrator.

Login to the OA CLI with an account having administrator privilege and bay permissions to the corresponding iLO. Perform the `hponcfg X Y` command where X is the bay number containing the iLO to be configured and Y is the HTTP, FTP, or TFTP server network path to the script file (example hponcfg 2 http://10.128.126.204/Mod_Network_Settings.xml). Using Onboard Administrator to perform the `hponcfg` command uses single-sign-on to the selected iLO, instead of configuring the RIBCL script with the unique default iLO username/password. Application of the RIBCL script resets the iLO network settings to the configured values. Repeat these steps for each iLO. When all iLOs in the enclosure have static IP addresses configured, turn off the EBIPA setting for the servers.

Alternative 5 using the iLO BIOS ROM during server POST:

Connect each server to a KVM. Reboot each server and stop POST during iLO ROM initialization. Change the iLO network configuration and manually enter the IP address, netmask and gateway. Reboot the server. Repeat for each iLO.

Pinout signals for Onboard Administrator Serial RS232 connector

The pinout for the DB9 serial connector (Onboard Administrator Serial RS232 port) used on the c7000 serial port is as follows:

Pin	Name	Direction	Description
1	CD	In	Carrier detect
2	RXD	In	Receive data
3	TXD	Out	Transmit data
4	DTR	Out	Data terminal ready
5	GND		System ground
6	DSR	In	Data set ready
7	RTS	Out	Request to send
8	CTS	In	Clear to send
9	RI	In	Ring indicator

Using the service port connection

The Onboard Administrator service port is the enclosure link-up connector which also has a laptop icon next to the up arrow. When the enclosure link connectors are used to link enclosures, the top enclosure link-up connector will be the Service Port for all the linked enclosures. This port is a 100BaseT Ethernet jack and may be directly connected to a laptop or PC RJ45 Ethernet connector using a standard CAT5 patch cable as the wiring on the link-up connector is crossed over to allow direct connect to a PC 100BaseT connector.

The Service Port provides direct connection to any of the active Onboard Administrator modules in all linked enclosures or just the active Onboard Administrator module in a single enclosure if there are no other linked enclosures. The network connection is private to the enclosures and cannot be used to access any device outside the internal enclosure management network. It can be used to directly access the active Onboard Administrator at the active service IP address, found on that enclosure Insight Display, Enclosure Info screen.

The laptop or PC connected to the enclosure service port must have DHCP enabled its network connection, and obtains a zero-conf IP address in the range 169.254.x.y after a DHCP timeout if the laptop or PC is running windows. If the laptop or PC is running Linux, you might have to manually set the network port to 169.254.2.1 with a netmask of 255.255.0.0.

To access an active Onboard Administrator GUI**—**Use the active OA service IP address from the Insight Display on that enclosure as the web address in your laptop or PC browser. Log into the OA with a configured user account and password.

To access an active Onboard Administrator CLI**—**Use a Telnet or SSH program based on the configured network access settings and connect to the active OA service IP address. Log into the OA with a configured user account and password.

Since none of the configured device bay iLO have an IP address in the zero-conf IP address range, you must manually add a network route on the laptop or PC if you need to access the iLO IP address from the service port. The syntax if using a windows laptop or PC command shell is:

route add iLO_IP_address mask 255.255.255.255 OA_service_IP_address

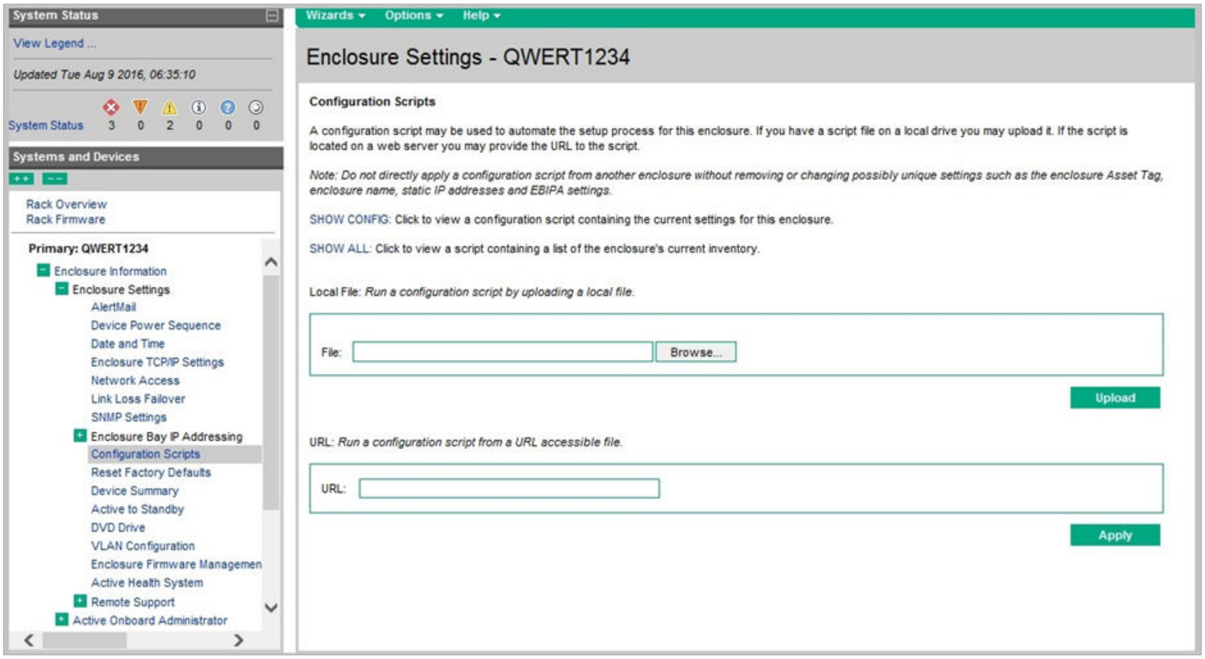
After the route to an iLO has been added to the laptop or PC, the iLO can be accessed from the OA GUI or directly using SSH.

The active Onboard Administrator does not support routing from the service port to an interconnect module management processor. However if the interconnect module supports the serial connection to the OA, then the OA CLI “connect interconnect” command can be used to connect to an interconnect module.

The service port connection is only intended as a temporary Ethernet connection to the enclosure private network to eliminate disconnecting the management port from the external management network for access to the Onboard Administrator during a maintenance event.

Configuration scripts

Use configuration scripts to maintain settings and configuration information, particularly when setting up multiple enclosures and Onboard Administrator modules. This can eliminate the need to configure each enclosure manually. Configuration scripts can be created and used with Onboard Administrator in the browser or through the CLI, executing them in the same manner as a shell script is executed in Linux or UNIX.



Enclosure Settings - QWERT1234

Configuration Scripts

A configuration script may be used to automate the setup process for this enclosure. If you have a script file on a local drive you may upload it. If the script is located on a web server you may provide the URL to the script.

Note: Do not directly apply a configuration script from another enclosure without removing or changing possibly unique settings such as the enclosure Asset Tag, enclosure name, static IP addresses and EBIPA settings.

SHOW CONFIG: Click to view a configuration script containing the current settings for this enclosure.

SHOW ALL: Click to view a script containing a list of the enclosure's current inventory.

Local File: *Run a configuration script by uploading a local file.*

File:

URL: *Run a configuration script from a URL accessible file.*

URL:

Viewing a current configuration

To view a current configuration for the enclosure:

1. Click the **SHOW CONFIG** link. The configuration opens in a new browser window.
2. To save the configuration as a text file, choose one of the following options:
    - If you use Microsoft Internet Explorer, select **Save As**.
    - If you use Mozilla Firefox, select **Save Page As**.
    - If you use Google Chrome, select **Save Link As**.

You can also select a local file or a URL for the configuration script.

- **Local file**—You can browse for the configuration file or you can enter the path of the configuration file into the text box. The maximum number of characters in the file path cannot exceed 256. After entering the configuration file path, click **Upload**.
- **URL**—If the configuration file is located on a web server, enter an HTTP:// path to it. The maximum number of characters in the file path cannot exceed 256. Enter the URL, and then click **Apply**.

For security, the retrieved current configuration does not contain any user passwords. You can manually edit the script to add the user passwords after the user name on the ADD USER lines. Also, the retrieved current configuration does not contain any of the LCD settings (Lock Buttons, Enable PIN Protection, and PIN Code). These settings cannot be added from the configuration script.

Viewing the current enclosure inventory

To view a script of the current enclosure inventory, click the **Show All** link. The current enclosure inventory opens in a new browser window. To save the inventory as a text file, choose either of the following options:

- If you are using Microsoft Internet Explorer, select **Save As**.
- If you are using Mozilla Firefox, select **Save Page As**.
- If you use Google Chrome, select **Save Link As**.

The downloaded text file provides the same information as a CLI `SHOW ALL` command. The text file also displays the current configuration for the enclosure.

NOTE:

The enclosure inventory information in the new browser window might take a few minutes to load. You must wait until the `Variable list` command appears.

USB support

This field appears when a USB key is detected in the Active Onboard Administrator USB port and configuration files are present. To download a configuration file, select a file from the menu, and then click Apply. The maximum supported file size for USB keys formatted with FAT32 is 4GB. For SPP images greater than 4GB, use an ext2-formatted USB key.

To save the current Onboard Administrator configuration file to the USB key, enter a simple file path, either a relative path in the format `path/file` or with a leading dot (.), such as `./path/file`, or an absolute path beginning with a slash (/), in the format `/path/file`. Do not enter a URL. Do not include spaces within the file name. Click **Apply**.

Reset factory defaults

ⓘ **IMPORTANT:**

If the enclosure is in VC mode, you must clear the mode before resetting factory defaults.

Additionally, save your configuration before resetting factory defaults. Click **SHOW CONFIG** to download a script containing your current configuration. You can use this script later to restore settings that are lost after a factory reset.

NOTE:

After a factory reset, the enclosure IPv6 network settings (IPv6, SLAAC, and DHCPv6) are enabled by default.

When you reset the enclosure to the factory defaults, all enclosure settings are reset except the built-in Administrator password. All Alert Mail, Network and Network Protocol, SNMP, and Power Management settings are reset.

To reset all enclosure settings including the Administrator password to the factory defaults, use the Onboard Administrator CLI `SET FACTORY RESTORE_FACTORY_PASSWORD` command.

To reset the enclosure, click **Reset Factory Defaults**. A confirmation screen appears. To confirm resetting the enclosure, click **OK**. To exit without resetting the enclosure to factory defaults, click **Cancel**.

NOTE:

This feature is disabled while in the FIPS Mode ON/DEBUG/Top-Secret/Top-Secret Debug.

To view a current configuration for the enclosure:

1. Click the **SHOW CONFIG** link. The configuration opens in a new browser window.
2. To save the configuration as a text file, choose one of the following options:

- If you use Microsoft Internet Explorer, select **Save As**.
- If you use Mozilla Firefox, select **Save Page As**.
- If you use Google Chrome, select **Save Link As**.

For security, the retrieved current configuration does not contain any user passwords. You can edit the script manually to add the user passwords after the user name on the ADD USER lines. Also, the retrieved current configuration does not contain any of the LCD settings (Lock Buttons, Enable PIN Protection, and PIN Code). These settings cannot be added using the configuration script.

Clearing the VC mode removes all VC settings from the enclosure. Power off all VC-configured servers before clearing the VC mode. If servers are not powered down, they might maintain the VC settings until they are rebooted. You must clear the VC mode before changing to the FIPS Mode OFF/ON/DEBUG/Top-Secret/Top-Secret Debug.

To clear the VC Mode:

1. Click **Clear VC Mode**. A confirmation screen appears, stating `All servers should be powered off and not configured by Virtual Connect prior to clearing VC mode. Are you sure that you wish to clear VC mode?`
2. Click **OK**.

HPE Integrity i2 server blade support

Updated support for HPE Integrity BL860c i2, BL870c i2, and BL890c i2 Server Blades

The Integrity i2 server blades include Blade Link hardware assemblies that conjoin multiple BL860c i2 Server Blades to create dual-blade four-socket and quad-blade eight-socket servers.

Onboard Administrator firmware version 3.00 or later is required to support these server blades.

The Onboard Administrator GUI tree view and graphical view has been updated to support the Integrity i2 server blades. The Port Mapping, Firmware, and Partner Blade screens are also updated.

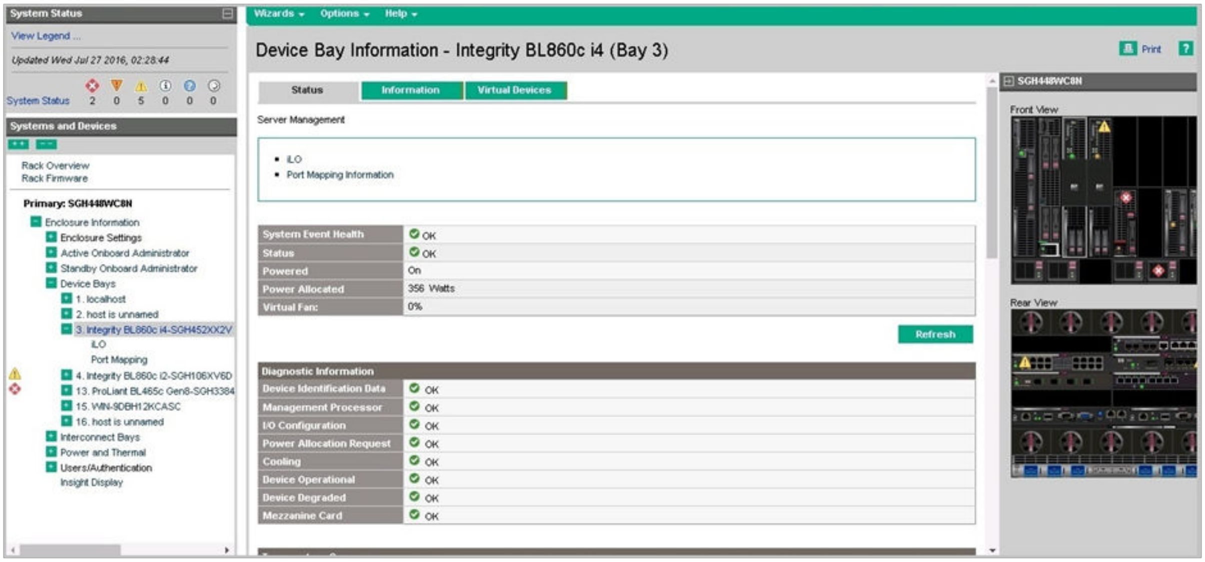
Tree view and graphical view changes for HPE Integrity i2 Server Blades

All Integrity i2 server blades include a Blade Link. The main tree view entry for a conjoined server blade indicates the range of bays containing all the individual server blades that are conjoined.

Selecting the main tree view entry for the conjoined server blade highlights the Blade Link in the graphical view with a solid blue box, and each of the conjoined server blades and associated partner blades are individually highlighted with dotted blue boxes. The Device Bay Information title includes the size of the Blade Link and the range of bays in the conjoined server.

The Device Bay Information Virtual Device tab is only available on the main entry of the tree view for the entire conjoined server blade.

The iLO entry in the tree view is only under the main entry for the entire conjoined server blade.



Device Bay Information - Integrity BL860c i4 (Bay 3)

Server Management

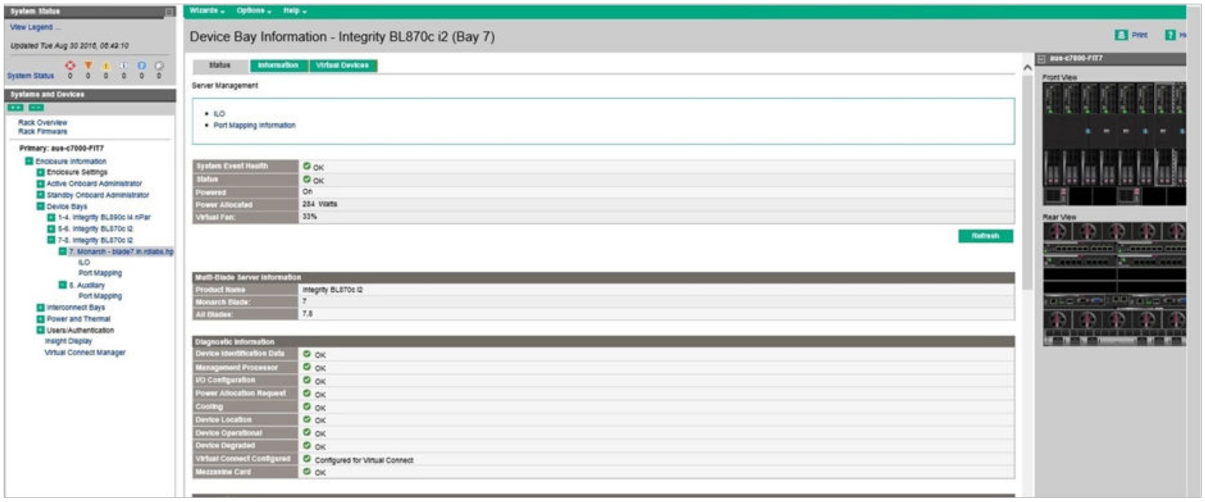
- iLO
- Port Mapping Information

System Event Health	✓ OK
Status	✓ OK
Powered	On
Power Allocated	356 Watts
Virtual Fan:	0%

Diagnostic Information	
Device Identification Data	✓ OK
Management Processor	✓ OK
I/O Configuration	✓ OK
Power Allocation Request	✓ OK
Cooling	✓ OK
Device Operational	✓ OK
Device Degraded	✓ OK
Mezzanine Card	✓ OK

A new item is added to the tree view under the conjoined server blade iLO titled Monarch or Auxiliary based on the role of that server blade in the conjoined server.

Selecting Monarch or Auxiliary navigates to the Device Bay Information page for that particular blade. The selected blade has a solid blue highlight in the graphical view, and the other conjoined server blades and any associated partner blades have dotted blue highlights. The Multi-Blade Server Information table indicates the product name and Monarch bay, and also lists all the server blade bays of the conjoined server.



System Status

View Legend ...

Updated Tue Aug 30 2016, 06:49:10

System Status 0 0 0 0 0 0

Systems and Devices

Rack Overview
Rack Firmware

Primary: aus-c7000-FIT7
- Enclosure Information
  - Enclosure Settings
  - Active Onboard Administrator
  - Standby Onboard Administrator
  - Device Bays
    - 1-4. Integrity BL890c i4 nPar
    - 5-6. Integrity BL870c i2
    - 7-8. Integrity BL870c i2
      - 7. Monarch - blade7.in.rdlabs.hp
        - ILO
        - Port Mapping
      - 8. Auxiliary
        - Port Mapping
  - Interconnect Bays
  - Power and Thermal
  - Users/Authentication
  - Insight Display
  - Virtual Connect Manager

Device Bay Information - Integrity BL870c i2 (Bay 7)

Server Management

- ILO
- Port Mapping Information

System Event Health	OK
Status	OK
Powered	On
Power Allocated	284 Watts
Virtual Fan:	33%

Multi-Blade Server Information	
Product Name	Integrity BL870c i2
Monarch Blade:	7
All Blades:	7,8

Diagnostic Information	
Device Identification Data	OK
Management Processor	OK
I/O Configuration	OK
Power Allocation Request	OK
Cooling	OK
Device Location	OK
Device Operational	OK
Device Degraded	OK
Virtual Connect Configured	Configured for Virtual Connect
Mezzanine Card	OK

Port mapping changes for HPE Integrity i2 Server Blades

Port mapping for conjoined server blades is viewed on each individual server blade selected in the tree view under the Monarch or Auxiliary role for that server blade.

Partner blade changes for HPE Integrity i2 Server Blades

An HPE Integrity i2 conjoined server blade can have a maximum of three partner blades. For more information, see the appropriate *Integrity i2 Server Blade Installation Guide* in the **Hewlett Packard Enterprise Information Library**. (Under **Products and Solutions**, select **HPE BladeSystem**. Under **HPE BladeSystem**, select **Integrity Server Blades**.)

Troubleshooting Onboard Administrator

Onboard Administrator factory default settings

When resetting the Onboard Administrator to factory defaults, the administrator password is not reset to factory default. It remains set to the password that was last specified. In the event that the administrator password must be reset to factory defaults (as included on the tag that shipped with the Onboard Administrator), proceed to the **Recovering the administrator password** section in this guide.

Resetting the Onboard Administrator to factory defaults will also reset any certificates on the Onboard Administrator.

Onboard Administrator error messages

- Soap Response Errors—These are the general errors reported by the gSoap service for validation errors, device failures, and so on. These errors are organized into two categories:
    - User Request errors
    - Onboard Administrator errors
- Soap interface errors—These errors signal internal issues with the gSoap service
- CGI application errors—These errors are reported by individual CGI processes. Each one issues its own set of errors:
    - File upload errors
    - Insight Display screen shot errors

Onboard Administrator errors

1 The submitted user already exists.

2 The submitted user name is not valid.

3 The maximum number of users already exists.

5 The requested user does not exist.

6 The submitted group already exists.

7 Invalid privilege level.

8 Insufficient privileges for the requested operation.

10 The submitted user was already enabled.

11 The submitted user was already disabled.

12 The submitted user already has administrator rights.

13 The submitted user is not an administrator.

14 An error occurred while creating a group entry.

16 Unable to perform the operation. Retry the operation or restart OA. (System Error 16)

17 Unable to perform the operation. Retry the operation or restart OA. (System Error 17)

18 Unable to perform the operation. Retry the operation or restart OA. (System Error 18)

19 The submitted bay is already assigned.

20 The submitted bay is not assigned.

22 The submitted value is already in use.

23 The first character in the submitted value is not valid.

24 The submitted value contains an invalid character.

25 The submitted value is too short.

26 The submitted value is too long.

27 The submitted trap receiver already exists.

28 The maximum number of trap receivers already exists.

29 The maximum number of IP managers already exists.

30 The IP Manager already exists.

31 The submitted bay number is out of range.

32 The submitted IP address is not valid.

33 The submitted value is null.

34 An error occurred while generating an event.

35 An error occurred opening the enclosure system log.

36 The submitted date and/or time value was not formatted correctly.

37 An error occurred while opening the Onboard Administrator's system log.

38 The NMI Dump failed for the submitted blade.

39 Setting the UID for the submitted blade failed.

40 Setting the environment variable for the submitted blade failed.

41 Setting the boot order for the submitted blade failed.

42 Setting the power control for the submitted blade failed.

43 Setting the max power for the submitted bladed failed.

44 Shutting down the submitted blade failed.

45 Clearing the submitted blade failed.

46 Getting blade information for the submitted blade failed.

47 Getting blade status for the submitted blade failed.

48 Getting sensor information for the submitted sensor failed.

49 Setting the submitted rack name failed.

50 Getting power supply information for the submitted power supply failed.

51 Getting power supply status for the submitted power supply failed.

52 Getting power supply measurements for the submitted power supply failed.

53 Setting the Onboard Administrator's UID state failed.

54 Getting the Onboard Administrator's status failed.

55 Getting the Onboard Administrator's information failed.

56 Getting fan information for the submitted fan failed.

57 Rebooting the enclosure failed.

58 Shutting down the enclosure failed.

59 Getting the enclosure information failed.

60 Getting the enclosure names failed.

61 Getting the enclosure status failed.

62 Setting the enclosure name failed.

63 Setting the enclosure asset tag failed.

64 Setting the enclosure time zone failed.

65 Setting the enclosure UID failed.

66 Setting the UID for the submitted interconnect failed.

67 Resetting the submitted interconnect failed.

68 Getting interconnect information for the submitted interconnect failed.

69 Getting interconnect status for the submitted interconnect failed.

70 An error occurred while accessing the connected user for the requested blade.

71 An error occurred while reading the lockfile for the submitted blade.

72 The submitted E-mail address is not valid.

73 Libem is not able to talk to iLO.

74 Downloading the submitted file failed.

75 The certificate could not be verified.

76 Could not save the authorization keys.

77 The SSH key size is not correct.

78 Could not ping the requested url.

79 Could not generate the CSR.

80 Could not generate the SSO

81 Could not read the fingerprint.

82 Could not get SSH key.

83 The field is already enabled.

84 The field is already disabled.

85 The system is already in DHCP mode.

86 The system is currently in static IP mode.

87 Could not clear the system log.

88 Could not restore the factory settings.

89 Could not read the configuration file.

90 Could not write to the configuration file.

92 The submitted url is not valid.

93 Could not update the firmware with the submitted image file.

94 Unable to acquire the rack topology.

95 Invalid domain.

97 Connecting to the blade's iLO failed.

98 Sending the RIBCL command to the requested blade failed.

99 Could not find the requested element in the RIBCL response.

100 Could not find the requested attribute in the RIBCL response.

101 Could not find the starting boundary in the RIBCL response.

102 Could not find the ending boundary in the RIBCL response.

103 Could not determine the IP address of the management processor for the requested blade.

104 Could not locate a Primary NTP server.

105 You must set at least one (1) trusted host before enabling trusted hosts.

107 Could not create the RIBCL request.

108 This error message should be taken from the soap errorText (varies).

118 The management processor auto-login feature is not supported.

119 The maximum number of EBIPA DNS servers has already been reached.

120 The starting IP address and Net Mask must be set before enabling EBIPA.

121 The LDAP group does not exist.

122 The LDAP group already exists.

123 The maximum number of LDAP groups has already been reached.

125 Error getting Insight Display information.

126 Error getting Insight Display status.

127 Error reading the certificate

128 Error setting the time zone.

129 Error installing the certificate.

130 Exceeded the maximum number of SSO certificates.

131 The X509 Certificate is not formatted correctly.

132 SIM station already in trusted list.

133 SIM station name not found.

134 SIM SSO API received a bad parameter.

135 The maximum number of SIM XE stations already configured.

136 The maximum number of EBIPA interconnects DNS servers has been reached.

137 The session could not be created.

138 The session could not be deleted.

139 Not a valid request while running in standby mode.

140 Not a valid request while transitioning to active mode.

141 Not a valid request while running in active mode.

142 The maximum number of LDAP certificates already exist.

143 Could not remove LDAP certificate.

144 You must configure the directory server and at least one search context before enabling LDAP.

145 Could not set the LDAP group description.

146 An error occurred while communicating with the other Onboard Administrator.

147 Unable to perform the operation. Retry the operation or restart OA. (System Error 147)

148 The other Onboard Administrator is not present.

149 No redundant Onboard Administrator found. Cannot failover.

150 The user could not be authenticated.

151 Invalid parameter for setting blade one time boot.

152 Invalid parameter for setting the blade boot priority.

153 A blade boot device can only be listed once.

154 NTP Poll time must be between 60 and 86400 seconds.

155 Could not create new file.

156 Could not write the file to the disk.

157 The submitted image is too big.

158 The submitted image is not a BMP image.

159 The submitted image does not have the appropriate dimensions.

160 Non-standard BMP images are not supported.

161 The specified item was not found.

162 The protocol specified in the URL is not supported.

163 The upload to the specified URL failed.

164 The Onboard Administrator did not fail over.

165 The blade is in a powered off state.

167 The IP manager does not exist.

168 There is no SSH key installed.

169 There was a problem running the configuration script.

170 Missing credentials.

171 Caught the SIGSEGV signal.

173 No trap receivers were specified.

174 There are no SSH keys installed.

175 There was an error attempting to clear the SSH keys.

176 The IP address is already listed.

177 There was an error getting the SSO trust mode.

178 The submitted SSO trust mode is invalid.

179 The certificate cannot be removed because it does not exist.

180 The interconnect tray is not present.

181 The blade is not present.

182 Users cannot remove or disable themselves.

183 Invalid time zone

184 Error setting CLP strings

185 Error getting CLP status

186 Error setting ISMIC info block

187 Error reading ISMIC info block

188 Error clearing blade signature

189 Error setting blade signature

190 Request is valid only for server blades

191 Request is valid only for ProLiant server blades

192 The string entered is not a valid netmask.

193 The string entered is not a valid gateway.

194 The string entered for DNS server 1 is not valid.

195 The string entered for DNS server 2 is not valid.

196 Error trying to remove a nonexistent SSO name

197 Error trying to add an SSO name

198 Invalid SNMP trap community

201 Could not open the event pipe for reading.

202 Did not read the proper size for events.

203 Event length mismatch.

204 The event listener was terminated.

211 Error obtaining blade power reduction status

212 Update the other OA firmware to enable this feature.

213 Dates before 14 June 2006 are not valid.

214 The certificate exceeds the maximum valid size.

215 E-Fuse cannot be reset.

216 Firmware update in progress. Login is disabled.

217 An error occurred while setting the enclosure PDU type.

218 An error occurred while setting the enclosure part number.

219 An error occurred while setting the enclosure serial number.

220 Cannot set time when NTP is enabled.

221 Request is valid only for Itanium/BCS/IPF blades.

222 The Active and Standby Onboard Administrator are not the same hardware build.

223 The firmware installed on an Onboard Administrator module is incompatible with FirmwareSync.

224 Failed to create firmware image

225 The Active and Standby Onboard Administrator have the same firmware version installed.

226 Upgrade an Onboard Administrator to firmware 2.10 or later to enable this feature.

227 The requested user cannot be removed from iLO because it is the only remaining administrator account.

228 The requested user cannot be added to iLO because iLO local accounts have been disabled.

229 The requested user cannot be added to iLO because the maximum number of local accounts already exists.

230 One or more of the specified SNMP traps were not already configured on the Onboard Administrator and cannot be removed.

231 Reset Factory Defaults in progress. Login disabled.

232 The requested operation is not available on c3000 enclosures.

233 This feature requires the iLO Select Pack License or iLO Advanced Pack License on the server blade when LDAP is enabled on the Onboard Administrator.

234 Invalid characters detected.

235 Onboard Administrator is initializing. Login disabled.

236 Cannot retrieve Onboard Administrator media device array.

237 The requested device is not ready.

238 Power off or remove the partner blade.

239 The current firmware does not support this operation.

240 Serial number update requires newer firmware version.

241 The requested device is not present or no firmware upgrade is required.

242 The operation cannot be performed on the requested device.

243 iLO license information cannot be retrieved because iLO XML Reply is disabled.

244 SSH is disabled on this blade.

245 Disconnect the virtual media applet.

246 Invalid SNMP Write Community string

247 Invalid SNMP Read Community string

248 Invalid port number. The LDAP server SSL port can be any number between 1 and 65535.

249 Feb 29 was specified but the year is not a leap year.

250 The CA certificate is invalid.

251 Exceeded the maximum number of CA certificates.

252 No CA certificates are imported.

253 This CA certificate is already imported.

254 A certificate is already mapped to this user.

255 An undocumented error has occurred. Please update your firmware to the latest firmware version if necessary. Contact Hewlett Packard Enterprise if the problem persists.

256 This certificate is already mapped to another user.

257 The user certificate could not be verified.

258 This operation is not permitted when two-factor/CAC Authentication is enabled.

260 This operation cannot be performed when AlertMail is disabled.

261 This operation cannot be performed when the AlertMail settings are not configured.

262 This operation cannot be performed when SNMP is disabled.

263 A certificate must be mapped to Administrator or LDAP must be enabled with a configured groups with administrator privilege to enable certificate based authentication.

265 A certificate is not mapped to this user account.

266 Certificate based authentication is in effect. Please close the CLI/Browser and try login.

267 Two-factor authentication configuration was not changed.

268 An iLO image is already staged.

269 The file was not a proper iLO image for the blade.

270 The crc32 supplied does not match the provided file.

271 Cannot delete the last CA with Certificate based authentication enabled.

272 The Onboard Administrator cannot communicate with iLO.

273 An EBIPA configuration error occurred.

274 Link Loss Failover intervals must be between 30 and 86400 seconds.

275 Network speed must be either 10Mbit or 100Mbit.

276 Network duplex setting must be HALF or FULL.

277 The password does not conform to password rules.

278 Invalid minimum password value

279 A firmware image is already staged.

280 The provided file was not a proper image.

281 Bad image CRC checksum

282 Remote system logging must be enabled to perform this operation.

283 Invalid remote port. The port must be a number between 1 and 65535.

284 The remote syslog server address must be configured before enabling remote system logging.

285 Invalid remote server address

286 This setting is already enabled.

287 This setting is already disabled.

288 Enclosure IP mode was not enabled because the active Onboard Administrator does not have a static IPv4 address.

289 This feature is not available for this Onboard Administrator.

290 Request to enable DHCP addressing on the active Onboard Administrator is denied because Enclosure IP Mode is enabled.

291 The value provided is not proper base64.

292 The firmware image provided is an older version than the current firmware. Onboard Administrator settings cannot be preserved.

293 The file provided is not a valid Onboard Administrator firmware image.

294 There are no USB keys connected to the enclosure.

295 No valid firmware images found on USB key

296 No configuration scripts found on USB key

297 I/O error on USB key

298 Badly formatted USB file URL

299 Permission problems when accessing USB media

300 Error uploading to USB media

301 An invalid number of GUIDs was passed to the Onboard Administrator.

302 URL flash image for microcode download not available

303 Invalid session timeout

304 Invalid watts value

305 Failed to store change for power cap

306 Enclosure Dynamic Power Cap feature is not allowed.

307 Wrong number of bays specified for enclosure while setting capping bays to exclude.

308 The number of bays opted out exceeds the maximum allowed.

309 Enclosure Dynamic Power Cap feature is not allowed.

310 Enclosure Dynamic Power Cap is set.

311 Enclosure Dynamic Power Cap is not set. Cannot confirm that device tray meets minimum firmware version required.

312 Enclosure Dynamic Power Cap not set. Device tray fails to meet the minimum required firmware version.

313 The requested cap is outside the allowable range of Enclosure Dynamic Power Cap values.

314 Server Power Reduction cannot currently be enabled. Enclosure Dynamic Power Cap is not allowed.

315 No valid ISO images found on USB key

316 Bay privileges cannot be revoked for Administrators with OA permission.

317 Invalid DNS hostname

318 Factory defaults cannot be restored because the enclosure is in VC mode.

319 The string entered is not a valid IPv6 address.

320 IPv6 static address already exists

321 IPv6 static address not found

322 Unable to add

323 Invalid SMTP server

324 Invalid SNMP Trap receiver

325 Invalid NTP server

326 Invalid EBIPA configuration. Multiple subnets were detected.

327 Specified VLAN ID does not exist.

328 Cannot delete the default VLAN ID

329 Maximum VLAN entries reached

330 Duplicated VLAN ID

331 Specified VLAN ID is invalid.

332 Operation partially successful

333 Duplicated VLAN name

334 A pending command already exists.

337 The remote syslog server address cannot be cleared while remote logging is enabled.

338 Invalid search context number

339 Not on the same VLAN ID domain

340 This command is not valid for auxiliary blades.

341 No LDAP groups currently exist.

342 The requested Derated Circuit Capacity is outside the allowable range of values for this enclosure.

343 The requested Rated Circuit Capacity is outside the allowable range of values for this enclosure.

344 The requested cap is greater than the requested Derated Circuit Capacity.

345 The requested Derated Circuit Capacity is greater than the requested Rated Circuit Capacity.

346 The requested set of bays to exclude cause the cap to be outside the allowable range.

347 The requested set of bays to exclude cause the Derated Circuit Capacity to be outside the allowable range.

348 The requested set of bays to exclude cause the Rated Circuit Capacity to be outside the allowable range.

353 IPv6 is currently disabled. Cannot download certificate from the specified address.

354 The date cannot be set to a date in the past.

356 The setting cannot be cleared while LDAP is enabled.

357 URB reporting using HTTP(S) cannot be enabled until an HTTP(S) endpoint has been configured.

358 URB reporting using SMTP cannot be enabled until an SMTP server and mailbox have been configured.

359 URB reporting using SMTP and HTTP(S) cannot be enabled until HTTP(S) and SMTP settings have been configured.

360 Warning: Not all VC-Enet modules are on the same VLAN ID.

361 File doesn't exist.

362 This operation cannot be performed when AlertMail is enabled.

363 Setting SolutionsId failed

364 SolutionsId must be an 8-byte hex string, between 0000000000000000 and FFFFFFFFFFFFFFFF.

365 Failed Remote Support registration

366 Failed Remote Support un-registration

367 Failed Remote Support restore registration

368 Failed to send Remote Support message (Hint: Check the Remote Support proxy and endpoint URL. Use SET REMOTE_SUPPORT PROXY to configure and re-try.)

369 Failed to set Remote Support interval. Valid interval is 0 to 60 (days)

370 You must configure the directory server and SSL port before testing LDAP.

371 The string contains an invalid character.

372 This operation cannot be performed when Remote Support is disabled.

373 Cannot set Maintenance Mode Timeout. Value should be between 5 minutes and 2 weeks.

374 Insert eRs error here.

375 The string entered is not a valid LDAP server. A LDAP server must be a IP address or DNS name.

376 Unable to perform the operation. Retry the operation or restart OA. (System Error 376)

377 The HP Passport credentials provided are invalid.

378 This system is already registered.

379 Please disable Remote Support before performing this action.

380 Transaction UUID is mismatched.

381 Unable to download ilo flash image from the url provided. Supported protocols are http, https, tftp and ftp.

382 The Onboard Administrator is still initializing. Please try your request again later.

383 Failed to send Remote Support message. Please make sure DNS is enabled and verify Insight Remote Support host and port information.

384 Failed to resolve Insight Remote Support hosting server. Please verify DNS settings and Insight Remote Support host and port information.

385 Transmission to the Insight Remote Support receiver was unsuccessful. Please check connectivity between the OA and the Insight Remote Support receiver.

389 This action cannot be performed when FIPS Mode is enabled.

391 No Variable Name-Value pairs are provided for substitution.

392 Attempted to substitute more than 25 variables.

395 Trying to substitute the same variable twice.

396 String_list searchFlag out of range.

397 No variable names are passed in for searching.

398 No variable values are passed in for searching.

401 Enclosure Firmware Management is currently disabled.

402 The Enclosure Firmware Management ISO URL is not set.

403 The operation cannot be performed while Enclosure Firmware Management is running.

404 Unable to mount ISO or validate version information.

Check URL and validate ISO is available from URL entered.

405 Unable to open firmware log.

406 The blade's firmware has not been discovered.

407 An error occurred while reading the firmware log.

408 Enclosure Firmware Management is not supported by this device type

409 Firmware ISO image is in use, changing url is not allowed.

410 Blade must be powered off before starting Enclosure Firmware Management.

411 Unable to change passwords for any LDAP or SIM users.

412 Enclosure Firmware Management is not available. To use this feature, it needs to be unlocked.

413 Enclosure Firmware Management is not supported on the Active OA hardware present.

414 Could not persist firmware management log.

415 When FIPS Mode is enabled, the password length must be between 8 and 40 characters.

416 When FIPS Mode is enabled, strict passwords must be enabled.

417 Certificate hash algorithm is not supported. See OA syslog for more information.

418 The firmware image provided has an older version than the current firmware. This operation is not supported with FIPS Mode enabled. Set FIPS Mode to OFF and retry the operation using the force downgrade option.

419 Could not persist firmware management log.

427 E-Keying busy.

428 Error getting CLP strings.

431 Enclosure Firmware Management is not ready, please try again in a few minutes.

434 PIN Protection cannot be disabled in FIPS Mode.

435 Cannot restore the factory defaults while in FIPS Mode.

437 Bad EBIPAv6 device.

438 An EBIPAv6 configuration error occurred. Extended information is available as a bitcode reason code.

439 Invalid hash algorithm. The hash algorithm must be one of: SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. Only SHA-384 is allowed in FIPS Top Secret Mode.

440 You must set a new pin code before unlocking the LCD buttons.

441 The requested operation cannot be completed during a firmware update.

442 This enclosure is incapable of performing a reset on a non-redundant Onboard Administrator.

444 Power cap configuration locked due to active group management.

REMOTE SUPPORT TIER2

445 HPE Remote Support receiver temporarily unavailable. Please retry later.

446 Unregistration request was not processed successfully by the Remote Support receiver. Remote Support has been disabled locally. No service events or data collections will be sent until this device has been re-registered.

447 Authentication error. Please unregister and re-register device.

448 Missing device identifiers. Please unregister and re-register device.

449 Corrupt device identifiers. Please unregister and re-register device.

450 Insufficient device identifier information. Please unregister and re-register device.

451 Invalid device identifier information. Please unregister and re-register device.

452 Stale device identifiers. Please unregister and re-register device.

453 Missing GDID. Please unregister and re-register device.

454 Corrupt GDID. Please unregister and re-register device.

455 Missing registration token. Please unregister and re-register device.

456 Corrupt registration token. Please unregister and re-register device.

457 Expired registration token. Please unregister and re-register device.

458 Invalid HP Passport credentials. Please verify and enter valid HP Passport account credentials.

459 Device is already registered. Please delete the device from Insight Remote Support user interface and retry registration.

460 Unknown device. Please unregister and re-register device.

461 Insufficient registration data. Please retry registration.

462 Missing SOAP header. Please retry your last step. If error persists and device is currently registered, unregister and re-register device.

463 Missing GUID. Please retry your last step. If error persists and device is currently registered, unregister and re-register device.

464 Corrupt GUID. Please retry your last step. If error persists and device is currently registered, unregister and re-register device.

465 Missing data package. Please retry your last step. If error persists and device is currently registered, unregister and re-register device.

466 Data Package validation failed. Please retry your last step. If error persists and device is currently registered, unregister and re-register device.

467 HP Passport password must be changed or reset. Please attempt to register again after correcting the HP Passport account issue.

468 Expired HP Passport credentials. Please attempt to register again after correcting the HP Passport account issue.

469 HP Passport account locked out. Please attempt to register again after correcting the HP Passport account issue.

470 GDID and device identifiers do not match. If error persists and device is not currently registered, unregister and re-register device.

471 Device is not registered. Remote Support registration has been disabled locally on this device. No service events or data collections will be sent until this device has been re-registered.

472 Deleted device. This device has been previously deleted from the Insight Remote Support user interface. Please unregister and re-register device.

473 Unhandled Error.

474 Failed to connect to Insight Remote Support direct connect web service. Please verify DNS settings, proxy settings and connectivity.

475 Dynamic DNS is not enabled.

476 Invalid SNMP Engine ID. The Engine ID must start with '0x' followed by an even number of up to 64 hexadecimal digits.

477 Invalid Authentication Protocol.

478 Invalid Authentication Password, must contain 8 to 40 printable characters.

479 Invalid Privacy Protocol.

480 Invalid Privacy Password, must contain 8 to 40 printable characters.

481 Duplicate user, a SNMP user by this name and engine id already exists.

482 Invalid minimal security setting.

483 Invalid security setting.

484 Selected algorithm cannot be used while FIPS Mode is enabled.

485 A user with read-write access cannot be created while FIPS Mode is enabled.

486 You cannot use a remote engine id with a trap.

487 You cannot use the local engine id with an inform.

489 Error adding the language pack.

490 Error removing the language pack.

491 The file provided is not a valid Onboard Administrator language pack image.

492 Cannot remove the English language pack.

493 The language support pack is not installed.

494 The submitted file is not a valid SSH key.

499 The firmware image provided doesn't meet the VC Minimum Firmware Version requirement. Check the OA Syslog for more details.

500 The action did not complete successfully.

502 Invalid response. No connection or network busy.

503 Web server busy or in service.

510 Remote Support services are provided by other solution.

511 DHCP-Supplied Domain Name cannot be disabled when the user-supplied domain name is not set.

512 The text must contain at least one visible character.

514 User ID is a required field. Please retry registration.

515 The user must have an active authenticated session. Please retry registration.

516 HP Passport system failure occurred. A problem has been detected in the HP Passport system. Please retry later.

517 The session token is invalid due to any of the following reasons: failed decoding, token is null or empty, userId is empty or session start value is not a number. Please retry registration.

518 Password is required. Please retry registration.

519 HP Passport user ID is invalid. Please retry registration with a valid user ID.

520 HP Passport account is locked out due to excessive login authentication failures. Please reset your password and retry registration.

521 User has reached half the maximum allowed HP Passport login authentication failures. Please verify your username and password are correct and retry registration.

522 HP Passport password has expired. Please update your password and retry registration.

523 User has at least one of the HP Passport required on-line identity elements missing. Please update your HP Passport profile and retry registration.

524 HP Passport Security Q and A is not compliant; the user must enter a new security Q and A upon login. Please update your HP Passport security Q and A and retry registration.

525 HP Passport password entered is incorrect. Please retry registration using the correct password.

526 HP Passport user has been added to a group. Please reset your password and retry registration.

527 User must enter an HP Passport security Q and A and change password. Please update your security Q and A, update your password, and retry registration.

528 Protocol error occurred while communicating with the Insight Remote Support receiver.

529 Failed to resolve proxy. Please verify DNS settings, proxy settings and connectivity.

530 Failed to connect to the Insight Remote Support hosting server. Please verify Insight Remote Support host and port information.

531 Failed to connect to the Insight Remote Support direct connect web service. Please verify DNS settings, proxy settings and connectivity.

532 HPE Remote Support receiver protocol error.

533 The setting cannot be cleared when user domain name is enabled.

534 The operation cannot be performed while Enclosure Firmware Management is enabled.

535 Invalid SNMP Engine ID string. The Engine ID string must contain 1 to 27 printable characters.

536 The password is too short.

537 The password is too long.

538 Error installing the certificate.

539 Enclosure IP mode requires the active Onboard Administrator to have a static IPv4 address or a static IPv6 address. If IPv6 is not enabled, only the static IPv4 address can be used.

540 Configure a static IPv6 address for your active OA or disable Enclosure IP Mode before enabling DHCP for IPv4.

541 Configure a static IPv4 address for your active OA or disable Enclosure IP Mode before disabling IPv6.

542 The submitted URL is invalid for uploading.

543 This version of Onboard Administrator firmware does not support boot options for servers configured in UEFI Boot mode.

544 This operation cannot be performed while Secure Boot is enabled.

545 This operation cannot be performed while Secure Boot is enabled or blade is booting the OS.

561 Transmission from the Insight Remote Support receiver was unsuccessful.

562 Transmission from the Insight Remote Support receiver was unsuccessful. Please check connectivity between OA and the Insight Remote Support receiver.

563 The key strength for the provided key is invalid for this configuration.

564 This command is not supported by the interconnect.

565 The string entered is a link-local address and cannot be used for assignment.

566 Invalid IPv6 static route gateway. Route gateway must not be empty and must not contain prefix length.

567 IPv6 static route destination already exists.

568 Unable to add IPv6 route. The maximum number of IPV6 static routes already exist.

569 IPv6 static route not found.

570 Invalid IPv6 static route destination. The route destination must be a valid IPv6 address.

571 All items cannot be disabled.

572 This action requires the OA to have FIPS Mode enabled.

573 Must set MINRATE option if using timeout range.

574 Minimum data rate must be larger than 0.

575 Maximum timeout must be larger than minimum timeout.

576 Timeout must be larger than 0.

577 HTTP Read Timeout is already set to the requested value.

579 CAC Authentication configuration was not changed.

580 CAC Authentication cannot be enabled while TFA authentication is enabled.

582 This operation is not allowed while certificate based Authentication is in effect.

583 LDAP Service account details cannot be empty when Service account is enabled

Insight Display screen shot errors

1 Missing credentials.

2 The getLCDImage CGI process has caught the SIGSEGV signal.

3 Could not acquire access to the image in a reasonable amount of time.

4 Cannot open semaphores.

5 Produce SEMV does not work.

6 Consume SEMV does not work.

7 Cannot lock the image file.

8 Cannot open the image file.

9 Cannot seek in the image file.

10 Unable to resume session.

11 Insufficient privileges.

Onboard Administrator SNMP traps

The BladeSystem Onboard Administrator supports the following SNMP traps.

Trap ID	Trap name	Description
22001	cpqRackNameChanged	Rack Name has changed
22002	cpqRackEnclosureNameChanged	Enclosure Name has changed
22003	cpqRackEnclosureRemoved	Linked Enclosure removal detected

Table Continued

Trap ID	Trap name	Description
22004	cpqRackEnclosureInserted	Linked Enclosure insertion detected
22008	cpqRackEnclosureFanFailed	Enclosure fan has failed
22009	cpqRackEnclosureFanDegraded	Enclosure fan is degraded
22010	cpqRackEnclosureFanOk	Enclosure fan is OK
22011	cpqRackEnclosureFanRemoved	Enclosure fan is removed
22012	cpqRackEnclosureFanInserted	Enclosure fan is inserted
22013	cpqRackPowerSupplyFailed	Enclosure power supply has failed
22014	cpqRackPowerSupplyDegraded	Enclosure power supply is degraded
22015	cpqRackPowerSupplyOk	Enclosure power supply is OK
22016	cpqRackPowerSupplyRemoved	Enclosure power supply is removed
22017	cpqRackPowerSupplyInserted	Enclosure power supply is inserted
22018	cpqRackPowerSubsystemNotRedundant	Enclosure power subsystem is not redundant
22019	cpqRackPowerSubsystemLineVoltageProblem	Enclosure power subsystem line voltage problem
22020	cpqRackPowerSubsystemOverloadCondition	Enclosure power subsystem overload condition
22028	cpqRackServerBladeRemoved	Blade removed (replaced by 22050 in OA v1.30)
22029	cpqRackServerBladeInserted	Blade inserted (replaced by 22051 in OA v1.30)
22037	cpqRackEnclosureManagerDegraded	Onboard Administrator degraded
22038	cpqRackEnclosureManagerOk	Onboard Administrator OK
22039	cpqRackEnclosureManagerRemoved	Onboard Administrator removed
22040	cpqRackEnclosureManagerInserted	Onboard Administrator inserted
22041	cpqRackManagerPrimaryRole	Onboard Administrator is Active
22042	cpqRackServerBladeEKeyingFailed	Blade eKeying config failed
22044	cpqRackNetConnectorRemoved	Interconnect removed
22045	cpqRackNetConnectorInserted	Interconnect inserted
22046	cpqRackNetConnectorFailed	Interconnect failed
22047	cpqRackNetConnectorDegraded	Interconnect degraded
22048	cpqRackNetConnectorOk	Interconnect OK
22049	cpqRackServerBladeToLowPower	Blade requested too low power
22050	cpqRackServerBladeRemoved2	Blade removed2
22051	cpqRackServerBladeInserted2	Blade inserted2

Table Continued

Trap ID	Trap name	Description
22083	cpqRackEnclosureManagerLinkDown	Standby Onboard Administrator network link down
22084	cpqRackEnclosureManagerLinkUp	Standby Onboard Administrator network link up
22085	cpqRackErsCommFailure	Onboard Administrator to remote support communication failure
22086	cpqRackPowerSubsystemOverloadConditionRepaired	Enclosure power subsystem overload condition was repaired

Known browser issues

- **General problems accessing applications from links provided by the Onboard Administrator GUI**

  For a management application to work properly when accessed from an Onboard Administrator link, you might have to add the Onboard Administrator domain to your trusted sites. In addition, note that the management applications opened by the links might not support the same browser versions supported by the Onboard Administrator.

- **Connections to the Onboard Administrator fail via Internet Explorer and Windows 2003 Active Directory**

  The OA 4.30 no longer supports several cipher suites due to the generally acknowledged weakness of the associated encryption algorithms. To connect successfully to the Onboard Administrator, clients must support one or more of the cipher suites listed in the following table. Attempts to connect via Internet Explorer and Windows 2003 Active Directory will fail because this version of Windows lacks default support for at least one of the supported cipher suites. You can add the necessary support by installing and enabling AES-based cipher suites in Windows 2003. Refer to the Microsoft hotfix available at the **Microsoft Support website**.

SSL/TLS cipher suites	Standard names for SSL/TLS cipher suites
EDH-RSA-DES-CBC3-SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
DHE-RSA-AES128-SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
DHE-RSA-AES256-SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256

- **Mozilla Firefox 3.6 (or above) issues**

  If you are using Mozilla Firefox 3.6 or above, pressing the ESC key disconnects any open XMLHttpRequest connections, resulting in unexpected client behavior. For more information, see the **Mozilla article**.

- **Browser issues on operating systems released prior to 2004**

  Browsers on operating systems released prior to 2004 that do not have the latest security related patches and updates applied might not be able to connect to the Onboard Administrator web interface. Onboard Administrator 3.70 changed the default certificate hash algorithm from SHA1 to SHA256. SHA256 support was not generally available until after 2003. Ensure that the following minimum requirements for each operating system are met to support SHA256:

  - Windows XP requires SP3.
  - Windows 2003 Server SP2 requires an update to support SHA256. For more information see, the **Microsoft Support website**.
  - Red Hat 4 was originally shipped with OpenSSL 0.9.7, which does not support SHA256. Update the operating system with the appropriate RPM to use OpenSSL 0.9.8 or later.

- **Certain browsers are unable to access Onboard Administrator if the Onboard Administrator certificate is generated using SHA-224 as SSL hash signature**

  - OA 3.70 and later allows the hash signature algorithm to be changed. If a SHA1 certificate is needed in your network infrastructure, use the Onboard Administrator `GENERATE KEY` command to change the key size and hash algorithm.

    NOTE:

    When running on a Windows platform, certain browsers (such as Microsoft Internet Explorer and Google Chrome) might not be able to access the web interface of the Onboard Administrator (version 3.70 or later) if the Onboard Administrator certificate was generated using SHA-224 as SSL hash signature. SHA-224 is not the default hash function for Onboard Administrator self-signed certificates. By default, the Onboard Administrator uses SHA-256 hashing for self-signed certificates.

    The Mozilla Firefox browser is able to access the web interface of these versions of the Onboard Administrator with a certificate generated using SHA-224 as SSL hash signature.

  - Unable to access OA using browsers like Internet Explorer and Google Chrome when keys generated using SSL and hash algorithm SHA-224 from OA version 3.70 to 4.50.

    NOTE:

    Microsoft Internet Explorer, Google Chrome and Safari browsers may not be able to access the Onboard Administrator web interface if the Onboard Administrator certificate is generated using SHA-224 as SSL hash signature when running on Windows XP, Windows Vista and Windows 7. SHA-224 is not the default hash function for Onboard Administrator self-signed certificates.

- **Some browsers do not support %scope_id" notation with an IPv6 link local address: certain Onboard Administrator features are lost when the address is used**

  Some browsers do not support the "%scope_id" notation with an IPv6 link local address. Certain browsers might accept a web address using this notation, but certain features might be lost when the address is used for accessing the Onboard Administrator. The Onboard Administrator GUI features effected include Insight Display and the **Configuration Scripts** screen configuration gathering (**SHOW CONFIG**) and **SHOW ALL** features.

- **Google Chrome v27.0.1453.94 does not function properly with Onboard Administrator 4.01**

  Chrome stops loading images. Other content such as scripts load successfully. For more details, see the **Google issue report**.

- **Google Chrome v43.0.2357.10 to v44.0.2383 does not function properly with Onboard Administrator**

  If the user tries to log in from any of these Chrome versions, login is allowed but the OA GUI does not display information or take input from user. For more details, see the **Google issue report**.

- **Firefox version - "31.6.0" does not function properly with Onboard Administrator**

  If the user tries to log in using this Firefox version, login shows error when Onboard Administrator is operating in FIPS Top-Secret mode: ssl_error_protocol_version_alert: Peer reports incompatible or unsupported protocol version.

Known network issues

With Emulex firmware prior to version 4.1.450.7, DCC is unavailable with a 10Gb physical link

An issue exists with the Emulex firmware prior to version 4.1.450.7 that can result in the DCC being unavailable with a 10Gb physical link. When this issue exists for full height G7 and Gen8 server blades (including the ProLiant BL680 G7, BL685c G7, BL620 G7, and BL660 Gen8) with HPE NC55x LOMs or FLB554 FlexibleLOMs configured in a Virtual Connect environment, a loss of network connectivity might occur when updating the OA firmware from version 3.56 or earlier to version 3.60 or later.

To prevent loss of network connectivity during the Onboard Administrator firmware update, prior to performing the update ensure that network adapter firmware is updated to correct the DCC unavailable condition, as recommended in the **Customer Advisory c03600027**. For more information, refer to this Customer Advisory.

Miscellaneous known issues

- **CLI access denied using an SSH key**

  Upon attempting to log in to the Onboard Administrator CLI using an SSH key, access might be denied, in which case you are prompted for a password. This problem might occur with FIPS Mode enabled, after updating the Onboard Administrator from version 3.7x to a later version. Some third-party utility tools generate keys smaller than the minimum length allowed by the current version of the Onboard Administrator. Make sure the installed key length is at least 2048 bits in length. For more information about SSH key size requirements (in particular the default SSH key type size), see the table in "Cryptographic security capabilities and defaults."

- **Inability to reconnect to Onboard Administrator after reboot (Trusted Hosts enabled)**

  With Trusted Hosts enabled, an attempt to reconnect to the Onboard Administrator from a client hosted on an OS that supports RFC 4941 might fail after that OS has rebooted.

  RFC 4941 describes an extension to IPv6 SLAAC that allows for generation of global-scope temporary IPv6 addresses using interface identifiers that change over time. When an OS that supports RFC 4941 (such as Windows 7) reboots or the current address expires, a new temporary IPv6 address is generated. When you access the Onboard Administrator from a client hosted on an OS with RFC 4941 support, after a reboot the connection fails because of the client's new IPv6 address and the resulting mismatch between that address and the IPv6 address configured for the client in the Trusted Addresses list.

  To avoid this issue, either disable generation of global-scope temporary IPv6 addresses in the OS, or reconfigure the Trusted Host IP address with the newly generated client IPv6 address.

- **Certificate generation fails (`Could not generate the CSR` error message)**

  When attempting to generate a certificate from the Active or Standby Onboard Administrator, or using the GENERATE CERTIFICATE command from the CLI, a `Could not generate the CSR` error message results. This occurs when attempting to generate either a self-signed certificate or a certificate-signing request (CSR), and with both mandatory and optional information provided.

  This problem might have occurred because the optional Alternative Name was specified incorrectly. The Alternative Name must be 0 to 511 characters in length, and if not 0, it must contain a list of keyword:value pairs separated by commas. The valid keyword:value entries include IP:<ip address> and DNS:<domain name>.

- **Attempt to add (upload) a CA user certificate fails with verification error**

  An attempt to add a certificate to the **Local Users** > **Administrator** > **Certificate Information tab** ends with the following message:

  ```
  The user certificate could not be verified. Please upload the corresponding CA
  certificate.
  ```

  Reason and workaround: The CA certificate from the CA that issued this user certificate needs to be installed using the Two-Factor Authentication Certificate Upload tab.

- **Limit the number of simultaneous iLO virtual media sessions to avoid timeout and performance issues**

  The c-Class BladeSystem ProLiant and Integrity iLO virtual media performance is limited by the activity and number of simultaneous iLO virtual media sessions and the OA workload. The Onboard Administrator Enclosure DVD and Enclosure Firmware Management features use the iLO virtual media feature and might have similar performance limitations.

  To prevent media timeout issues, Hewlett Packard Enterprise recommends that you limit the number of simultaneous sessions. If timeout issues are experienced during OS installation or firmware updates, reduce the number of virtual media sessions in progress, and restart the operation.
- **Onboard Administrator link to iLO 3 Integrated Remote Console might occasionally fail to launch**

  The OA Link to iLO 3 .NET Integrated Remote Console might occasionally fail to launch. For more information including how to resolve the issue, see the **Customer Advisory c03077476**.
- **Denial-of-service for attempts to connect to the OA web server**

  Attempts to connect to the OA web server are denied due to a denial-of-service attack (such as a Slowloris attack) where a malicious client opens many TCP connections to tie up all available connections. To mitigate the effects of attacks from malicious web server clients, you can use the Onboard Administrator CLI `SET HTTP REQUESTREADTIMEOUT` command. For more information, see the Onboard Administrator Command Line Interface User Guide.
- **EFM discover/update processes fail - unsupported ISO image size**

  The OA only supports SPP ISO images that are less than 4GB in size. If the image is 4GB or greater, EFM functionality fails. The OA CLI `SHOW FIRMWARE MANAGEMENT` command displays ISO URL Status as `Invalid URL`.

  You must create a custom ISO image that excludes components unnecessary to the OA EFM blade firmware update process. For more information, see **Enclosure Firmware Management**.
- **Users/Authentication (LDAP) page (Directory Settings) does not load after an upgrade from certain older versions of the OA**

  After upgrading the OA in FIPS Mode ON/DEBUG from older versions (versions 3.71 to 4.11) to 4.20 or later, the **Users/Authentication** > **Directory Settings** page does not load. The following message is displayed:

  ```
  The key strength for the provided key is invalid for this configuration.
  ```

  This is a result of the stronger security features implemented beginning with OA 4.20. The minimum key length was increased to 2048 bits. The error message indicates that the OA detected LDAP certificates containing non-compliant keys that had been installed on the older version of the OA.

  The OA administrator must remove the non-compliant keys and replace them with keys that are 2048 bits or greater.

Enabling LDAP Directory Services Authentication to Microsoft Active Directory

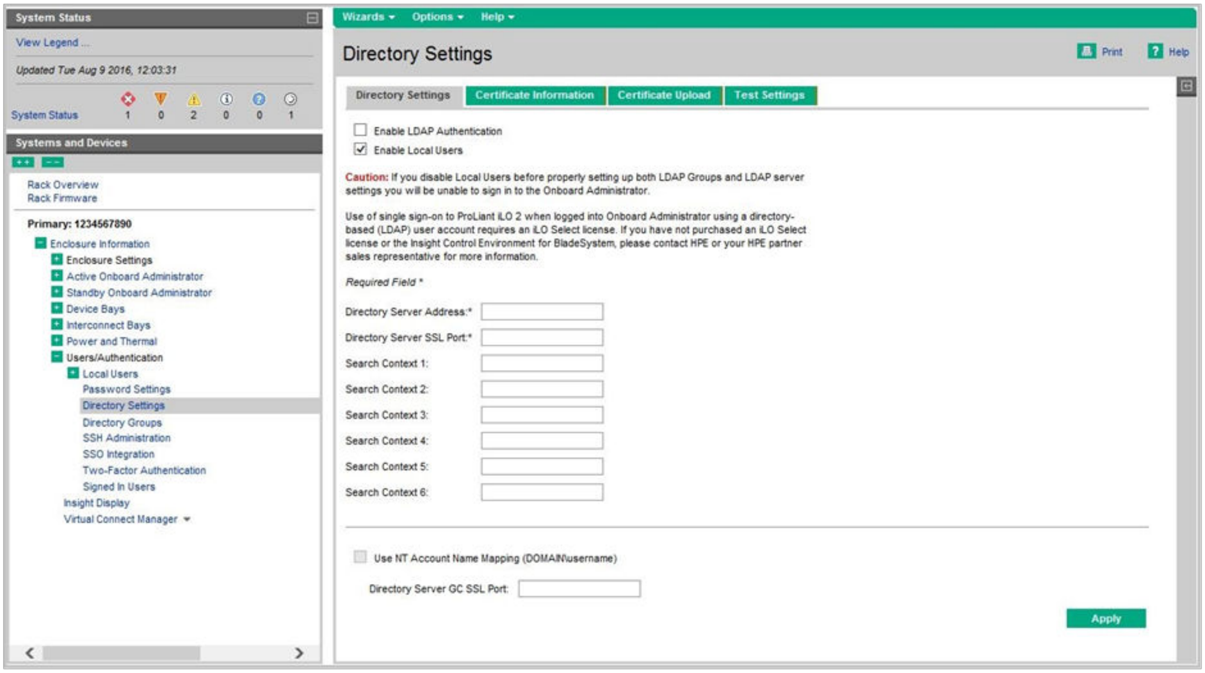
Certificate Services

The Microsoft® implementation of LDAP over SSL requires that the Domain Controllers install DC certificates from the CA of the organization. This process occurs when the Enterprise Root CA service is added to a server in Active Directory. Hewlett Packard Enterprise strongly recommends using an Enterprise Root CA to minimize the complexities of requesting and accepting DC certificates from a stand-alone CA.

NOTE:

The Onboard Administrator LDAP feature supports Microsoft® Active Directory using the `memberOf` attribute. Novell eDirectory is also supported with the `groupMembership` attribute. OpenLDAP is not supported.

Preparing the directory



Directory Settings

□ Enable LDAP Authentication

☑ Enable Local Users

Caution: If you disable Local Users before properly setting up both LDAP Groups and LDAP server settings you will be unable to sign in to the Onboard Administrator.

Use of single sign-on to ProLiant iLO 2 when logged into Onboard Administrator using a directory-based (LDAP) user account requires an iLO Select license. If you have not purchased an iLO Select license or the Insight Control Environment for BladeSystem, please contact HPE or your HPE partner sales representative for more information.

Required Field *

Directory Server Address:*

Directory Server SSL Port:*

Search Context 1:

Search Context 2:

Search Context 3:

Search Context 4:

Search Context 5:

Search Context 6:

□ Use NT Account Name Mapping (DOMAIN\username)

Directory Server GC SSL Port:

To prepare the directory:

1. Create an Active Directory group named OA Admins, and then add a user named TestAdmin in this group.
2. Create a group called OA Operators, and then add a user named TestOperator in this group. User permissions are irrelevant.
3. Navigate to the Directory Settings screen located under Users/ Authentications for the enclosure.
4. Click **Enable LDAP** and then enter the IP address or the name of one of your DCs.

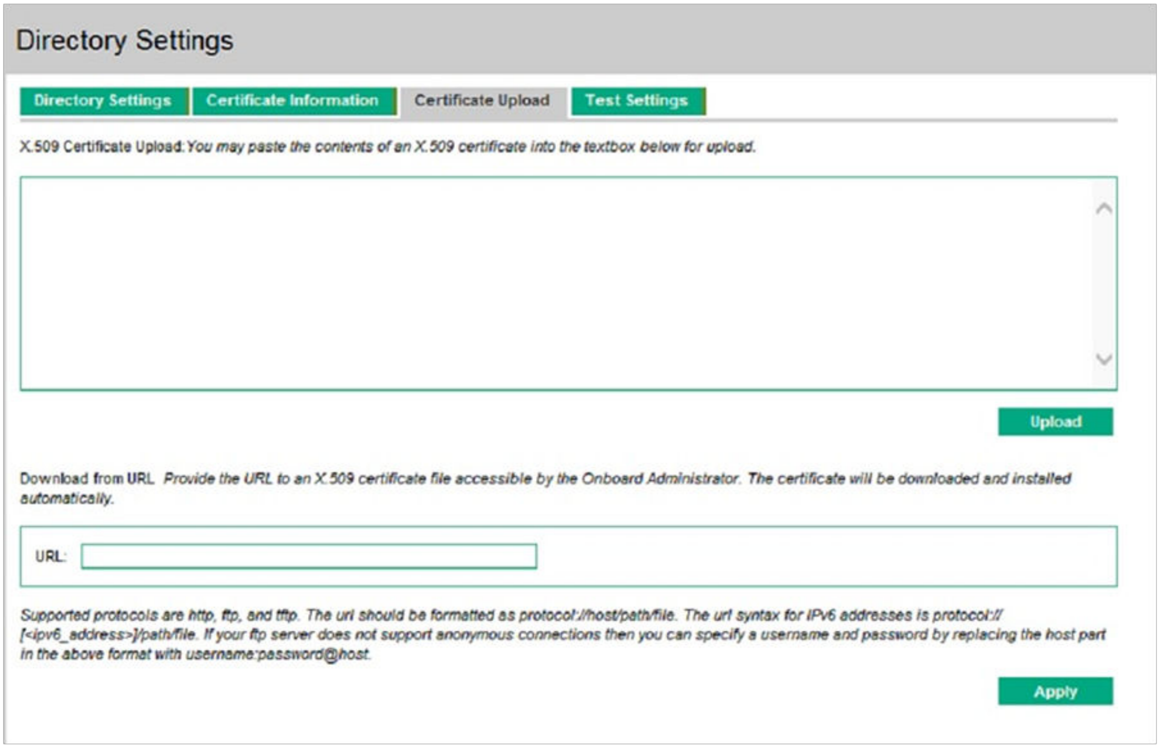
   For more information on verifying that the DC is listening on port 636, see **Troubleshooting LDAP on Onboard Administrator**. Alternatively, to force the DNS servers defined for the domain to offer DCs, enter the domain name of your AD domain (DOMAIN.COM) instead of a server name. For simplicity during initial setup, Hewlett Packard Enterprise recommends using a single IP address. The Search Context is standard LDAP format. For example, if the user accounts are in the Users OU in a domain named BLADEDEMO.HPE.COM, the Search Context is:

CN=Users,DC=bladedemo,DC=hp,DC=com

Uploading the DC Certificate (optional)

You can upload multiple DC certificates. Upload a certificate that permits LDAP over SSL.

1. Click the **Upload Certificate** tab.

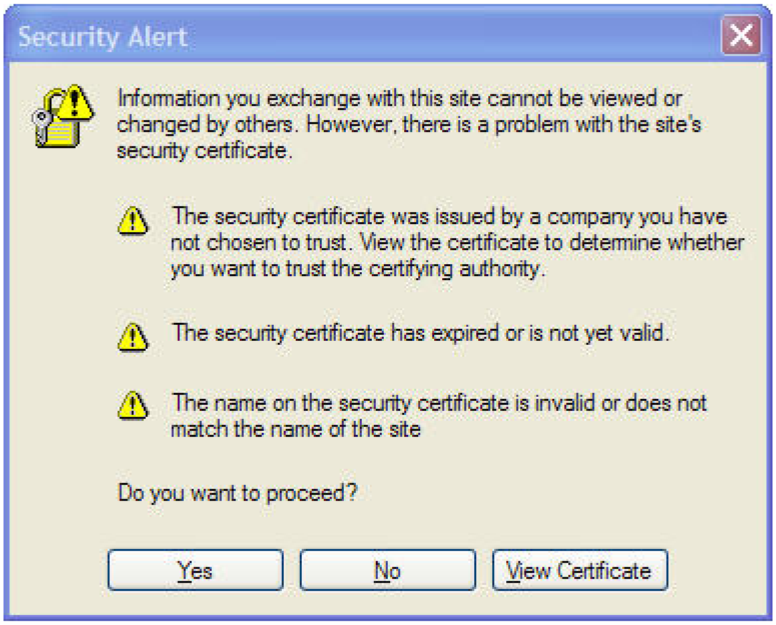


X.509 Certificate Upload: *You may paste the contents of an X.509 certificate into the textbox below for upload.*

Download from URL *Provide the URL to an X.509 certificate file accessible by the Onboard Administrator. The certificate will be downloaded and installed automatically.*

Supported protocols are http, ftp, and tftp. The url should be formatted as protocol://host/path/file. The url syntax for IPv6 addresses is protocol://[<ipv6_address>]/path/file. If your ftp server does not support anonymous connections then you can specify a username and password by replacing the host part in the above format with username:password@host.

2. Obtain the certificate from the DC by opening a new web browser window to https://<domain_controller>:636 (where domain_controller is your DC). This HTTPS URL is secure, so you are prompted to accept a certificate. Click **View Certificate**.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

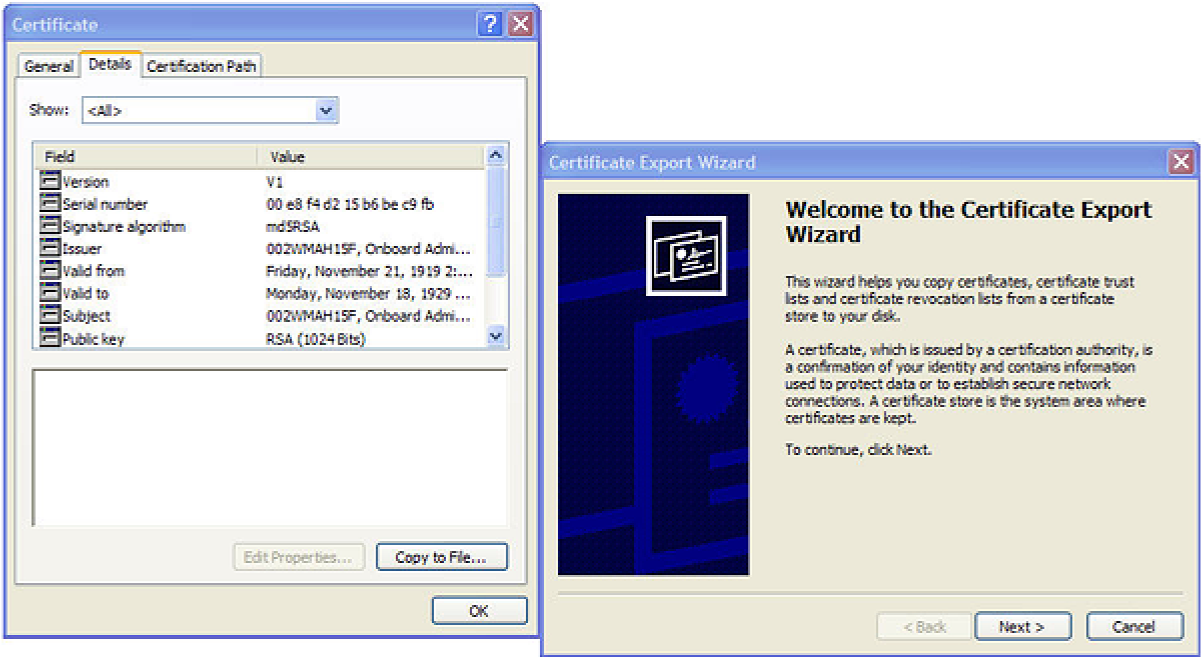
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate has expired or is not yet valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

3. Click the **Details** tab, and then click **Copy to File**.



Show: <All>

Field	Value
Version	V1
Serial number	00 e8 f4 d2 15 b6 be c9 fb
Signature algorithm	md5RSA
Issuer	002WMAH15F, Onboard Admi...
Valid from	Friday, November 21, 1919 2:...
Valid to	Monday, November 18, 1929 ...
Subject	002WMAH15F, Onboard Admi...
Public key	RSA (1024 Bits)

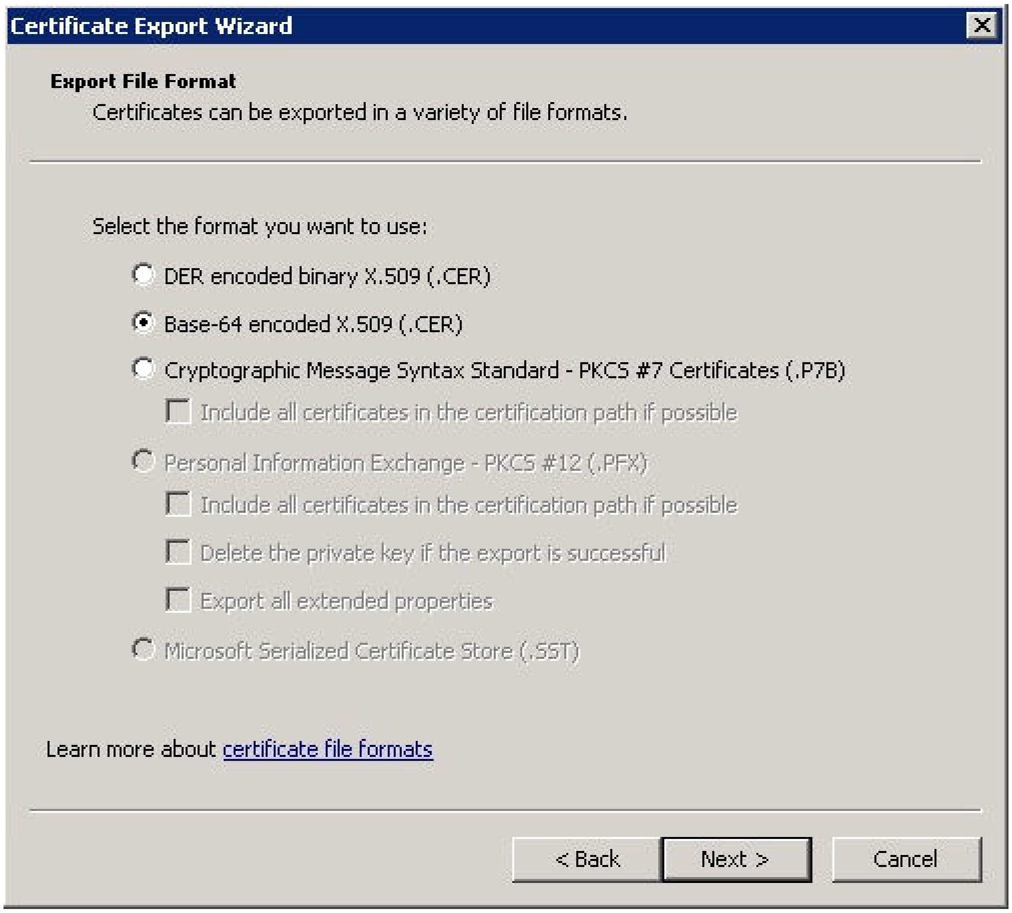
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4. Select **Base-64 encoded x.509 (.CER)** from the list of export options (this is important). Provide a name and location for the file (c:\dccert.cer) and finish the wizard.



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

5. Locate the exported certificate file in explorer and rename it with a .txt extension (dccert.txt). Open the file in notepad and copy the entire contents to the clipboard. The following is an example of the certificate file contents:

```
-----BEGIN CERTIFICATE-----
MIIFxDCCBKygAwIBAgIKJWUSwAAAAAAAAjANBgkqhkiG9w0BAQUFADBVMRMwEQYK
CZImiZPyLGQBGRYDY29tMRIwEAYKCZImiZPyLGQBGRYCaHAxFzAVBgoJkiaJk/Is
ZAEZFgdhdGxkZW1vMREwDwYDVQQDEwh3aW5kb3pDQTAeFw0wNjA4MjIyMDIzMTFa
Fw0wNzA4MjIyMDIzMTFaMCAxHjAcBgNVBAMTFXdpbmRvei5hdGxkZW1vLmhwLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAy4zeh3iXydUAWKVHIDsxLJ6B
aRuVT9ZhkL5NQHIDeRjumsgc/jHSERDmHuyoY/qbF7JMhJ9Lh9QQHUg8QfEYsC1y
qTvgisrZeHtvmrmecvSxZm27b4Bj5XYN0VYcrwqKnH7X/tVhmwqGls7/YZyahNU1
lGB2OjoCq5eJxX+Ybx0CAwEAAaOCA00wggNJMAsGA1UdDwQEAwIFoDBEBgkqhkiG
9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4D
…output truncated…
-----END CERTIFICATE-----
```

6. Return to the OA Upload Certificate screen, paste the certificate contents into the window, and then click **Upload**.

Creating directory groups

Onboard Administrator authenticates users and assigns privileges by first verifying that the user name and password provided to Onboard Administrator match the credentials in the Directory. When a match is verified, Onboard Administrator queries the Directory to discover the names of the Active Directory groups the user is a member of. Onboard Administrator then matches those group names against the Directory Group names that exist in Onboard Administrator. In the following example, Onboard Administrator Directory Groups are created in this step. The group name is used to determine LDAP users' group membership and must match one of the following five properties of a directory group: the name, distinguished name, common name, Display Name, or SAM Account Name.

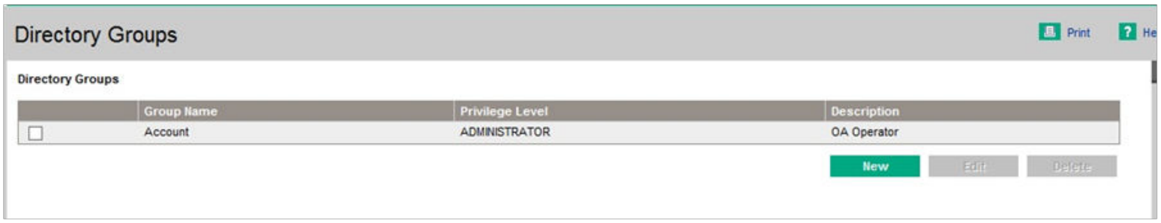
To create a directory group:

1. In Onboard Administrator, navigate to **Users** > **Authentications** > **Directory Groups**.
2. To add a new directory group, click **New**.
3. Create a group named OA Admins, which is the same name created in the Active Directory.

NOTE:

Group names with spaces might not be supported on some LDAP servers.

4. Assign this group full administrative privileges over all server bays and interconnect bays, and then click **Add Group**.

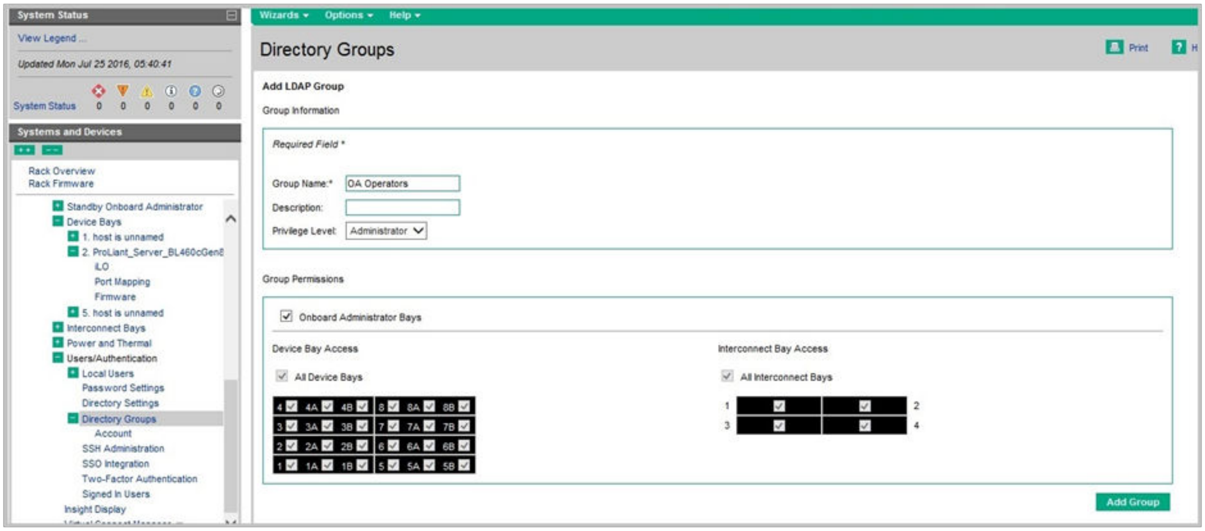


Directory Groups

Directory Groups

	Group Name	Privilege Level	Description
□	Account	ADMINISTRATOR	OA Operator

5. Create a Second Directory Group named OA Operators to match the operator group created in Active Directory. Assign the group Operator privilege level instead of Administrator. Allow access to Interconnect bays, but do not allow the group access to Server Bays. Click **Add**.



Directory Groups

Add LDAP Group

Group Information

Required Field *

Group Name:* OA Operators

Description:

Privilege Level: Administrator

Group Permissions

☑ Onboard Administrator Bays

Device Bay Access

☑ All Device Bays

4 ☑	4A ☑	4B ☑	8 ☑	8A ☑	8B ☑
3 ☑	3A ☑	3B ☑	7 ☑	7A ☑	7B ☑
2 ☑	2A ☑	2B ☑	6 ☑	6A ☑	6B ☑
1 ☑	1A ☑	1B ☑	5 ☑	5A ☑	5B ☑

Interconnect Bay Access

☑ All Interconnect Bays

1	☑	☑	2
3	☑	☑	4

Add Group

If you downgrade Onboard Administrator firmware from 2.40 to 2.31, you lose any groups in addition to the first five groups. Onboard Administrator version 2.40 supports 20 groups, while earlier versions only support five groups.

Testing the directory login solution

1. Log out of the current Onboard Administrator session, and then close all browser windows.
2. Browse to the Onboard Administrator, and then log in using one of the following options:
   - TestAdmin
   - TestAdmin@domain.com
   - DOMAIN\TestAdmin
   - FQDN: cn=<TestAdmin>,cn=<users>dc=<domain>,dc=<com>
3. Enter the corresponding password used for the user account.

   If you cannot log in with full Administrative privileges, see **Troubleshooting LDAP on Onboard Administrator**. Note that you cannot log in using your user name. For example, if your account name is John Brownie and your account is jbrownie, you cannot log in as jbrownie, because this format is not currently supported by LDAP.
4. Log off of Onboard Administrator, and then log in using one of the following options:
   - TestOperator
   - TestOperator@Domain.com
   - DOMAIN\TestOperator
   - FQDN: cn=<TestOperator>,cn=<users>dc=<domain>,dc=<com>
5. Enter the corresponding password used for this account. You have full access to interconnect bays but not to any server blades.

Troubleshooting LDAP on Onboard Administrator

To verify that SSL is working on the Domain Controllers (DC) in your domain, open a browser and then navigate to https://<domain_controller>:636 (substitute your Domain Controller for <domain_controller>). You can substitute <domain> in place of <domain controller> which goes to DNS to verify which Domain Controller is currently answering requests for the domain. Test multiple Domain Controllers to verify that all of them have been issued a certificate. If SSL is operating properly on a Domain Controller (for example, a Certificate has been issued to it), you are prompted by the Security dialog that asks if you want to proceed with accessing the site or view the certificate. If you click Yes, a webpage does not appear. The test is to make the Security Dialog prompt appear. A server not accepting connections on port 636 displays the `page cannot be` `displayed` message. If this test fails, the Domain Controller is not accepting SSL connections possibly because a certificate has not been issued. This process is automatic, but might require a reboot.

To avoid a reboot:

1. On the Domain Controller, load the Computer Account MMC snap-in, and navigate to **Personal** >**Certificates**.
2. Right-click the Certificates folder, and select **Request New Certificate**. The type default is Domain Controller.
3. Click **Next**, and repeat until the Domain Controller issues the certificate.

A second method for troubleshooting SSL is going to the DC and running the following command:

```
C:\netstat -an | find /i "636"
```

If the server is listening for requests on port 636,the following response appears:

TCP 0.0.0.0:636 0.0.0.0:0 LISTENING

A third issue might be that the domain controllers have not auto-enrolled. DCs can take up to 8 hours to auto-enroll and get their certificates issued because MS uses GPO to make the DC's aware of the newly installed CA. You can force this by running DSSTORE -pulse from the DCs (tool is in the w2k reskit). It is triggered by winlogon. Therefore, for auto-enrollment to function, you must log off and then log on again. The certificates appear automatically in the CAs Issued Certs list. Make sure the CA is not listing them in Pending Certs. If it is, change the CA to auto issue certificates when a request comes in. If the auto-enrollment feature still does not function, request the certificate using the following procedure:

1. On the Domain Controller, open MMC, and then add Certificate Snap-in (Computer Account).
2. Navigate to Personal, and then right-click the folder.
3. Click **Request New Cert,** and then click **Next.**
4. Enter a name for the certificate.

If an RPC error occurs, verify that the CA is listed in DNS and that the CA is running.

If the wizard does not start, force the server to see the CA and then allow the wizard to run:

To speed up the GPO process and make the DCs acknowledge the CA, use one of the following commands:

- Windows® 2003, Gpupdate /force
- Windows® 2000, Secedit /refreshpolicy machine_policy /enforce

Verify that the Onboard Administrator has all the appropriate network settings unique to your network (such as DNS) and that the time and date are correct (certificates are date sensitive). Ensure that Onboard Administrator can reach the DNS server (by pinging it from the Onboard Administrator command line interface).

If LDAP is enabled while booting into Lost Password mode, the local Administrator password is reset, LDAP is disabled, and local login is re-enabled.

NOTE:

The Onboard Administrator LDAP feature supports Microsoft® Active Directory using the `memberOf` attribute. Novell eDirectory is also supported with the `groupMembership` attribute. OpenLDAP is not supported.

Creating CAs and configuring Two-Factor Authentication for local user and LDAP group accounts

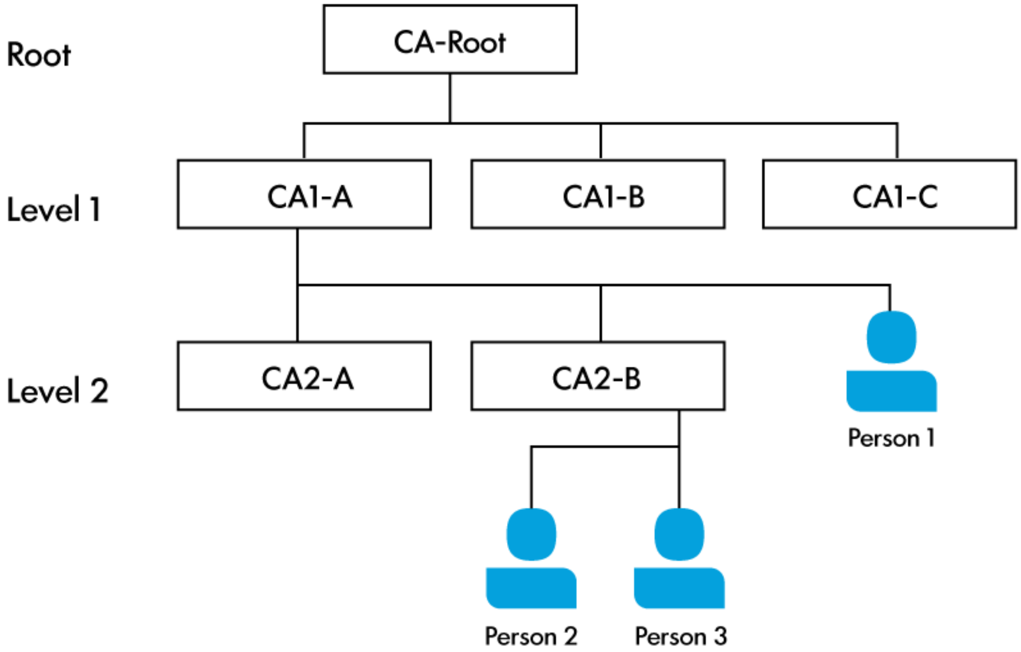
Introduction

Two-Factor Authentication is an optional feature that provides enhanced security for the Onboard Administrator. To permit access to the Onboard Administrator, two-Factor Authentication requires something that a user has (a certificate) and something that a user knows (a password or PIN). The certificate is stored directly in a browser or on the accessing device (as a smartcard, dongle, or TPM).

You can use Two-Factor Authentication with either local user accounts or directory (LDAP) group accounts. For LDAP accounts, you can use the subject or subject alternate name to provide the LDAP login name. In all cases, the user certificate must be validated against a CA.

Two-Factor Authentication public key infrastructure map

CAs are based on a tree structure. Root certificates are self signed. All other certificates can be traced back to the root by following the certificate issuer field. User certificates may be issued by any of the CAs in the tree. The Onboard Administrator has limited storage space and therefore supports storing a maximum of 12 CA certificates. The following diagram shows a tree structure similar to that used in the examples to follow.



CA maps can be very simple or complex. For an example of a complex map, see the **United States Department of Defense public key infrastructure**.

Steps for creating CAs and configuring Two-Factor Authentication with local user and LDAP group accounts

The following sections provide instructions and examples for creating CAs and configuring Two-Factor Authentication with local user and LDAP group accounts. For simplicity, the CA certificates in the provided examples are created on a single system instead of multiple systems. A real CA implementation would use multiple systems.

The following table lists the steps for setting up Two-Factor Authentication with local user and LDAP group accounts, and indicates the section documenting each step plus any subordinate steps.

Step	Section
1	**Configuring the directories** • Create the initial directories for the root CA • Modify and store an OpenSSL configuration file in each CA • Modify the default directories to suit your structure
2	**Creating a root CA** • Copy the OpenSSL configuration file to the root CA • Create the root CA certificate and private key • Create a combined root CA private key and certificate PEM file
3	**Creating subordinate CAs** • Create the directories for the subordinate CAs • Provide x509 certificate information • Generate a CSR and server key for each subordinate CA • Have the root CA sign the CSR
4	**Creating user keys and CSR**s • Create the directories for the user keys and CSRs • Provide x509 certificate information • Generate a CSR and server key for each user • Have the appropriate subordinate CA sign the CSR
5	**Verifying certificates**
6	Storing a user certificate on a smart card or browser
7	**Configuring the Onboard Administrator for Two-Factor Authentication with local accounts** • Establish an Onboard Administrator recovery plan • Configure the Onboard Administrator session timeout • Install the CA chain • Install user certificates on the local Administrator account • Enable Two-Factor Authentication • Log in to the Onboard Administrator using Two-Factor Authentication
8	**Enabling TFA+LDAP authentication**

The following sections also include:

- **Methods for specifying the subject field on a CSR**
- **Troubleshooting TFA and LDAP authentication problems**
- **CLI examples configuring a user account and certificates**
- **Information about CAs and certificates available from the Web**

Configuring the directories

This section describes the setup steps required prior to creating the root CA.

Creating a directory to represent each CA and user

In this tutorial, the following example sets up the initial directories for the root CA. A description of each directory follows. In this and subsequent examples, user input to prompts is indicated by **boldface** type.

NOTE:

This is a tutorial for creating CAs in a simple test environment. In an actual production environment, the CA servers would be on separate servers. In this tutorial example, the CA servers are represented by separate directories on a single server.

```
[~/]$    mkdir -m 0755 ~/examples
[~/]$ mkdir -m 0755 \
    ~/examples/rootCA \
    ~/examples/rootCA/private \
    ~/examples/rootCA/certs \
    ~/examples/rootCA/newcerts \
    ~/examples/rootCA/crl
[~/]$ mkdir -m 0755 \
    ~/examples/level1CA \
    ~/examples/level1CA/private \
    ~/examples/level1CA/certs \
    ~/examples/level1CA/newcerts \
    ~/examples/level1CA/crl
[~/]$ mkdir -m 0755 \
    ~/examples/TestUser \
    ~/examples/TestUser/private \
    ~/examples/TestUser/certs
```

Directory descriptions

- `./private`—The location for private keys. Normally, permissions on this directory should be set to restrict read access to root (0200) or to the user account for the web server. This example starts with full read/write access for everyone (0755).
- `./certs`—The location for the CA certificates.
- `./newcerts`—The location for new signed certificates. They are stored in unencrypted PEM format with a file name format cert_serial_number.pem (such as `03.pem`).
- `./crl`—The location for the certificate revocation list.

Modifying and storing an OpenSSL configuration file in each CA directory

The OpenSSL configuration file (`openssl.cnf`) contains the default directory structure, names, and options. On most Linux distributions, a default `openssl.cnf` file is located in `/etc/pki/tls`, as shown in the following example.

```
[~/examples]$ cp -v /etc/pki/tls/openssl.cnf ~/examples/
```

Changing the default directories

In this example, a change is made for all CAs and users. You can use this file as a template for other directories.

```
#########################################################################
[ CA_default ]
dir             = .   # CHANGE from “../../CA” # Everything is stored here
certs           = $dir/certs            # Issued certs are stored here
```

Creating a root CA

This section describes the steps for creating a root CA.

Copying the OpenSSL configuration file to the rootCA directory

Copy the `openssl.cnf` file to the root CA directory (`rootCA` in this example):

```
[~/examples]$ cp ~/examples/openssl.cnf ~/examples/rootCA/openssl-rootCA.cnf
[~/examples]$ cd ~/examples/rootCA
```

Creating the certificate and private key

Create the root CA key and certificate (`rootCA-private.key` and `rootCA.crt`). In the following example, the key length is set to 2048 and the hash signature algorithm to SHA256. When prompted, enter a secure passphrase. When using the `-nodes` option, you may omit the passphrase. When prompted for input such as the country, state, city, and so forth, you may specify an empty field by entering a dot ("."), as shown.

```
[~/examples/ rootCA]$ openssl req -config ./openssl-rootCA.cnf -newkey \
rsa:2048 -x509 -extensions v3_ca -keyout private/rootCA-private.key -out \
certs/rootCA.crt -days 1825 -sha256 -nodes
Generating a 2048 bit RSA private key
................+++
............+++
writing new private key to 'private/rootCA-private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]: .
State or Province Name (full name) [Berkshire]: .
Locality Name (eg, city) [Newbury]: .
Organization Name (eg, company) [My Company Ltd]: .
Organizational Unit Name (eg, section) []: .
Common Name (eg, your name or your server's hostname) []: My Root CA
Email Address []: .
[~/examples/rootCA]$ ]$ ls -l private/ certs/
certs/:
total 4
-rw-rw-r-- 1 xxx 1314 Nov 10 08:11 rootCA.crt
private/:
total 4
-rw-rw-r-- 1 xxx 1675 Nov 10 08:11 rootCA-private.key
```

To verify that the newly created certificate is correct, view the certificate by entering the command shown in the following example:

```
[~/examples/rootCA]$ openssl x509 -in certs/rootCA.crt -text
```

For a root self-signed certificate, the `-issuer` and `-subject` fields should match. To verify that they match, use the following command to display just the `-issuer` and `-subject` fields:

```
[~/examples/rootCA]$ openssl x509 -in certs/rootCA.crt \
   -noout -issuer -subject
```

Creating a combined private key and certificate PEM file

A combined private key and certificate PEM file is needed when the CA cross-signs other certificates. The file is referenced by the OpenSSL configuration file. The following commands change the default directory and create the combined private key and certificate PEM file `cakey.pem`:

```
[ ]$ cd ~/examples/rootCA
[ rootCA]$ cat private/rootCA-private.key certs/rootCA.crt > private/cakey.pem
```

Creating subordinate CAs

This section describes steps for creating server certificates that are issued (signed) by another CA.

Creating the directories for the subordinate CA

If not already present, create the directory structure to contain the subordinate CA database, as shown in the following example:

```
[~/]$ mkdir -m 0755 \
     ~/examples/level1CA \
     ~/examples/level1CA/private \
     ~/examples/level1CA/certs \
     ~/examples/level1CA/newcerts \
     ~/examples/level1CA/crl
```

Copy the modified `openssl.cnf` file to the working directory, as shown:

```
[~/examples]$ cp -v openssl.cnf level1CA/
`openssl.cnf' -> `level1CA/openssl.cnf'
```

Providing x509 certificate information

A certificate includes numerous data items that describe the certificate. The data can be entered manually when prompted or provided automatically via an OpenSSL configuration file. The following shows an example of how to create an OpenSSL configuration file via a script file.

```
#!/bin/sh
#
cat << _end_marker_ > openssl-level1CA.cnf
[ req ]
distinguished_name=req_DN
attributes=req_attr
prompt=no
[ req_DN ]
CN=level1CA
C=US
ST=TX
L=Houston
O=Development
```

```
subjectAltName=otherName:Gorilla
OU=Jungle
emailAddress=george@theJungle.com
surname=.
givenName=Frederick
initials=FGG
# dnQualifier=
name=George of the Jungle
[ req_attr ]
# challengePassword=
# unstructuredName=
_end_marker_
```

Generating a CSR and new server key

This step generates a new key (`-newkey)` and generates a CSR that can be submitted to a CA. The new private key is stored in the `keyout` location. The CSR is dumped to the `-out` parameter. For simplicity, the `-nodes` option is used to eliminate the need for protection from a passphrase.

```
[~/examples/level1CA]$ openssl req -config ./openssl-level1CA.cnf -newkey rsa:
2048 -sha256 -keyout \ ./private/level1CA-private.key -nodes -out ./temp-
level1CA.csr
```

Generating a CSR without generating a new key (Optional)

Generate the CSR without generating a new private key, as shown in this example:

```
[~/examples/level1-ca]$ openssl req -config ./openssl-level-1-ca.cnf \
-new -key ./level-1-CA-private.key  -nodes -out ./level-1-CA.csr
```

Viewing the private key

To view the private key, use the command shown in the following example:

```
[~/examples/level1CA]$ openssl rsa -in ./private/level1CA-private.key -text
```

Signing the level1CA CSR with the rootCA key

After a CSR is generated (in the preceding step), it must be signed by an established CA in the chain of trust. After the first signing request (when only the root CA exists), the CSR must be signed by the root CA. Subsequent CSRs may be signed by lower-level CAs, if they have permission to do so.

In this example, the root CA signs the first-level CSR (`level-1-CA.csr`).

1. Go to the CA that is signing. View the CSR and confirm that it should be signed:

   ```
   [ ]$ cd ~/examples/rootCA/

   [ rootCA]$ openssl req -in ../level1CA/temp-level1CA.csr -noout -text
   ```

2. Perform the following one-time setup step:

   ```
   [ rootCA]$ echo '01' > serial

   [ rootCA]$ touch index.txt
   ```

3. After verifying that you want to sign the CSR, have the CSR signed by issuing the following command:

   ```
   [~/examples/rootCA]$ openssl ca \

    -config openssl-rootCA.cnf \
   ```

```
-extensions v3_ca -policy policy_anything \

-in ../level1CA/temp-level1CA.csr \

-cert certs/rootCA.crt \

-default_md sha256 \

-key private/rootCA-private.key
```

The signed certificate is written to `./certs/{serialNumber}.pem`. The files `serial` and `index.txt` have been updated.

4. Install the certificate onto the first-level CA server, specifying the appropriate serial number (in this example, the serial number is `01`).

```
[ ~]$ cp ~/examples/rootCA/newcerts/01.pem ~/examples/level1CA/certs/
level1CA.pem
```

Creating user keys and CSRs

The steps for creating a new user key and CSR are similar to those for creating a CSR for a CA except a different type is specified.

Creating a directory for the user key and CSR database

If not already present, create the directory structure to contain the user key and CSR database:

```
[~/]$ mkdir -m 0755 \
     ~/examples/TestUser \
     ~/examples/TestUser/private \
     ~/examples/TestUser/certs
```

Copy the modified `openssl.cnf` file to the working directory:

```
[~/examples]$ cp -v ~/examples/openssl.cnf ~/examples/TestUser/
`~/examples/openssl.cnf' -> `~/examples/TestUser/openssl.cnf'
```

Providing x509 user certificate information

The data can be entered manually when prompted or provided automatically via an OpenSSL configuration file. The default configuration file is sufficient.

Generating a user CSR and new server key

This step generates a new key (`-newkey)` and generates a certificate request for a user. The resulting certificate will include the subject field (`-subj`). The subject field can be specified on the OpenSSL command line as a single parameter, or it can be populated from various fields in the `openssl.cnf` file. (For more information, see **Methods for specifying the subject field on a CSR**.) The CSR is written to the file specified by the `-out` parameter. In the following command example, the subject field is specified as a single parameter, and the CSR is written to `./temp-test-user.csr`.

```
[~/examples/TestUser]$ openssl req \
-subj "/O=Hewlett-Packard Company/OU=Employment Status - Employees/OU=VPN-WEB-H/
CN=Jonathan Smith/emailAddress=jonathan.smith@hp.com" \
-config ./openssl.cnf \
-newkey rsa:2048 -sha256 \
-keyout ./private/test-user-private.key \
-nodes \
-out ./temp-test-user.csr
```

View the CSR and verify that it is what you want signed. The following command displays the CSR:

```
[ ]$ openssl req -in ./temp-test-user.csr -text
```

Signing the user CSR with the level1CA key

To sign and configure a user certificate:

1. Sign the user CSR with the `level1CA` key, as in the following example:

   ```
   [ ]$ cd ~/examples/level1CA/
   ```

2. View the CSR and verify that it is what you want to sign. The following command displays the CSR:

   ```
   [ level1CA]$ openssl req -in ../TestUser/temp-test-user.csr -text
   ```

3. Specify how the user certificate may be used using x509 extensions. (For more information about x509 extensions, see the **OpenSSL website**.)

   The difference between a server certificate and a user certificate is the permissions that the CA assigns to the certificate. For example, a CA certificate is typically used as an SSL server, while a user certificate needs to be used as an SSL client and smart card login.

   To specify the extensions, modify the `openssl.cnf` file `[ user_cert ]` section, as shown in the following example. Uncomment the `nsCertType` and `keyUsage` lines as shown. The modified lines are shown in boldface type.

   ```
   [ usr_cert ]

   # These extensions are added when 'ca' signs a request.
   # This goes against PKIX guidelines but some CAs do it and some software
   # requires this to avoid interpreting an end user certificate as a CA.

   basicConstraints=critical, CA:FALSE

   # Here are some examples of the usage of nsCertType. If it is omitted
   # the certificate can be used for anything *except* object signing.

   # This is OK for an SSL server.
   # nsCertType                    = server

   # For an object signing certificate this would be used.
   # nsCertType = objsign

   # For normal client use this is typical
   nsCertType = client, email # Uncomment this line

   # and for everything including object signing:
   # nsCertType = client, email, objsign

   # This is typical in keyUsage for a client certificate.

   # Uncomment this line:
   keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment

   # If extendedKeyUsage is specified, it MUST include all three items
   # to be used for Two-Factor authentication.
   #       Client Authentication (1.3.6.1.5.5.7.3.2)
   #       Code Signing (1.3.6.1.5.5.7.3.3)
   ```

```
#       Smart Card Login (1.3.6.1.4.1.311.20.2.2)
#

extendedKeyUsage=clientAuth,codeSigning,1.3.6.1.4.1.311.20.2.2

# This will be displayed in Netscape's comment listbox.
nsComment = "OpenSSL Generated Certificate"

# PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

# This stuff is for subjectAltName and issuerAltname.

# Import the email address.
# subjectAltName=email:copy
# An alternative to produce certificates that aren't

# deprecated according to PKIX.
# subjectAltName=email:move

# Copy subject details
# issuerAltName=issuer:copy

# For testing purposes we will just use some well known CR

nsCaRevocationUrl = http://onsitecrl.verisign.com/
HewlettPackardCompanyITInfrastructure/LatestCRL.crl

#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName
```

4. Sign the certificate request, as in the following example:

   ```
   [level1CA]$ openssl ca -config
                                ./openssl.cnf -extensions usr_cert \ -policy
   policy_anything -in
                                ../TestUser/temp-test-user.csr -cert \ certs/
   level1CA.pem -md sha256
                                -keyfile private/level1CA-private.key
   ```

5. To view the results, issue the following command:

   ```
   [ level1CA]$ openssl x509 -in newcerts/07.pem -noout –text
   ```

6. To enable certificate usage in smart cards, the `keyUsage` field must include `sslAuth` and, if present, the `extendedKeyUsage` field must specify client authentication, code signing, and smart card login. For more information, see **Troubleshooting TFA and LDAP authentication problems**.

7. Give the public certificate to the user, using the following command:

   ```
   [ TestUser]$ cp -v ~/examples/level1CA/newcerts/07.pem ~/examples/Test/User/certs/test-user.pem
   ```

   ```
   `../level1CA/newcerts/06.pem' -> `certs/test-user.pem'
   ```

8. Combine the public certificate and private key into a PKCS #12 `.pem` file by creating a PKCS #12 certificate and providing a password (PIN) for the certificate. The user is prompted for the password (PIN). This password protects the private key contained in the PKCS #12 certificate.

```
[ ]$ cd ~/examples/TestUser
```

```
[ TestUser]$ openssl pkcs12 -export -in certs/test-user.pem -inkey \ private/test-user-
private.key -out private/test-user-private.p12
```

Verifying certificates

To verify the certificates, follow these steps.

1. To verify the certificates, use the commands shown in the following example:

```
[ examples]$ mkdir CA
[ examples]$ cp -v rootCA/certs/rootCA.crt CA/CA.pem
`rootCA/certs/rootCA.crt' -> `CA/CA.pem'
[ examples]$ cat  level1CA/certs/level1CA.pem >> CA/CA.pem
[ examples]$ openssl verify -CAfile CA/CA.pem -verbose -purpose sslserver./
level1CA/certs/level1CA.pem
./level1CA/certs/level1CA.pem: OK
```

2. Verify that the user certificate cannot be used for SSL server purposes, as is done in the following example:

```
[examples]$ openssl verify -CAfile CA/CA.pem -verbose -purpose sslserver./
TestUser/certs/test-user.pem
./TestUser/certs/test-user.pem: /O=Hewlett-Packard Company/
OU=EmploymentStatus - Employees/OU=VPN-WEB-H/CN=JonathanSmith/
emailAddress=jonathan.smith@hp.com
error 26 at 0 depth lookup:unsupported certificate purpose
OK
```

Verify that the user certificate can be used for SSL client purposes:

```
[user1@user1-station examples]$ openssl verify -CAfile CA/CA.pem -verbose-
purpose sslclient./TestUser/certs/test-user.pem
./TestUser/certs/test-user.pem: OK
```

Storing a user certificate on a smart card or browser

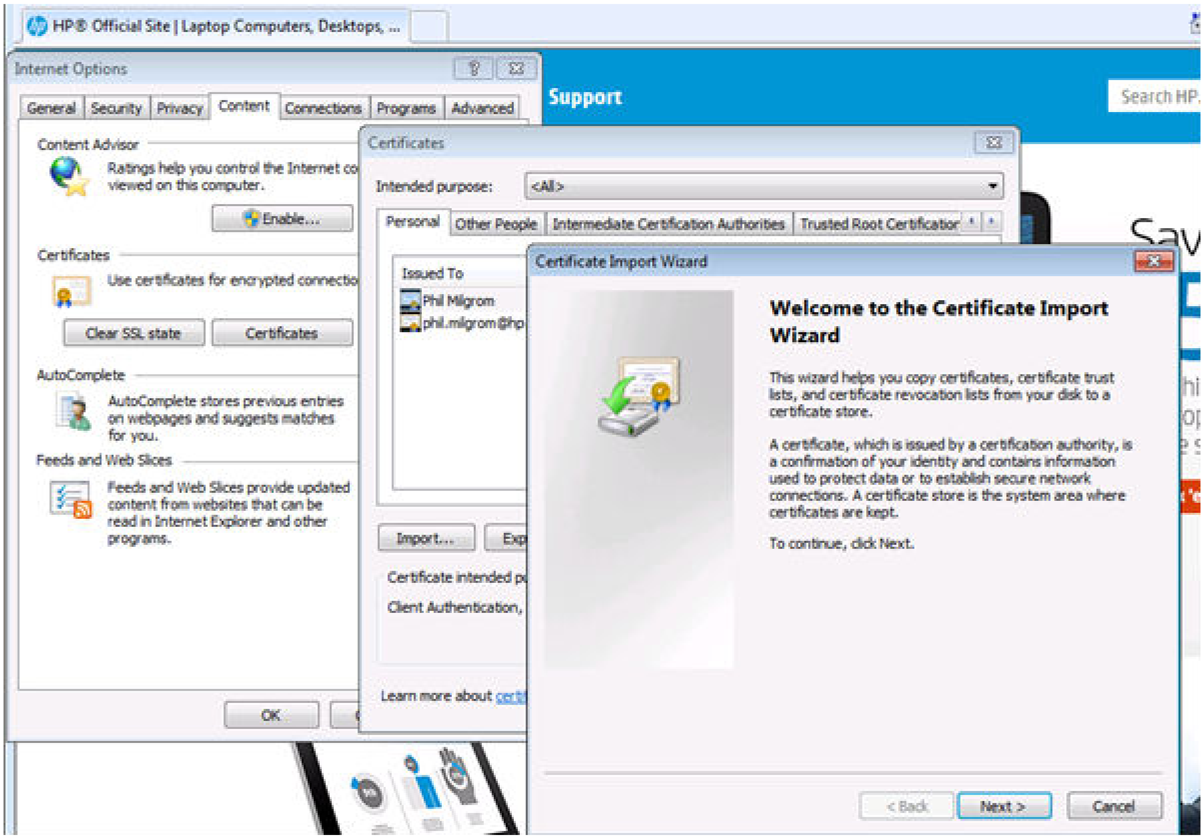
This section explains how to store a user certificate on a smart card or browser. The browser information in this section is based on Microsoft Internet Explorer.

The Microsoft Internet Explorer does not support PEM formatted files. Create a `.p12` certificate that contains both the private and public keys, using a command such as the following:

```
[ TestUser]$ openssl pkcs12 -export -in certs/test-user.pem -inkey private/test-
user-private.key -out private/test-user-private.p12
```

To install the `.p12` certificate using Internet Explorer 8, follow these steps:

1. Access the Internet Explorer Internet Certificate Wizard by clicking **Tools** > **Internet Options** > **Content** > **Certificates**:



Ratings help you control the Internet co viewed on this computer.

Use certificates for encrypted connectio

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

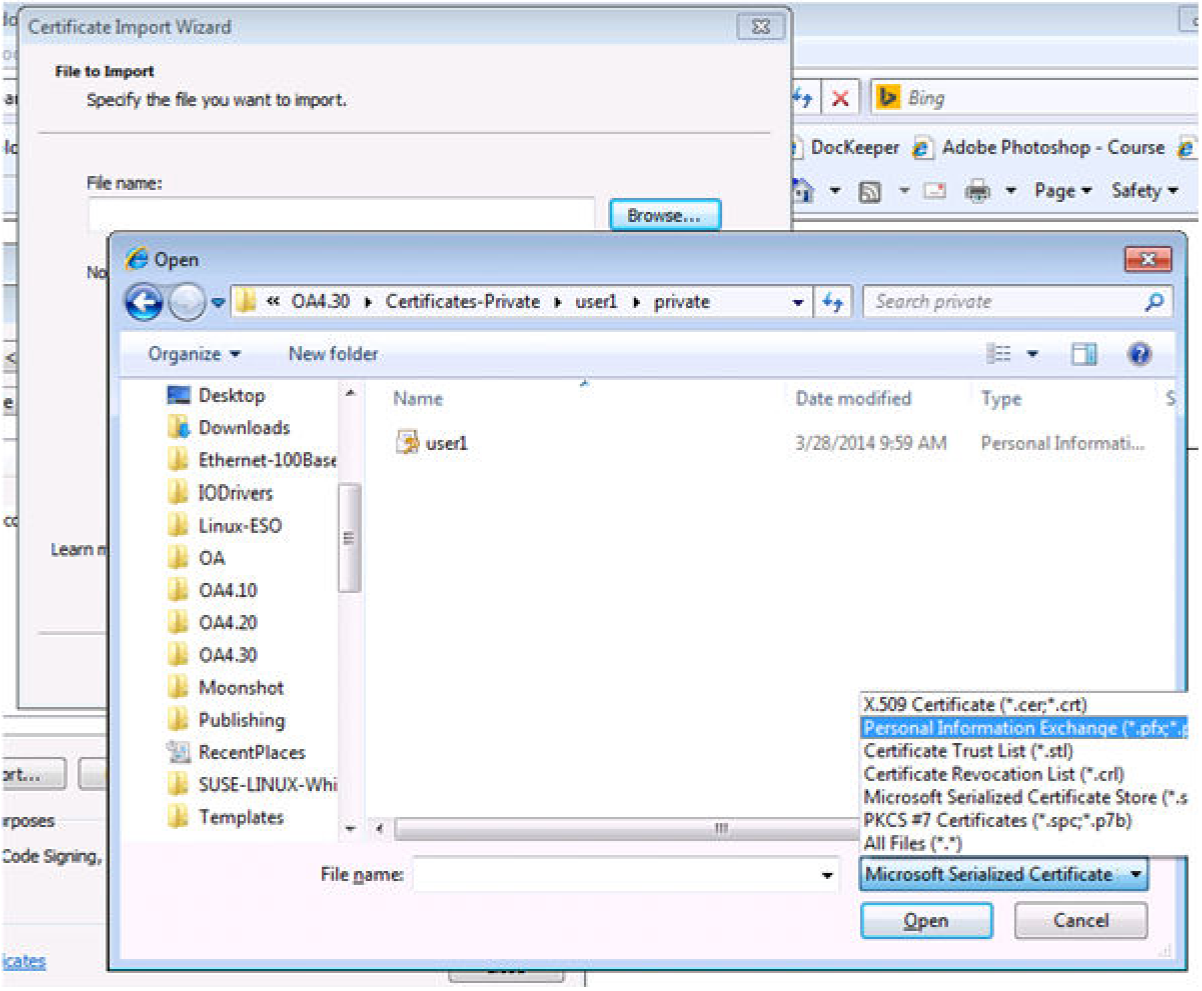
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

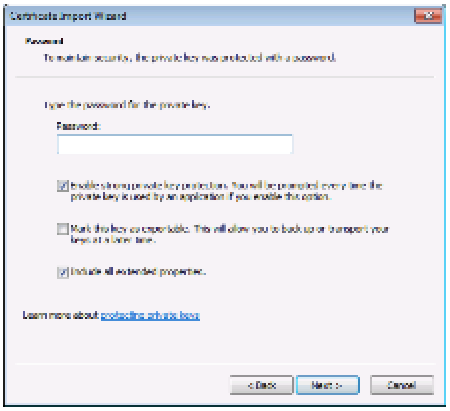
To continue, click Next.

2. Click **Next**.
3. Click **Browse...**.
   a. Locate the directory that contains the `.p12` certificate file.
   b. Change the file type to `Personal Information Exchange (.p12)`.


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Learn m
Bing
DocKeeper
Adobe Photoshop - Course
Page
Safety
Open
« OA4.30 ▸ Certificates-Private ▸ user1 ▸ private
Search private
Organize
New folder
Desktop
Downloads
Ethernet-100Base
IODrivers
Linux-ESO
OA
OA4.10
OA4.20
OA4.30
Moonshot
Publishing
RecentPlaces
SUSE-LINUX-Whi
Templates
Name
Date modified
Type
user1
3/28/2014 9:59 AM
Personal Informati...
X.509 Certificate (*.cer;*.crt)
Personal Information Exchange (*.pfx;*.p
Certificate Trust List (*.stl)
Certificate Revocation List (*.crl)
Microsoft Serialized Certificate Store (*.s
PKCS #7 Certificates (*.spc;*.p7b)
All Files (*.*)
File name:
Microsoft Serialized Certificate
Open
Cancel

c. Select the appropriate `.p12` certificate file.

4. Select the `.p12` file and click **Next**.
5. Enter the password specified when the PKCS#12 file was created (see **Signing the user CSR with the level1CA key**) and click **Next**. (Accept the default check-box values.)



To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☑ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

The Certificate Store window appears.

6. Click **Next**.
7. To complete the Wizard installation (import) process, click **Finish**.

8. The next window indicates that an application is creating a protected item and the security level is set for that item. Click **OK**.
9. When the wizard indicates that the import was successful, click **OK**.

Configuring the Onboard Administrator for Two-Factor Authentication with local accounts

This section provides an example showing how to configure the Onboard Administrator to enforce Two-Factor Authentication.

Establishing an Onboard Administrator recovery plan

Hewlett Packard Enterprise recommends establishing a recovery plan prior to configuring the Onboard Administrator for two-factor certificate authentication. If something goes wrong with the configuration, the Onboard Administrator configuration may be recovered accessing the USB key drive either through the serial port or the Insight Display panel. Both methods require physical access to the Onboard Administrator.

IMPORTANT:

If an LCD PIN has been configured (and forgotten), and local accounts have been disabled or TFA has been incorrectly configured, then the only way to recover is through a serial port.

The two most common situations where Onboard Administrator recovery is needed are when LDAP has been configured with local accounts disabled or when Two-Factor Authentication has been configured without certificate access (`keyUsage`).

Recovering via Insight Display and USB key

To recover the Onboard Administrator via USB key, create a configuration file on the USB key to restore the needed settings. The file can be configured to reset only what is needed to regain access or to completely restore factory settings:

- `GAIN_ACCESS.CFG` (reset only what is needed to regain access):

  ```
  DISABLE TWOFACTOR
  ```

  ```
  DISABLE LDAP
  ```

  ```
  SET USER PASSWORD “Administrator” “My.Password123”
  ```
- `SET_FACTORY.CFG` (reset to factory defaults):

  ```
  SET FACTORY
  ```

To recover a configuration:

1. Insert the USB key that contains the configuration file into the USB port of the Onboard Administrator.
2. Using the Insight Display display, navigate to the main menu, select **USB Key Menu**, and click **OK**.
3. Select **Restore Configuration**, then click **OK**.
4. Select the listed configuration file, then click **OK**.
5. The Confirm Operation screen appears. Click **OK**.

Recovering via serial console

To recover the Onboard Administrator via the serial port, follow these steps:

1. Ensure that you have the appropriate cables and software to connect to the Onboard Administrator serial port. The default serial connection setting is 9600, 8, N,1. For more information, see "**Recovering the Administrator password**."
2. Press and hold the **Reset** button for five seconds.
3. On the serial console, when you are prompted for Flash Recovery or Reset Password, press the **L** key (Lost Password).

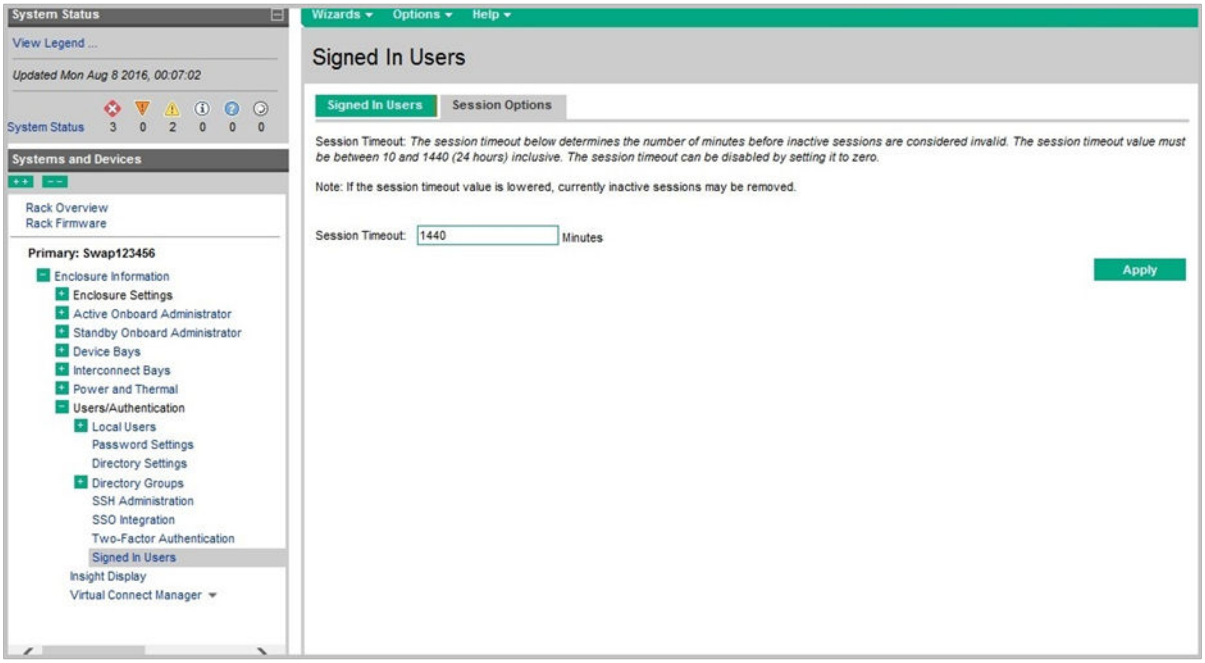
   The console displays the built-in Administrator account password and local logins are enabled.

Configuring the Onboard Administrator session timeout

By default, if a user session is inactive for one day (1440 minutes), a timeout occurs. Reduce this setting to a value that is suitable for your security policy. For testing purposes, you can set the timeout value to a minimum of 10 minutes. To modify the timeout setting, use the Onboard Administrator GUI or a CLI command. Valid timeout values are 0 (which disables the timeout), or an integer ranging from 10 to 1440.

Using the GUI

1. Navigate to the **Signed in Users** screen (**Enclosure Information** > **Users/Authentication** > **Signed in Users** and select the **Session Options** tab.



Session Timeout: *The session timeout below determines the number of minutes before inactive sessions are considered invalid. The session timeout value must be between 10 and 1440 (24 hours) inclusive. The session timeout can be disabled by setting it to zero.*

Note: If the session timeout value is lowered, currently inactive sessions may be removed.

Session Timeout: 1440 Minutes

2. Modify the **Session Timeout** field.
3. Click **Apply**.

Using the CLI

Use the following command, where *<timeout-value>* is the number of minutes:

```
SET SESSION TIMEOUT <timeout-value>
```

Installing the CA chain for TFA

A certificate chain consists of all the certificates needed to verify the user certificate. The certificate chain starts with the root certificate followed by all intermediate authority certificates. Every intermediate CA in the chain holds a certificate issued by the CA that is one level above it in the trust hierarchy. The root CA issues a certificate for itself.

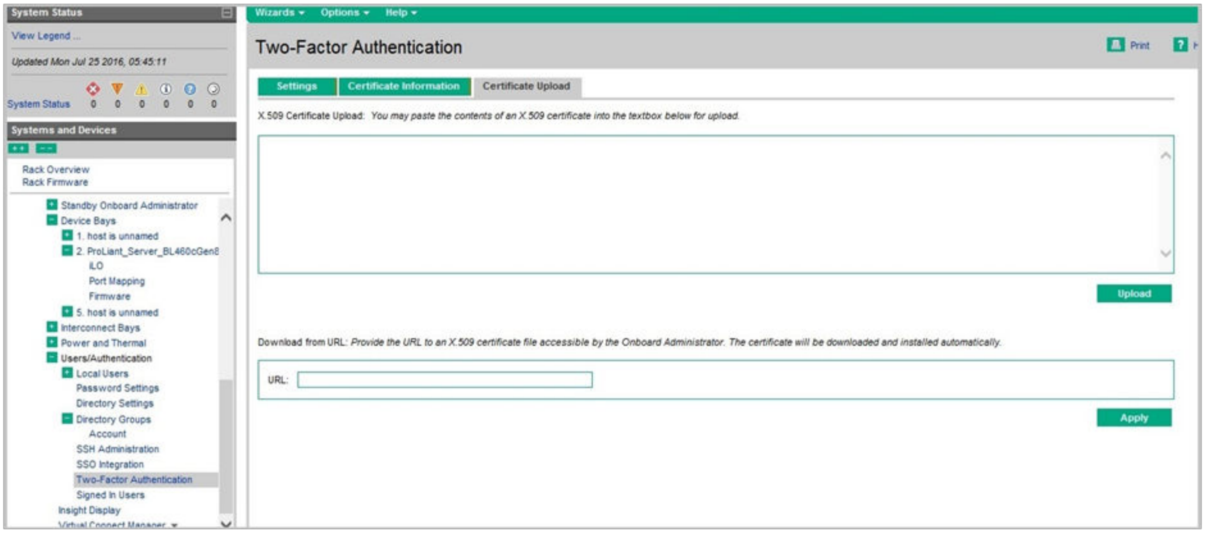
This section describes how to install CAs for Two-Factor Authentication.

IMPORTANT:

Two-Factor Authentication and LDAP have separate repositories for CAs. Do not confuse them with one another.

To install CA certificates for Two-Factor Authentication, use the Onboard Administrator GUI as follows:

1. Navigate to the Two-Factor Authentication screen: **Enclosure Information** > **Users/Authentication** > **Two-Factor Authentication**.
2. Click the **Certificate Upload** tab. The Certificate Upload screen appears as shown in the following example.



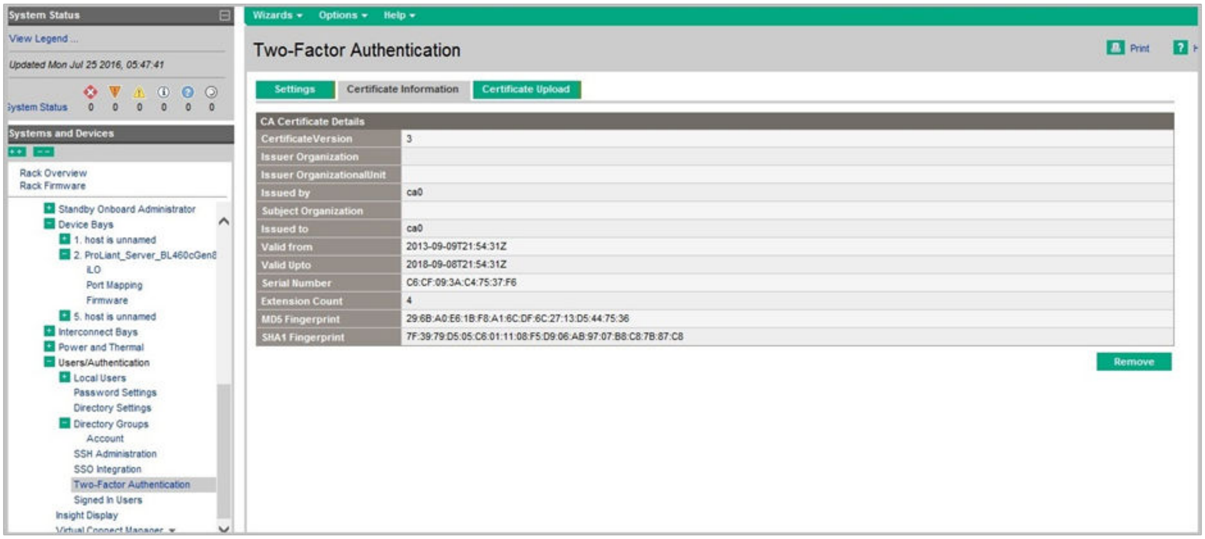
X.509 Certificate Upload: *You may paste the contents of an X.509 certificate into the textbox below for upload.*

Download from URL: *Provide the URL to an X.509 certificate file accessible by the Onboard Administrator. The certificate will be downloaded and installed automatically.*

3. Copy and paste the root CA certificate into the text box provided by the **Certificate Upload** screen. The certificate includes beginning and ending delimiters, as shown:

```
-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIJALg8cO2Ikvr8MA0GCSqGSIb3DQEBBQUAMDkxDDAKBgNV
BAMTA2NhMDEUMBIGCgmSJomT8ixkARkWBHRlc3QxEzARBgoJkiaJk/IsZAEZFgNj
.
.
.
Ob6IFCSUTKbCVT95cYTRHiSbgBYaqDXBJk3Lyjvtb7ZovmMT5dnU/w061wV5MEce
RZfXH3U=
-----END CERTIFICATE-----
```

4. Click **Upload**. After the certificate is uploaded successfully, the **Certificate Information** tab displays, as in the following example.

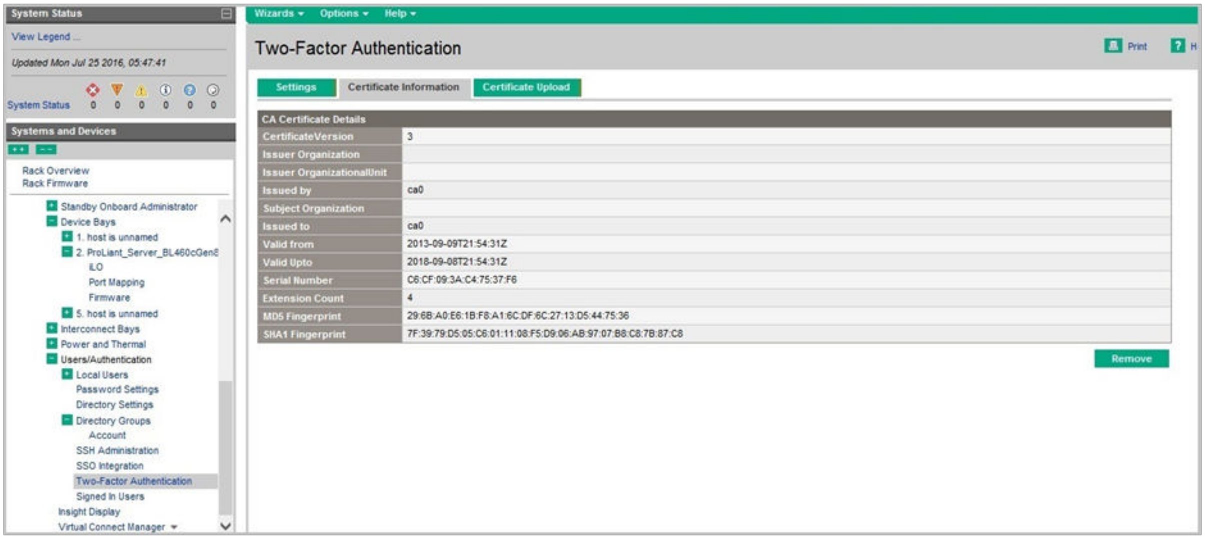


Two-Factor Authentication

CA Certificate Details	
CertificateVersion	3
Issuer Organization	
Issuer OrganizationalUnit	
Issued by	ca0
Subject Organization	
Issued to	ca0
Valid from	2013-09-09T21:54:31Z
Valid Upto	2018-09-08T21:54:31Z
Serial Number	C6:CF:09:3A:C4:75:37:F6
Extension Count	4
MD5 Fingerprint	29:6B:A0:E6:1B:F8:A1:6C:DF:6C:27:13:D5:44:75:36
SHA1 Fingerprint	7F:39:79:D5:05:C6:01:11:08:F5:D9:06:AB:97:07:B8:C8:7B:87:C8

5. Add an intermediate or end CA in the chain:
   a. Return to the **Certificate Upload** tab.
   b. Copy and paste the next CA certificate into the text box provided.
   c. Click **Upload**.

      After the certificate is successfully uploaded, the **Certificate Information** tab appears, as in the following example (in this example, the CA1 certificate was issued by the root CA CA0).



Two-Factor Authentication

CA Certificate Details	
CertificateVersion	3
Issuer Organization	
Issuer OrganizationalUnit	
Issued by	ca0
Subject Organization	
Issued to	ca0
Valid from	2013-09-09T21:54:31Z
Valid Upto	2018-09-08T21:54:31Z
Serial Number	C6:CF:09:3A:C4:75:37:F6
Extension Count	4
MD5 Fingerprint	29:6B:A0:E6:1B:F8:A1:6C:DF:6C:27:13:D5:44:75:36
SHA1 Fingerprint	7F:39:79:D5:05:C6:01:11:08:F5:D9:06:AB:97:07:B8:C8:7B:87:C8

   d. To install additional CAs, repeat steps a through c for each intermediate certificate.

CLI commands for administrating certificates

Use the following CLI commands to add, download, display, and remove certificates. For more information, see the *Onboard Administrator Command Line Interface User Guide*.

- `ADD CA CERTIFICATE`
- `DOWNLOAD CA CERTIFICATE`
- `SHOW CA CERTIFICATE`
- `REMOVE CA CERTIFICATE`

Configuring the HTTP proxy

The Onboard Administrator might require a proxy server to reach addresses such as those needed to verify a certificate or to obtain a CRL. (A CRL is a database of certificates that have been revoked before they expired.) For this purpose, configure the HTTP proxy server on the Onboard Administrator by using the following command:

```
SET URB PROXY URL { <URL> }
```

The specified URL can contain up to 128 characters.

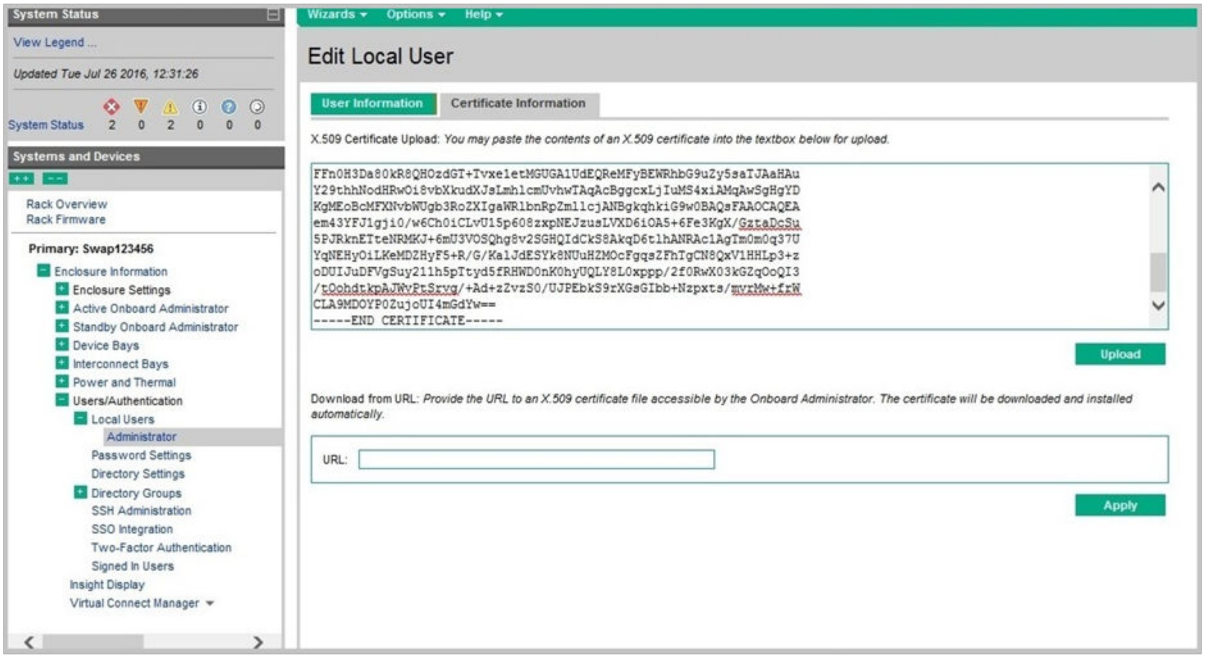
The Onboard Administrator GUI does not include the ability to set a proxy URL.

Installing user certificates on the local Administrator account

To install a user certificate on the Onboard Administrator Administrator account:

1. Navigate to the Local Users Administrator screen (Edit Local User): **Enclosure Information** > **Users/Authentication** > **Local Users** > **Administrator**.
2. Click the **Certificate Information** tab.

   If an Administrator certificate has not yet been installed, the Certificate Information screen appears with an empty text box. Copy and paste the appropriate user certificate into the text box as shown.



Edit Local User

X.509 Certificate Upload: *You may paste the contents of an X.509 certificate into the textbox below for upload.*

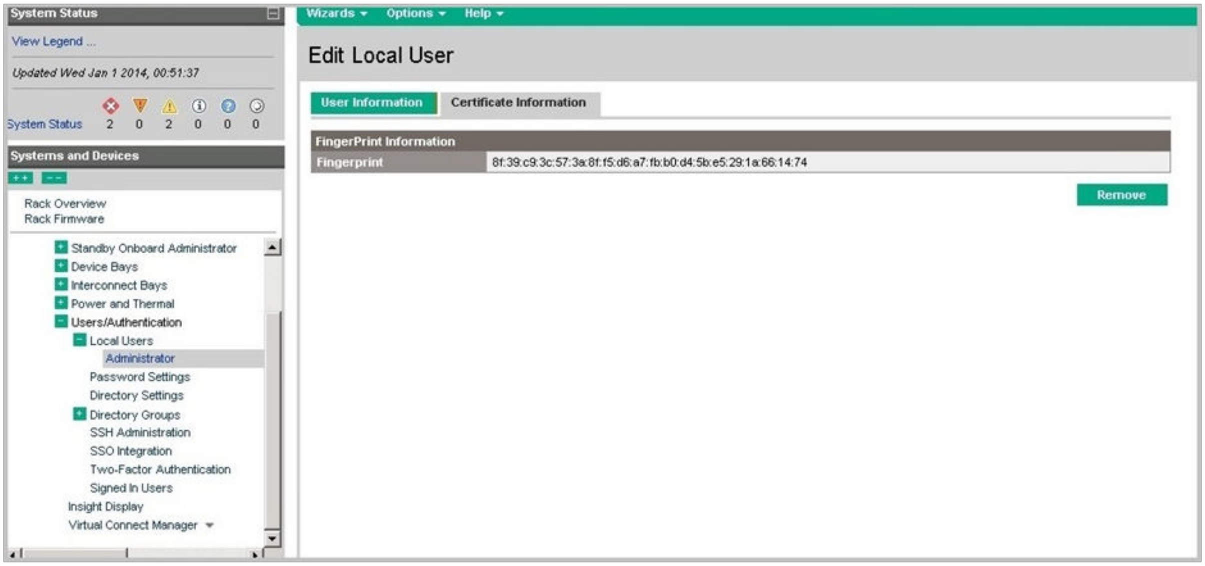
```
FFn0H3Da80kR8QHOzdGT+Tvxe1etMGUGA1UdEQReMFyBEWRhbG9uZy5saTJAaHAu
Y29thhNodHRwOi8vbXkudXJsLmhlcmUvhwTAqAcBggcxLjIuMS4xiAMqAwSgHgYD
KgMEoBcMFXNvbWUgb3RoZXIgaWRlbnRpZmllcjANBgkqhkiG9w0BAQsFAAOCAQEA
em43YFJ1gji0/w6Ch0iCLvU15p608zxpNEJzusLVXD6iOA5+6Fe3KgX/GztaDcSu
5PJRknETteNRMKJ+6mU3VOSQhg8v2SGHQIdCkS8AkqD6tlhANRAc1AgTm0m0q37U
YqNEHyOiLKeMDZHyF5+R/G/KalJdESYk8NUuHZMOcFgqsZFhTgCN8QxV1HHLp3+z
oDUIJuDFVgSuy211h5pTtyd5fRHWD0nK0hyUQLY8L0xppp/2f0RwX03kGZqOoQI3
/tOohdtkpAJWvPtSrvg/+Ad+zZvzS0/UJPEbkS9rXGsGIbb+Nzpxts/mvrMw+frW
CLA9MDOYP0ZujoUI4mGdYw==
-----END CERTIFICATE-----
```

Download from URL: *Provide the URL to an X.509 certificate file accessible by the Onboard Administrator. The certificate will be downloaded and installed automatically.*

URL:

3. Click **Upload**.

   After the certificate is uploaded successfully, the **Certificate Information** tab displays, as in the following example:



Edit Local User

FingerPrint Information

Fingerprint 8f:39:c9:3c:57:3a:8f:f5:d6:a7:fb:b0:d4:5b:e5:29:1a:66:14:74

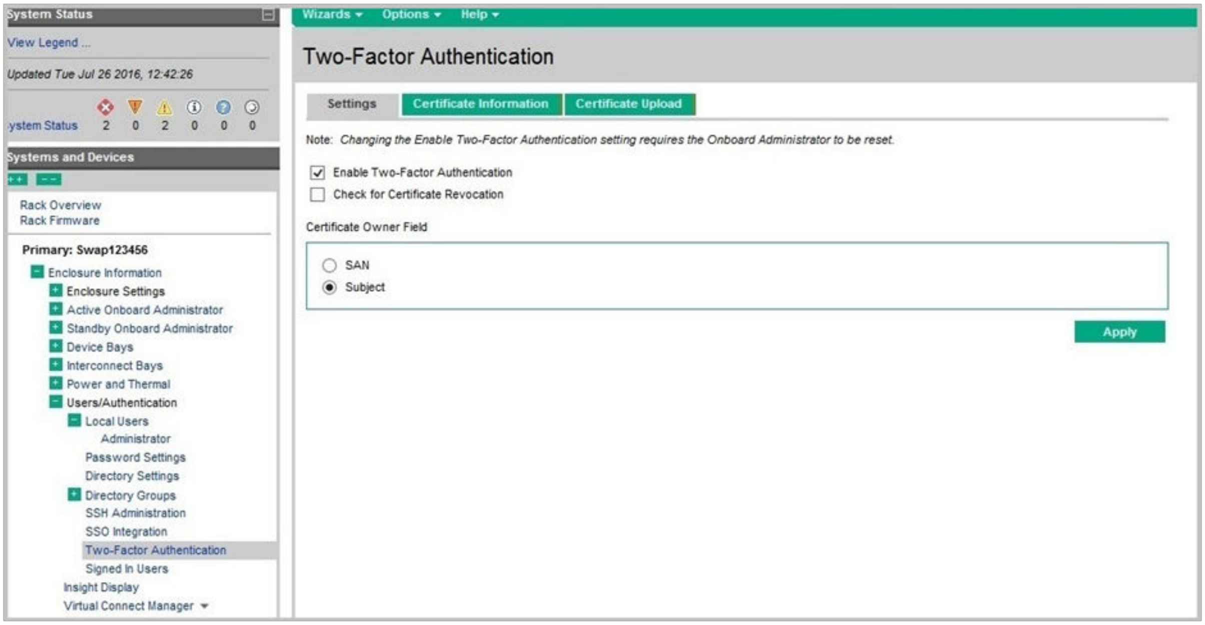
If the uploaded user certificate cannot be verified, see **Miscellaneous known issues**.

Enabling Two-Factor Authentication

After successfully uploading CA certificates for Two-Factor Authentication and uploading at least one Onboard Administrator Administrator account, you may enable Two-Factor Authentication:

1. Navigate to the **Two-Factor Authentication Settings** tab (click **Enclosure Information** > **Users/ Authentication** > **Local Users** > **Two-Factor Authentication**).
2. Select the **Enable Two-Factor Authentication** check box, as shown in the following example.

   If using Two-Factor Authentication in combination with LDAP, use the **Certificate Owner** field to specify whether to have the Onboard Administrator use the subject alternative name field (**SAN**) or the certificate subject field (**Subject**). For more information about using Two-Factor Authentication with LDAP, see **TFA +LDAP Authentication**.



Two-Factor Authentication

Note: *Changing the Enable Two-Factor Authentication setting requires the Onboard Administrator to be reset.*

☑ Enable Two-Factor Authentication

□ Check for Certificate Revocation

Certificate Owner Field

○ SAN

● Subject

3. Click **Apply**.

Logging in to the Onboard Administrator web GUI using Two-Factor Authentication

Browse to the Onboard Administrator web GUI and click the appropriate user certificate (if there is more than one). The browser should ask you to confirm the certificate.

The certificate is necessary for establishing an SSL/TLS session with the Onboard Administrator. If the connection is made successfully, you are logged in to the Onboard Administrator as the local user account associated with the user certificate.

If problems occur, see **Troubleshooting TFA and LDAP authentication problems**.

TFA+LDAP Authentication

In addition to normal Two-Factor Authentication, the Onboard Administrator also supports TFA+LDAP authentication. In this mode, the user must:

- Have a user certificate installed on the Onboard Administrator
- Know the PIN to the certificate
- Know the associated LDAP user password

The advantages of TFA+LDAP authentication are:

- Greater security is gained, as three items are required to authenticate instead of two.
- Authorization (access permission) is managed using LDAP groups instead of mapping user certificates to individual local Onboard Administrator user accounts.

How TFA+LDAP authentication works

If LDAP is configured and the Two-Factor Authentication user certificate is not mapped to a local Onboard Administrator user account, then when a user attempts to log into the Onboard Administrator GUI login page, the Onboard Administrator extracts a user ID from the user certificate and prompts the user for the LDAP password.

The LDAP user name is extracted from either the subject or subject alternative name field of the certificate and is visible in the Onboard Administrator login page, depending on your selection made on the Two-Factor Authentication Settings tab. For more information, see **Enabling Two-Factor Authentication**. If subject is selected, then the user name is formatted according to RFC 2253 to create an FQDN. If **SAN** (subject alternative name) is selected, the Onboard Administrator uses the first SAN field in the certificate that is of type EMAIL, OTHERNAME, DNS, or URI. The CA controls the order and content of subject alternative name fields during the signing process. You cannot change the name used in the GUI.

After you specify the LDAP password, the following checks occur:

- The user certificate is verified against the CA certificates installed on the Onboard Administrator.
- The LDAP credentials are authenticated against the configured LDAP server.
- The LDAP user is verified as a member of an authorized group on the Onboard Administrator.

If all three conditions are met, a session to the Onboard Administrator is established and the user is fully logged in to the Onboard Administrator.

Enabling TFA+LDAP authentication

To use TFA+LDAP authentication, perform the following steps:

1. Configure the Onboard Administrator for Two-Factor Authentication, following the instructions in **Configuring the Onboard Administrator for Two-Factor Authentication with local accounts**.
2. Configure the Onboard Administrator to use LDAP authentication, as described in **Directory Settings screen**.

3. Log in to the Onboard Administrator using only Two-Factor Authentication and then re-enable LDAP (required because enabling Two-Factor Authentication automatically disables LDAP). For more information about enabling LDAP, see **Directory Settings screen** and **Preparing the directory**.
4. After verifying that everything works as expected, you may disable Local Account access by deselecting the **Enable Local Users** check box on the Directory Settings screen.

Methods for specifying the subject field on a CSR

Use any of several methods to control the content of the **Subject** field on a CSR:

- Interactively, on the OpenSSL command line
- Manually, on the OpenSSL command line (for an example, see **Generating a user CSR and new server key**)
- In the OpenSSL configuration file (`.cnf`)
- Through an abbreviated OpenSSL response file (the response file is generated by the CA and contains your public key and is digitally signed by the CA; you install the response file on the web server)

Use the most suitable method for your needs.

Troubleshooting TFA and LDAP authentication problems

This section describes solutions for problems that might be seen when attempting to authenticate using TFA and LDAP certificates.

Problem:

Browser reports `cannot display webpage` or `authentication attempt failed` message.

Solution:

For the `cannot display webpage` problem:

1. Verify that the certificate has approved usage for the SSL client.

   For example, issue the following command

   ```
   [ examples]$ openssl verify -CAfile CA/CA.pem -verbose \-purpose sslclient ./
   TestUser/certs/test-user.pem
   ./TestUser/certs/test-user.pem: OK
   ```
2. Verify that this certificate is available to the browser. (In Internet Explorer, go to **Tools** > **Internet Options** > **Content** > **Certificates**.)
3. If the certificate is stored on a key or token, ensure that it has been properly installed on the key or token.

If the `authentication attempt failed` message appears in the browser, a certificate with SSL client usage was available to establish the SSL/TLS session, but other issues exist. Try the following steps:

1. Make sure the certificate is valid, using a command such as the following:

   ```
   [level1CA]$ openssl verify -CAfile CA/CA.pem -verbose -purpose sslclient ~/
   examples/level1CA/newcerts/0A.pem
   .
   .
   .
   error 9 at 0 depth lookup:certificate is not yet valid
   ```
2. If the certificate is not valid, follow the instructions provided by the OpenSSL error message. If the certificate is not valid, the system clock might be defective. If the certificate cannot be verified, the corresponding CA certificate might not be available. In addition, follow these steps:

a. Ensure that the dates associated with the certificate have not expired.

b. Examine the CSR OpenSSL configuration file `keyUsage` and `extendedKeyUsage` fields. The `keyUsage` field specifies usage restrictions. If present, the `extendedKeyUsage` field places additional restrictions on usage.

   If the `extendedKeyUsage` field is present and specifies `clientAuth` only, the browser (Internet Explorer) will not pass the certificate to the Onboard Administrator. This leads to the `cannot display web page` message.

   If the `extendedKeyUsage` field is not present, the certificate can be used for smart card login. To enable certificate usage in smart cards, the `keyUsage` field must include `sslAuth` and, if present, the `extendedKeyUsage` field must specify client authentication, code signing, and smart card login.

   Examples:

   The following certificate will not work because it is missing the sslClient usage:

```
X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

   The following certificate will work because it contains everything needed:

```
X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
```

Problem:

Issues attempting to switch among multiple client users on the same system.

Solution:

Sometimes browsers cache credentials to a greater extent than necessary. Try clearing the browser cache, deleting all temporary files, and then closing all browser windows. Otherwise, the issue might resolve simply by waiting a day for the sessions to expire.

To test multiple client certificates from the same client system, separate logins might be necessary. Otherwise, the browser might select the last known valid certificate.

CLI examples configuring a user account and certificates

The following example shows Onboard Administrator CLI commands used for configuring a local user account and certificates. Commentary follows the example.

```
=======================================
== Add user, CA certs, and user cert
=======================================
set script mode on
add user "marc" "password"
set user contact "marc" "800-555-1212"
set user fullname "marc" "Marc Last-name"
set user access "marc" ADMINISTRATOR
enable user "marc"
assign server all "marc"
assign interconnect all "marc"
assign oa "marc"
show user "marc"
download ca certificate http://dev-srvr/certs/Common-Policy.cer
download ca certificate http://dev-srvr/certs/SHA-1-Federal-Root-CA.cer
download ca certificate http://dev-srvr/certs/DoD-Interoperability-Root-CA-1.cer
download ca certificate http://dev-srvr/certs/DoD-Root-CA-2.cer
download ca certificate http://dev-srvr/certs/DOD-EMAIL-CA-19.cer
download user certificate "marc" http://dev-srvr/certs/Marc-Lastname.cer
show user "marc"
set script mode off
==================================================
== Go to the GUI, enable TFA, then
== log in via the Web browser using the TFA token.
==================================================
=======================================
== Remove Fed certificates and user
=======================================
set script mode on
remove ca certificate "CD:78:54:4C:CA:C6:EA:15:72:81:86:EB:
86:59:F6:E6:C0:FA:A7:41"
remove ca certificate "B1:10:5C:D1:0F:C3:70:F5:6B:89:DD:1D:49:F6:D8:30:DF:
35:F2:DE"
remove ca certificate "FD:F3:F4:F8:C7:3B:5A:
63:20:62:08:88:29:00:D1:92:B1:75:BA:E8"
remove ca certificate "30:BE:4D:
40:F6:10:E5:65:B3:53:F3:44:C7:27:64:1E:EE:E7:86:D2"
remove ca certificate "CB:44:A0:97:85:7C:45:FA:18:7E:D9:52:08:6C:B9:84:1F:2D:
51:B5"
remove user certificate "Marc"
remove user "marc"
set script mode off
```

The commands in the first section of the example add a user with Administrator privileges and install certificates:

- Adds a user account (`ADD USER`)
- Sets user properties (`SET USER`)
- Enables a user account (`ENABLE USER`)
- Assigns all server and interconnect bays to the control of the user (`ASSIGN SERVER ALL`, `ASSIGN INTERCONNECT ALL`)
- Grants the specified user access privilege to the Onboard Administrator's bays (`ASSIGN OA`)
- Displays user information, user access level, and bays assigned to the user (`SHOW USER`)
- Installs CA certificates from the specified locations (`DOWNLOAD CA CERTIFICATE`)
- Installs a user certificate from the specified location (`DOWNLOAD USER CERTIFICATE`)

The script comments are a reminder to use the Onboard Administrator GUI to enable Two-Factor Authentication and then to log in via the web browser, using the appropriate TFA key.

The second section of the example:

- Removes CA certificates (`REMOVE CA CERTIFICATE`)
- Removes a user certificate (`REMOVE USER CERTIFICATE`)
- Removes a user (`REMOVE USER`)

Information about CAs and certificates available from the Web

For more information about managing CAs and certificates, see the following websites:

- **OpenSSL documentation website**
- **Linux Documentation Project website** (How manage CAs and issue or sign SSL certificates)
- **G-Loaded Journal website** (How to become a CA and issue server certificates)
- **Debian Administration website** (Creating and using self-signed certificates)

Configuring CAC Authentication for local users and LDAP group accounts

For creating CAs and generating certificates, refer to below Two-Factor section:

Creating CAs and configuring Two-Factor Authentication for local user and LDAP group accounts

Establish an OA recovery plan

It is highly recommended to establish a recovery plan before getting started. If something goes wrong with the OA configuration, the OA may be recovered through the serial port or Insight Display panel and USB KEY. Both methods require physical access to the OA. However, **if an LCD PIN has been configured (and forgotten)** and local accounts have been disabled or CAC has been incorrectly configured then, **the only way to recover is through a serial port**.

The two most common situations where OA recovery is needed are when LDAP has been configured incorrectly with local accounts disabled or when CAC has been configured without loading the appropriate CA certificates.

Please refer to steps mentioned in the Two-Factor section for establishing a recovery plan prior to enabling CAC authentication.

Establishing an Onboard Administrator recovery plan

Enabling CAC Authentication for LDAP users

When LDAP is configured, then the OA extracts a user ID from the user's certificate for user authentication. Ensure that the same user certificate should not be mapped to the local user account. The user certificate is verified against the CA certificates installed on the OA . The service account configured in LDAP settings is used for accessing and authenticating the user against the configured LDAP server. If the LDAP user is a member of an authorized group on the OA, then a session to the OA is established and the user is fully logged into the OA.

The LDAP username is extracted from either the "Subject" or "Subject Alternative Name" field of the certificate .

If "Subject" is selected then OA will use the first common name (CN) field of "subject" as LDAP user name.

If "Subject Alternate Name" (SAN) is selected, then OA will use the first SAN field in the certificate that could be any of the EMAIL, OTHERNAME, DNS, or URL fields.

During certificate generation, ensure that the LDAP user name is the first CN of subject or first field in the SAN.

In the OA GUI, the Certificate Owner Field setting is used to specify "Subject" or "Subject Alternative Name (SAN)".

Prerequisites:

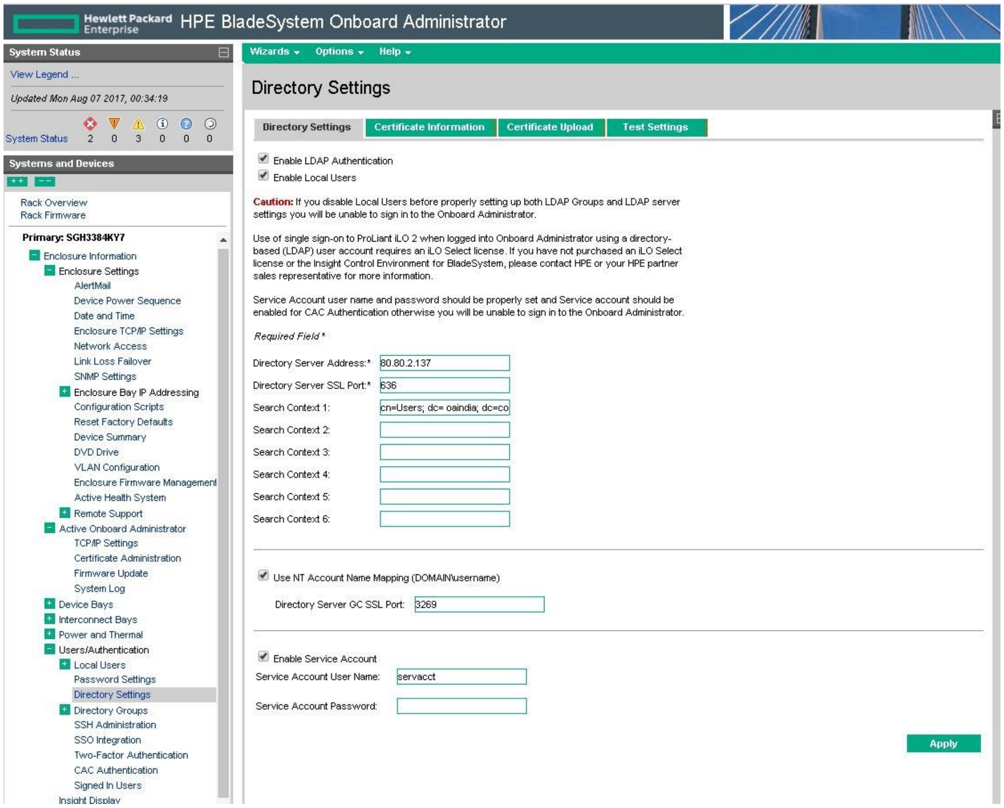
Below configuration should be done prior to enable CAC with LDAP.

1. LDAP configuration

   The Active Directory settings must be configured correctly. If they are not configured correctly, constrained delegation will not work. This includes configuring services account in the active directory settings.

   LDAP setting can be applied at **Enclosure Information** > **Users/Authentication** > **Directory Settings**.

To set service account, **Enable service account** option should be selected, and service account user name and password should be provided.



☑ Enable LDAP Authentication

☑ Enable Local Users

Caution: If you disable Local Users before properly setting up both LDAP Groups and LDAP server settings you will be unable to sign in to the Onboard Administrator.

Use of single sign-on to ProLiant iLO 2 when logged into Onboard Administrator using a directory-based (LDAP) user account requires an iLO Select license. If you have not purchased an iLO Select license or the Insight Control Environment for BladeSystem, please contact HPE or your HPE partner sales representative for more information.

Service Account user name and password should be properly set and Service account should be enabled for CAC Authentication otherwise you will be unable to sign in to the Onboard Administrator.

*Required Field **

Directory Server Address:* 80.80.2.137

Directory Server SSL Port:* 636

Search Context 1: cn=Users; dc= oaindia; dc=co

Search Context 2:

Search Context 3:

Search Context 4:

Search Context 5:

Search Context 6:

☑ Use NT Account Name Mapping (DOMAIN\username)

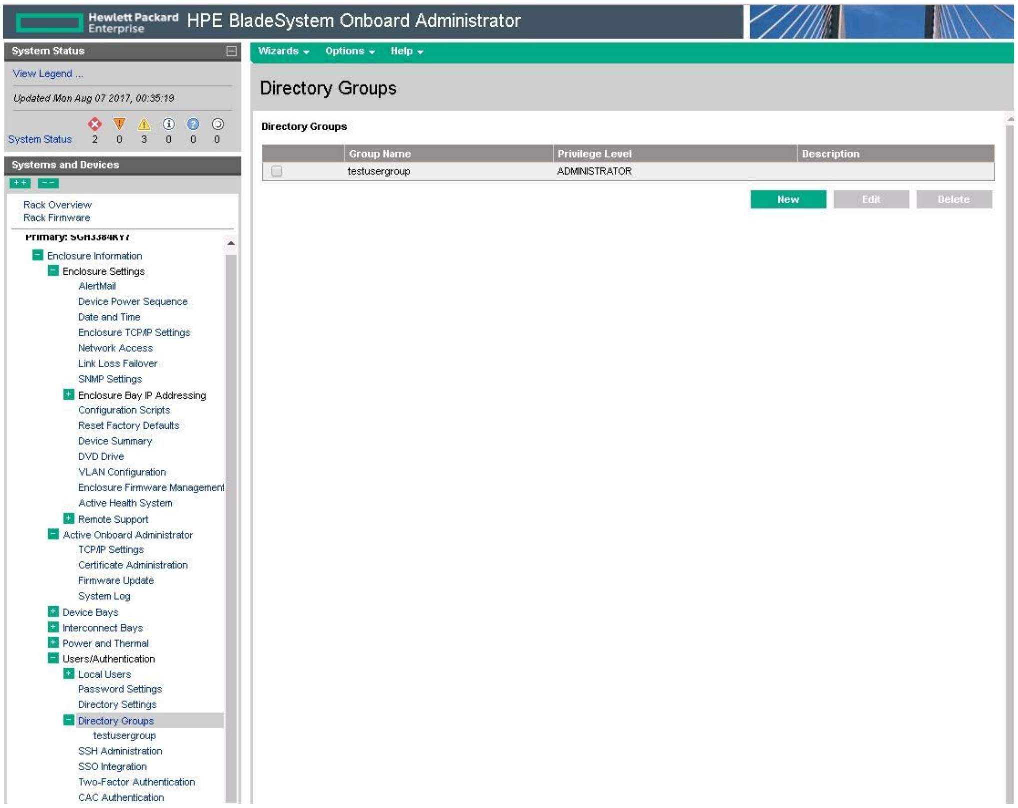
Directory Server GC SSL Port: 3269

☑ Enable Service Account

Service Account User Name: servacct

Service Account Password:

Directory groups consisting of users should be added at **Enclosure Information** > **Users/ Authentication** > **Directory Groups**.



Directory Groups

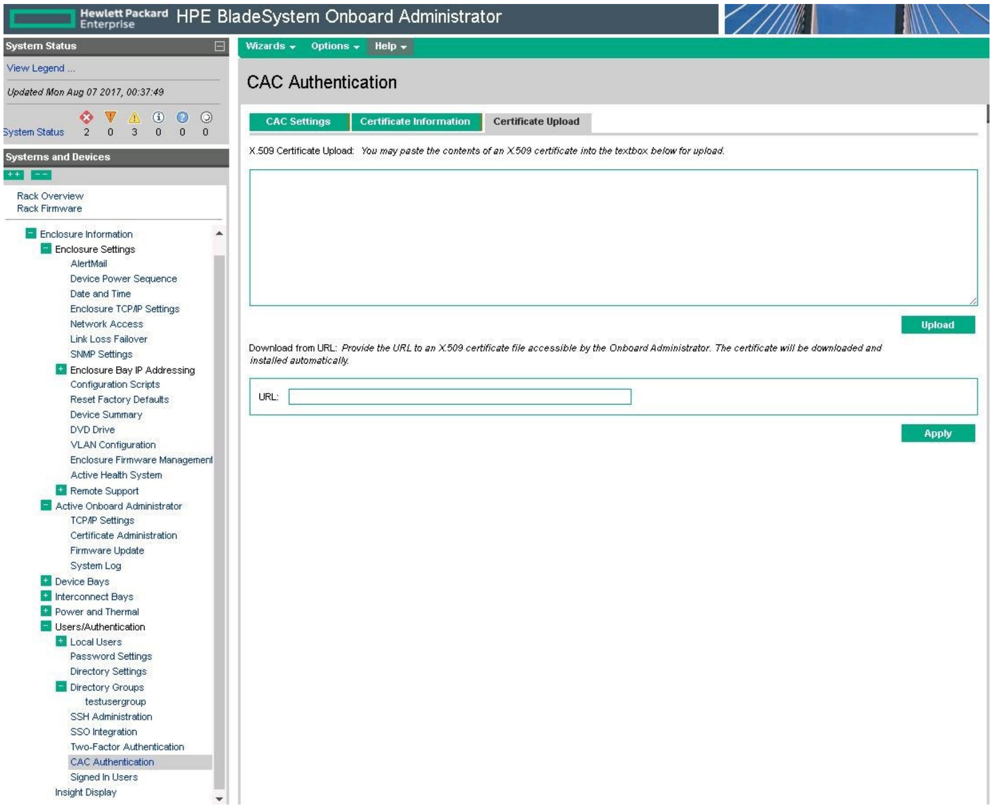
Directory Groups

	Group Name	Privilege Level	Description
□	testusergroup	ADMINISTRATOR	

2. Install CA chain

   To install a CA certificate, in the GUI navigate to **Enclosure Information** > **Users/Authentication** > **CAC Authentication**, then click on the "Certificate Upload" tab. Copy and paste the root CA certificates into the **x.509 certificate upload** test box . The certificate includes begin and end tags as shown:

```
-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIJALg8cO2Ikvr8MA0GCSqGSIb3DQEBBQUAMDkxDDAKBgNV
BAMTA2NhMDEUMBIGCgmSJomT8ixkARkWBHRlc3QxEzARBgoJkiaJk/IsZAEZFgNj
. . . . .
Ob6IFCSUTKbCVT95cYTRHiSbgBYaqDXBJk3Lyjvtb7ZovmMT5dnU/w061wV5MEce
RZfXH3U=
-----END CERTIFICATE-----
```



Updated Mon Aug 07 2017, 00:37:49

CAC Authentication

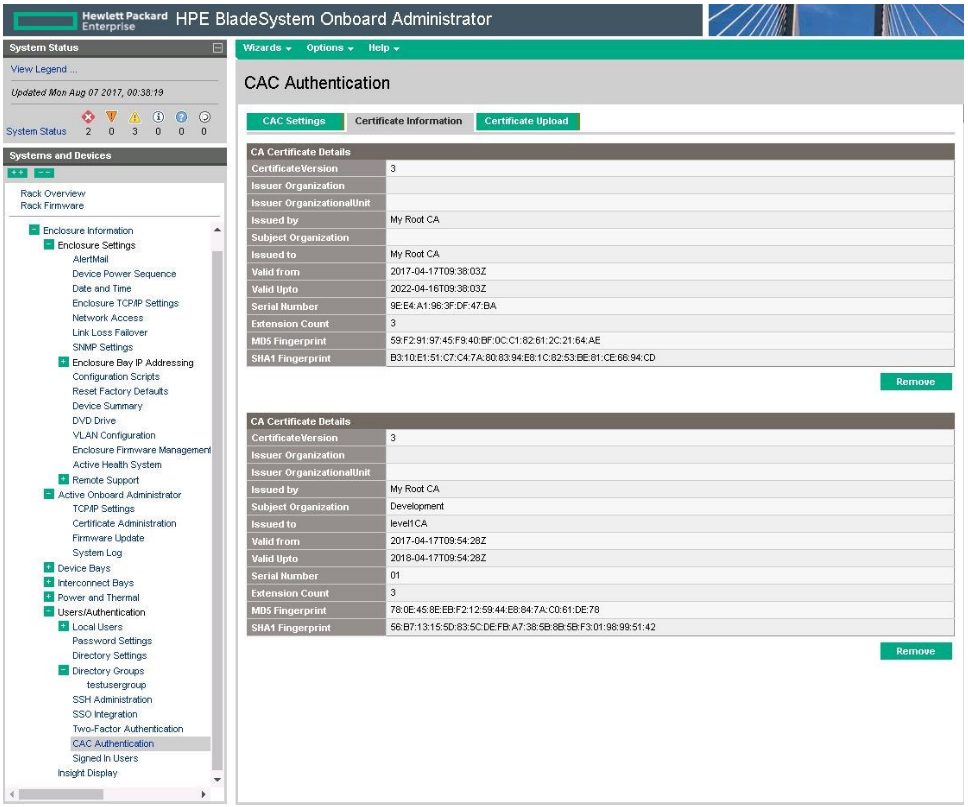
X.509 Certificate Upload: *You may paste the contents of an X.509 certificate into the textbox below for upload.*

Download from URL: *Provide the URL to an X.509 certificate file accessible by the Onboard Administrator. The certificate will be downloaded and installed automatically.*

URL:

Alternately, certificate can also be uploaded by providing the URL .

After successfully uploading a certificate , certificate details can be seen at "Certificate Information" tab.



Updated Mon Aug 07 2017, 00:38:19

CAC Authentication

CA Certificate Details	
CertificateVersion	3
Issuer Organization	
Issuer OrganizationalUnit	
Issued by	My Root CA
Subject Organization	
Issued to	My Root CA
Valid from	2017-04-17T09:38:03Z
Valid Upto	2022-04-16T09:38:03Z
Serial Number	9E:E4:A1:96:3F:DF:47:BA
Extension Count	3
MD5 Fingerprint	59:F2:91:97:45:F9:40:BF:0C:C1:82:61:2C:21:64:AE
SHA1 Fingerprint	B3:10:E1:51:C7:C4:7A:80:83:94:E8:1C:82:53:BE:81:CE:66:94:CD

CA Certificate Details	
CertificateVersion	3
Issuer Organization	
Issuer OrganizationalUnit	
Issued by	My Root CA
Subject Organization	Development
Issued to	level1CA
Valid from	2017-04-17T09:54:28Z
Valid Upto	2018-04-17T09:54:28Z
Serial Number	01
Extension Count	3
MD5 Fingerprint	78:0E:45:8E:EB:F2:12:59:44:E8:84:7A:C0:61:DE:78
SHA1 Fingerprint	56:B7:13:15:5D:83:5C:DE:FB:A7:38:5B:8B:5B:F3:01:98:99:51:42

The following command line commands can be used for LDAP configuration:

```
SET LDAP SERVICE_ACCOUNT { NONE | "<user name>" ["<password>"] }
```

```
ENABLE LDAP SERVICE_ACCOUNT
```

```
DISABLE LDAP SERVICE_ACCOUNT
```

```
ADD LDAP GROUP "<group name>"
```

```
ENABLE LDAP
```

```
SET LDAP SERVICE
```

```
SET LDAP PORT
```

The following command line commands are useful for certificate administration:

```
ADD CA CERTIFICATE
```

```
DOWNLOAD CA CERTIFICATE {url}
```

```
SHOW CA CERTIFICATE
```

```
REMOVE CA CERTIFICATE "fingerprint"
```

Configure HTTP proxy on the OA

If the OA requires a proxy server to reach addresses such those needed to verify a certificate or obtain a certificate revocation list, then it will be necessary to configure the HTTP Proxy server setting on the OA with this command:

```
SET URB PROXY URL { <url> }
```

There is no corresponding command in the web GUI to set a proxy URL.

Enabling CAC Authentication for local user-prerequisites

Below Prerequisites should be met to enable CAC :

1. Install CA chain

   The certificate authorities for CAC and LDAP are separate repositories on the OA and the certificate need to be installed in corresponding repositories.

   To install a CA certificate on the GUI, navigate to **Enclosure Information** > **Users/Authentication** > **CAC Authentication** , then click on the "Certificate Upload" tab. Copy and paste the root CA certificate into the **x.509 certificate upload** text box. The certificate includes begin and end tags as shown:

   ```
   -----BEGIN CERTIFICATE-----
   MIIDkTCCAnmgAwIBAgIJALg8cO2Ikvr8MA0GCSqGSIb3DQEBBQUAMDkxDDAKBgNV
   BAMTA2NhMDEUMBIGCgmSJomT8ixkARkWBHRlc3QxEzARBgoJkiaJk/IsZAEZFgNj
   . . . . .
   Ob6IFCSUTKbCVT95cYTRHiSbgBYaqDXBJk3Lyjvtb7ZovmMT5dnU/w061wV5MEce
   RZfXH3U=
   -----END CERTIFICATE-----
   ```

   The following CLI commands are useful for certificate administration:

   ```
   ADD CA CERTIFICATE
   ```

   ```
   DOWNLOAD CA CERTIFICATE {URL}
   ```

   ```
   SHOW CA CERTIFICATE
   ```

   ```
   REMOVE CA CERTIFICATE "fingerprint"
   ```

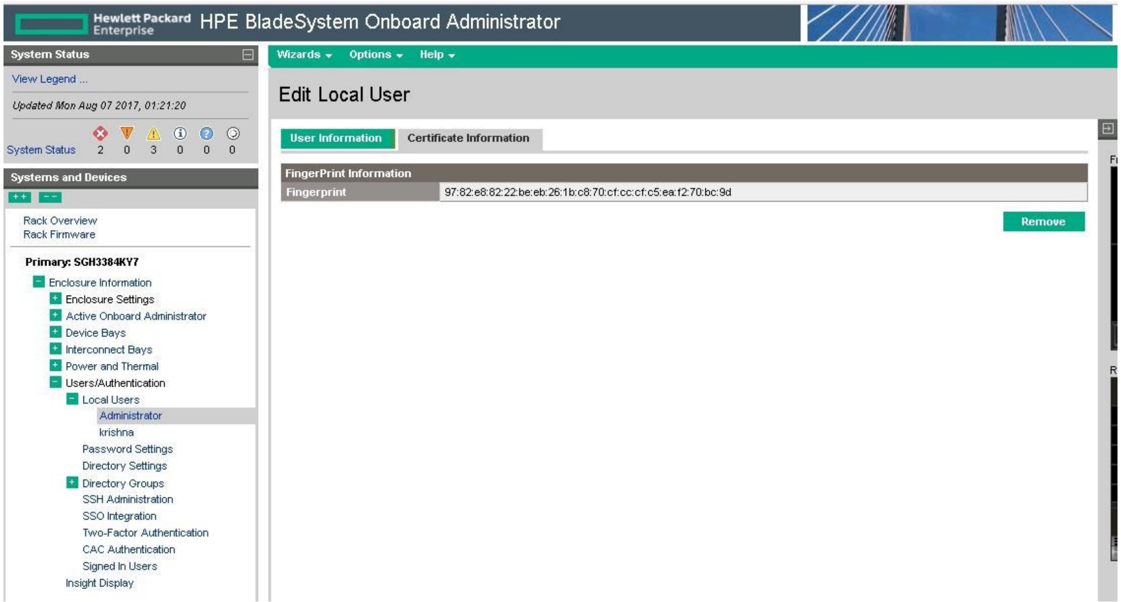
   Configuring HTTP proxy on the OA

If the OA requires a proxy server to reach addresses such those needed to verify a certificate or obtain a certificate revocation list, then it will be necessary to configure the HTTP Proxy server setting on the OA with this command:

```
SET URB PROXY URL { <url> }
```

There is no corresponding command in the web GUI to set a proxy URL.

2. Install User certificate on the OA Local Administrator Account .



Edit Local User

FingerPrint Information

Fingerprint 97:82:e8:82:22:be:eb:26:1b:c8:70:cf:cc:cf:c5:ea:f2:70:bc:9d

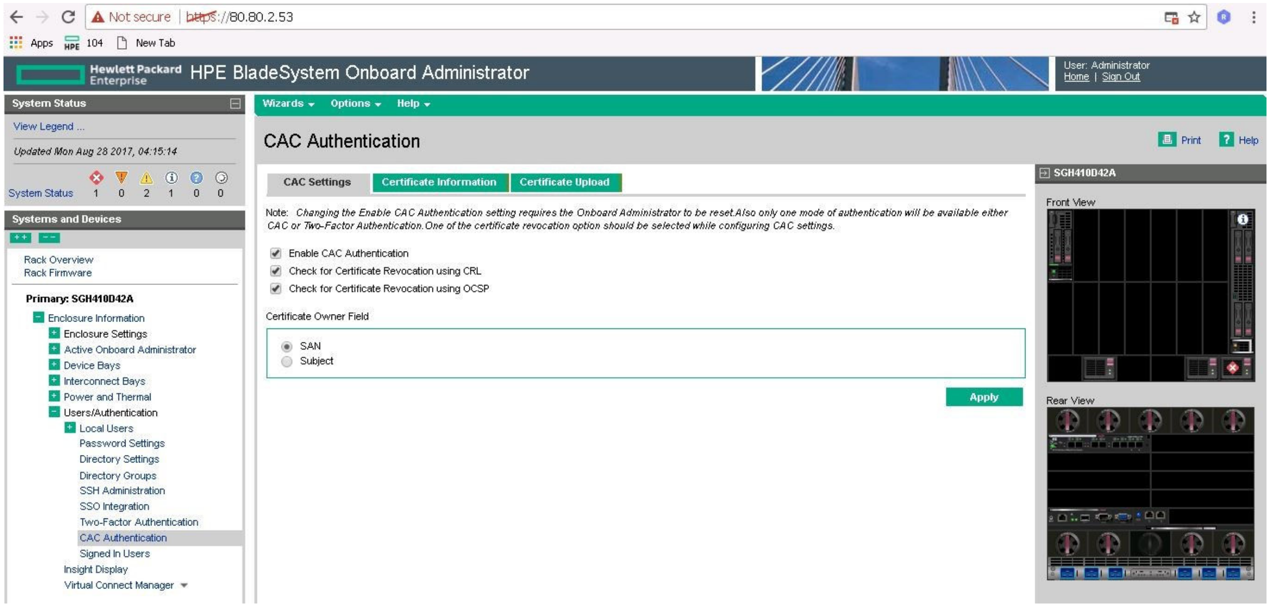
Below command line command can also be used for installing user certificates.

```
DOWNLOAD USER CERTIFICATE "<user_name>" <url>
```

Enable CAC Authentication

CAC Authentication may be enabled after the prerequisites are met for the LDAP user or the local user. While enabling CAC Authentication, it is always recommended to configure local administrator account with certificates so that it enables local administrator to recover OA in case of any LDAP configuration issues.

To enable CAC, navigate to **Enclosure Information** > **Users/Authentication** > **CAC Authentication**.



CAC Authentication

Note: *Changing the Enable CAC Authentication setting requires the Onboard Administrator to be reset.Also only one mode of authentication will be available either CAC or Two-Factor Authentication.One of the certificate revocation option should be selected while configuring CAC settings.*

☑ Enable CAC Authentication
☑ Check for Certificate Revocation using CRL
☑ Check for Certificate Revocation using OCSP

Certificate Owner Field

● SAN
○ Subject

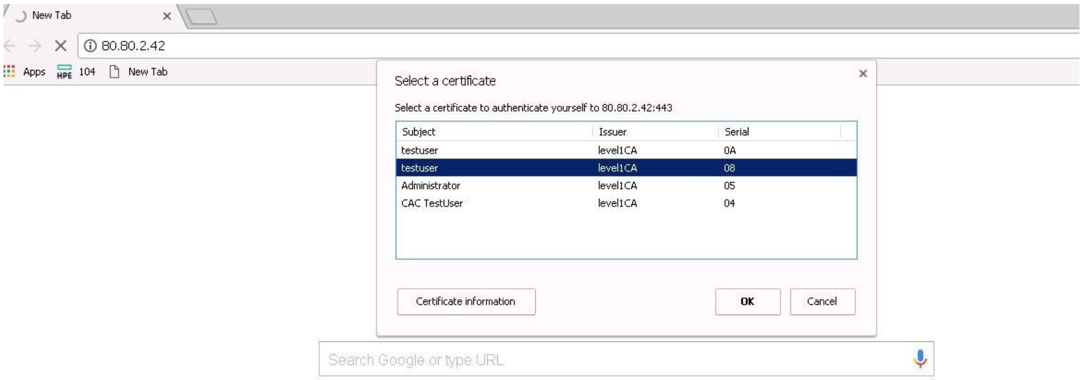
The "Certificate Owner Field" is used if CAC is used in combination with LDAP. It instructs the OA to use the certificate subject ("Subject.CN") field or a subject alternative name field as the user's LDAP username.

Certificate revocation check method should be selected as either by CRL or OCSP.

After clicking Apply, the OA will reboot with the new settings.

OA Web Login using CAC for LDAP user

Browse to the Onboard Administrators web GUI. The browser should first ask permission to use a certificate. This is needed to establish an SSL/TLS session to the OA .

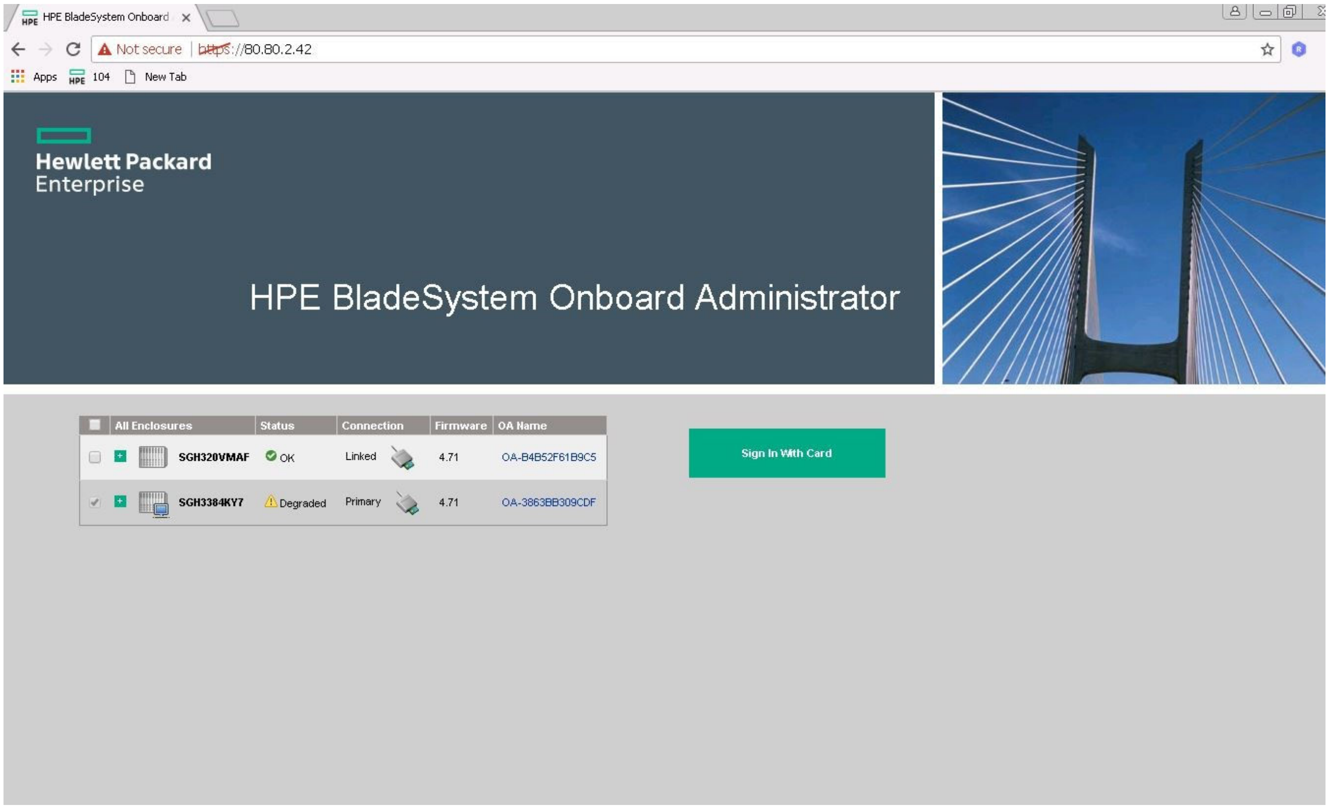


Select a certificate

Select a certificate to authenticate yourself to 80.80.2.42:443

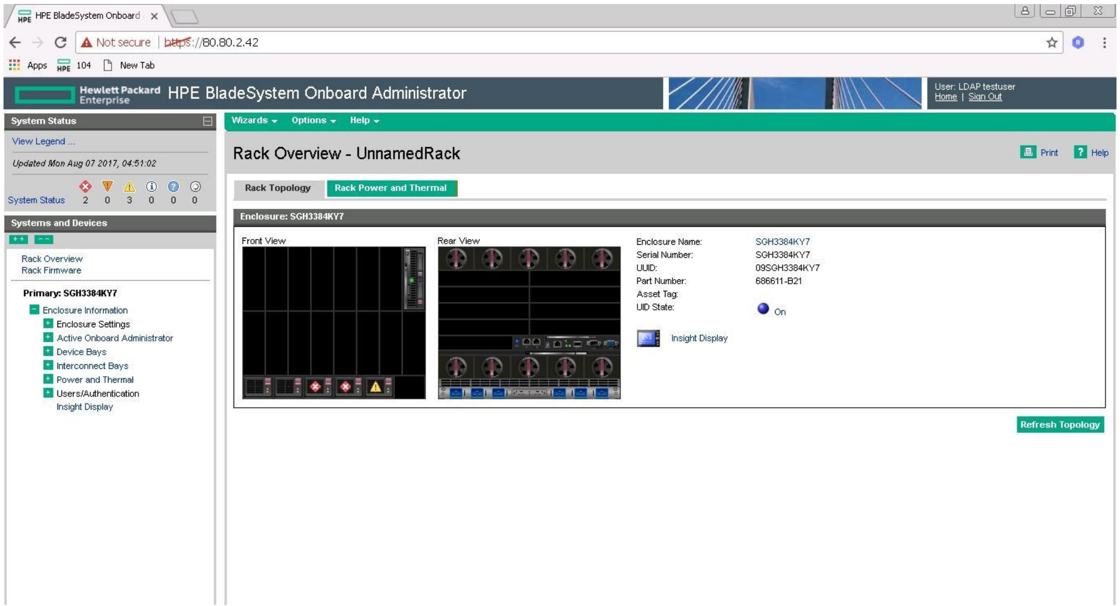
Subject	Issuer	Serial
testuser	level1CA	0A
testuser	level1CA	08
Administrator	level1CA	05
CAC TestUser	level1CA	04

If the certificate is validated successfully, OA login page with "Sign in with card" button is launched. Clicking on this button will initiate the LDAP verification of the user.



□	All Enclosures	Status	Connection	Firmware	OA Name
□	SGH320VMAF	✓ OK	Linked	4.71	OA-B4B52F61B9C5
☑	SGH3384KY7	⚠ Degraded	Primary	4.71	OA-3863BB309CDF

After the successful authentication of user with LDAP server, OA authentication will be completed and home page will be launched.



HPE BladeSystem Onboard Administrator

User: LDAP testuser
Home | Sign Out

System Status
View Legend ...
Updated Mon Aug 07 2017, 04:51:02
System Status 2 0 3 0 0 0

Systems and Devices
Rack Overview
Rack Firmware
Primary: SGH3384KY7
Enclosure Information
Enclosure Settings
Active Onboard Administrator
Device Bays
Interconnect Bays
Power and Thermal
Users/Authentication
Insight Display

Rack Overview - UnnamedRack

Rack Topology | Rack Power and Thermal

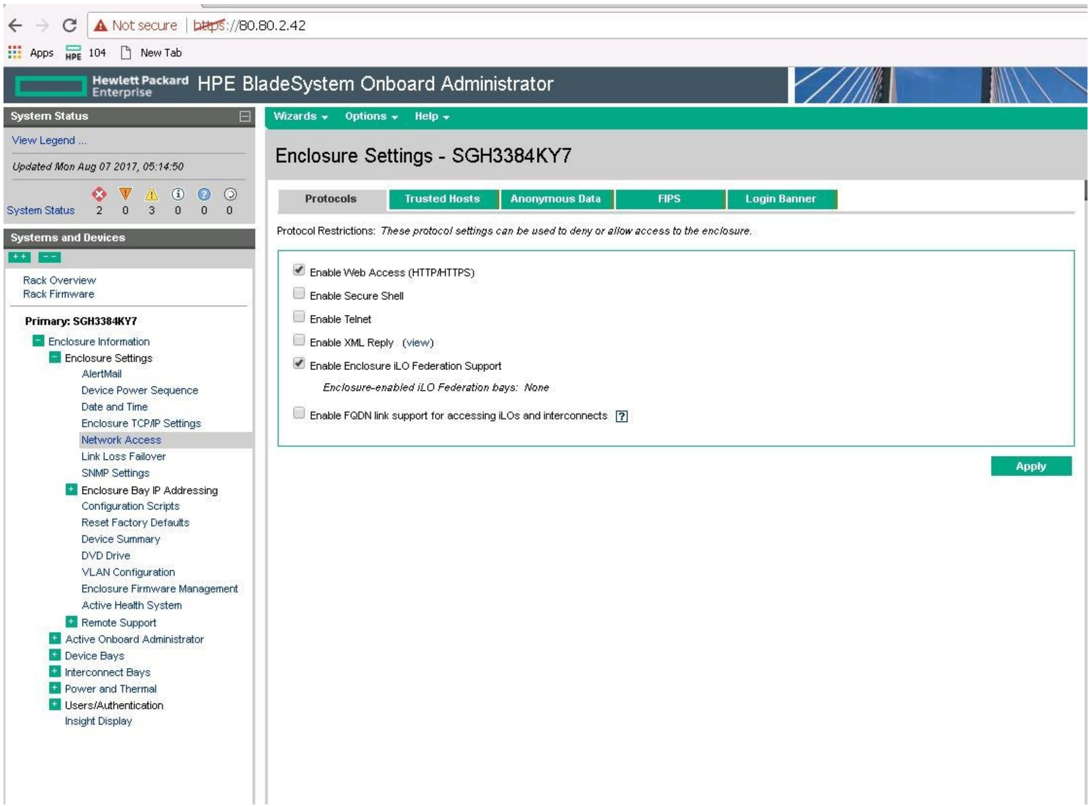
Enclosure: SGH3384KY7

Front View | Rear View

Enclosure Name:	SGH3384KY7
Serial Number:	SGH3384KY7
UUID:	09SGH3384KY7
Part Number:	686611-B21
Asset Tag:	
UID State:	On

Insight Display

When CAC authentication is enabled, SSH, TELNET and XMLReply are disabled by default. However SSH and Telnet can be enabled by the user in protocols tab of **Enclosure Information** > **Enclosure Settings** > **Network Access page** . XMLReply cannot be enabled in CAC Authentication mode.



HPE BladeSystem Onboard Administrator

System Status
View Legend ...
Updated Mon Aug 07 2017, 05:14:50
System Status 2 0 3 0 0 0

Systems and Devices
Rack Overview
Rack Firmware
Primary: SGH3384KY7
Enclosure Information
Enclosure Settings
AlertMail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
Configuration Scripts
Reset Factory Defaults
Device Summary
DVD Drive
VLAN Configuration
Enclosure Firmware Management
Active Health System
Remote Support
Active Onboard Administrator
Device Bays
Interconnect Bays
Power and Thermal
Users/Authentication
Insight Display

Enclosure Settings - SGH3384KY7

Protocols | Trusted Hosts | Anonymous Data | FIPS | Login Banner

Protocol Restrictions: *These protocol settings can be used to deny or allow access to the enclosure.*

☑ Enable Web Access (HTTP/HTTPS)
☐ Enable Secure Shell
☐ Enable Telnet
☐ Enable XML Reply (view)
☑ Enable Enclosure iLO Federation Support
Enclosure-enabled iLO Federation bays: None
☐ Enable FQDN link support for accessing iLOs and interconnects

These protocols can also be enabled through command line options:

```
ENABLE SSH
```

```
ENABLE TELNET
```

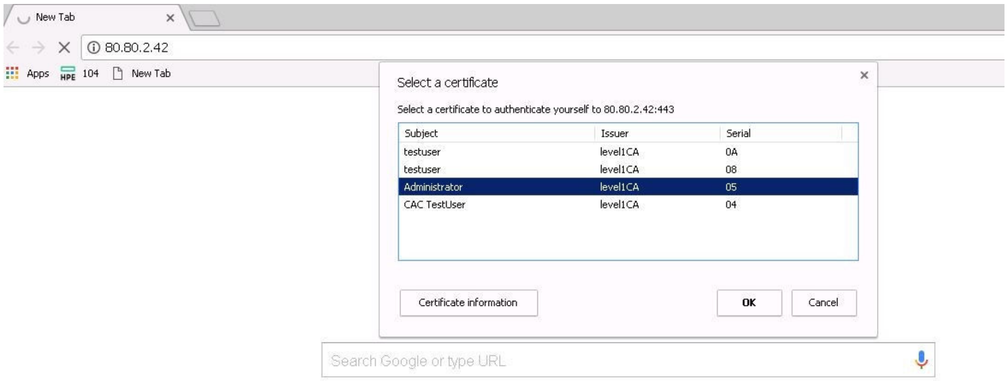
CAC setting can also be viewed from command line using following command:

```
SHOW CAC INFO
```

OA Web Login using CAC for local user

Browse to the Onboard Administrators web GUI. The browser should first ask permission to use a certificate. This is needed to establish a SSL/TLS session to the OA after which it will be used to authenticate the OA and home page will be opened.

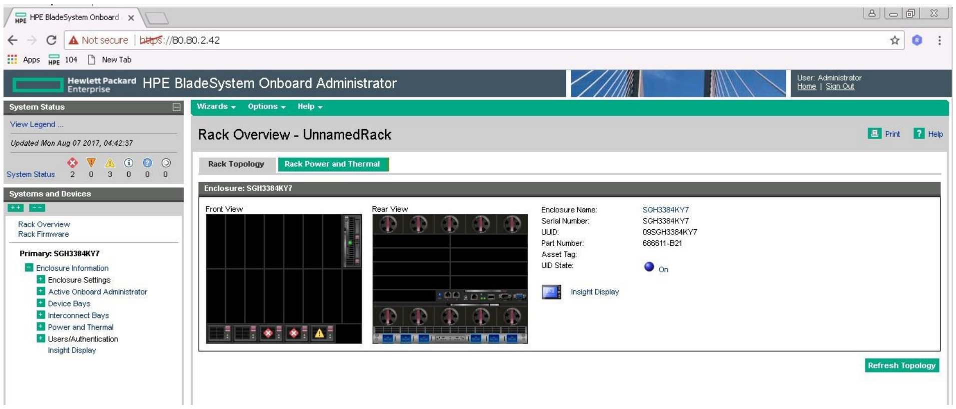
NOTE: The OA login page will not be shown in this case.



Select a certificate

Select a certificate to authenticate yourself to 80.80.2.42:443

Subject	Issuer	Serial
testuser	level1CA	0A
testuser	level1CA	08
Administrator	level1CA	05
CAC TestUser	level1CA	04



Updated Mon Aug 07 2017, 04:42:37

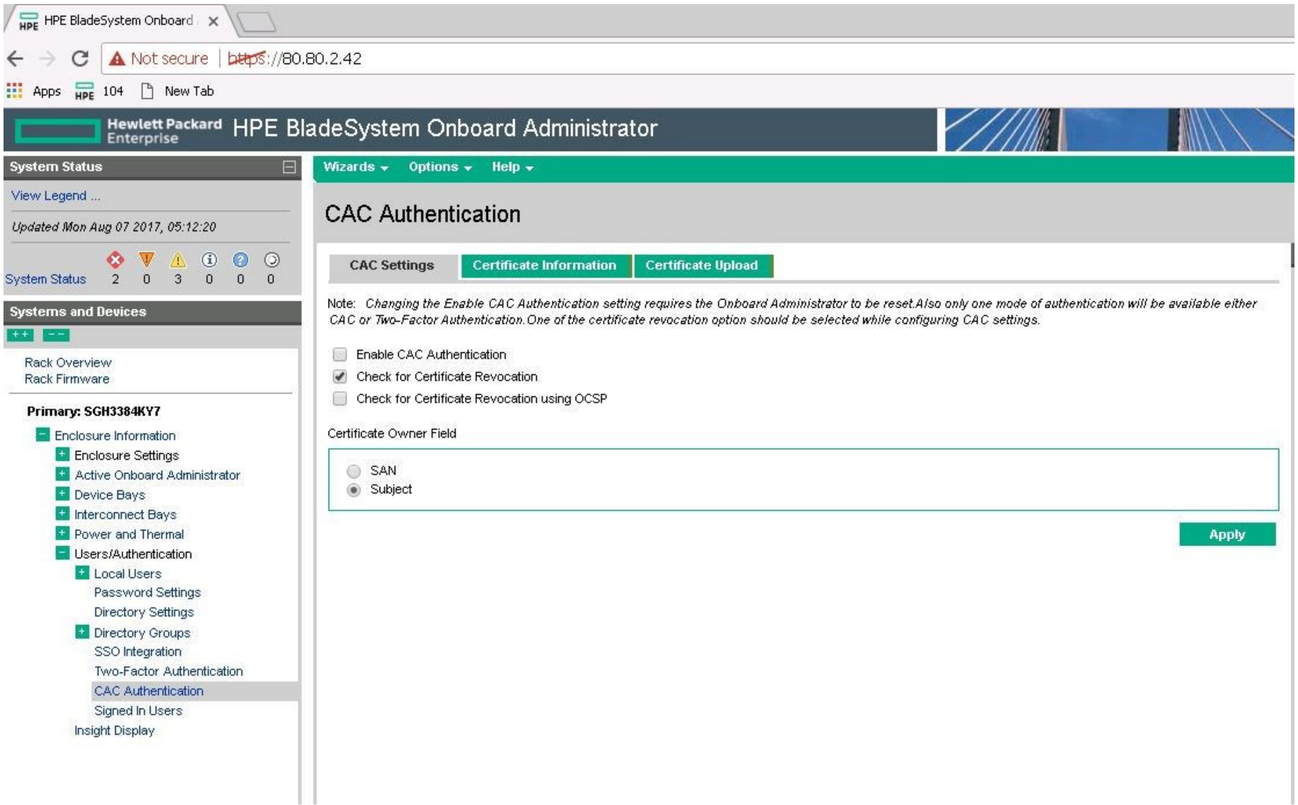
Rack Overview - UnnamedRack

Enclosure: SGH3384KY7

Enclosure Name:	SGH3384KY7
Serial Number:	SGH3384KY7
UUID:	09SGH3384KY7
Part Number:	686611-B21
Asset Tag:	
UID State:	On

Disable CAC Authentication

To disable CAC Authentication from Web GUI, navigate to **Enclosure Information** > **Users/Authentication** > **CAC Authentication** , uncheck Enable CAC Authentication box and click on Apply button. OA will reboot with the new settings.



CAC Authentication

Note: *Changing the Enable CAC Authentication setting requires the Onboard Administrator to be reset.Also only one mode of authentication will be available either CAC or Two-Factor Authentication.One of the certificate revocation option should be selected while configuring CAC settings.*

☐ Enable CAC Authentication
☑ Check for Certificate Revocation
☐ Check for Certificate Revocation using OCSP

Certificate Owner Field

○ SAN
● Subject

The following CLI commands can also be used for disabling CAC, CRL & OCSP:

```
DISABLE CAC
```

```
DISABLE OCSP
```

```
DISABLE CRL
```

Time zone settings

Universal time zone settings

IMPORTANT:
Time zones must be entered exactly as they appear.

The following table provides the Universal time zone settings that are supported by the Onboard Administrator.

CET	Etc/GMT+2	Etc/GMT+8	Etc/UCT	MST
CST6CDT	Etc/GMT-3	Etc/GMT-9	Etc/Universal	MST7MDT
EET	Etc/GMT+3	Etc/GMT+9	Etc/UTC	Navajo
EST	Etc/GMT-4	Etc/GMT-10	Etc/Zulu	PST8PDT
EST5EDT	Etc/GMT+4	Etc/GMT+10	Factory	UCT
Etc/GMT	Etc/GMT-5	Etc/GMT-11	GMT	Universal
Etc/GMT0	Etc/GMT+5	Etc/GMT+11	GMT+0	UTC
Etc/GMT-0	Etc/GMT-6	Etc/GMT-12	GMT0	WET
Etc/GMT+0	Etc/GMT+6	Etc/GMT+12	GMT-0	W-SU
Etc/GMT-1	Etc/GMT-7	Etc/GMT-13	Greenwich	Zulu
Etc/GMT+1	Etc/GMT+7	Etc/GMT-14	HST	—
Etc/GMT-2	Etc/GMT-8	Etc/Greenwich	MET	—

Africa time zone settings

IMPORTANT:
Time zones must be entered exactly as they appear.

The following table provides the African time zone settings that are supported by the Onboard Administrator.

Africa/Abidjan	Africa/Ceuta	Africa/Kinshasa	Africa/Niamey
Africa/Accra	Africa/Conakry	Africa/Lagos	Africa/Nouakchott
Africa/Addis_Ababa	Africa/Dakar	Africa/Libreville	Africa/Ouagadougou
Africa/Algiers	Africa/Dar_es_Salaam	Africa/Lome	Africa/Porto-Novo
Africa/Asmara	Africa/Djibouti	Africa/Luanda	Africa/Sao_Tome
Africa/Asmera	Africa/Douala	Africa/Lubumbashi	Africa/Timbuktu
Africa/Bamako	Africa/El_Aaiun	Africa/Lusaka	Africa/Tripoli
Africa/Bangui	Africa/Freetown	Africa/Malabo	Africa/Tunis
Africa/Banjul	Africa/Gaborone	Africa/Maputo	Africa/Wjndhoek
Africa/Bissau	Africa/Harare	Africa/Maseru	Egypt
Africa/Blantyre	Africa/Johannesburg	Africa/Mbabane	Libya

Table Continued

AfricaBrazzaville	Africa/Juba	Africa/Mogadishu	—
Africa/Bujumbura	Africa/Kampala	Africa/Monrovia	—
Africa/Cairo	Africa/Khartoum	Africa/Nairobi	—
Africa/Casablanca	Africa/Kigali	Africa/Ndjamena	—

Americas time zone settings

IMPORTANT:
Time zones must be entered exactly as they appear.

The following table provides the Americas time zone settings that are supported by the Onboard Administrator.

America/Adak	America/Guatemala	America/Rainy_River
America/Anchorage	America/Guayaquil	America/Rankin_Inlet
America/Anguilla	America/Guyana	America/Recife
America/Antigua	America/Halifax	America/Regina
America/Araguaina	America/Havana	America/Resolute
America/Argentina/Buenos_Aires	America/Hermosillo	America/Rio_Branco
America/Argentina/Catamarca	America/Indiana/Indianapolis	America/Rosario
America/Argentina/ComodRivadavia	America/Indiana/Knox	America/Santa_Isabel
America/Argentina/Cordoba	America/Indiana/Marengo	America/Santarem
America/Argentina/Jujuy	America/Indiana/Petersburg	America/Santiago
America/Argentina/La_Rioja	America/Indiana/Tell_City	America/Santo_Domingo
America/Argentina/Mendoza	America/Indiana/Vevay	America/Sao_Paulo
America/Argentina/Rio_Gallegos	America/Indiana/Vincennes	America/Scoresbysund
America/Argentina/Salta	America/Indiana/Winamac	America/Shiprock
America/Argentina/San_Juan	America/Indianapolis	America/Sitka
America/Argentina/San_Luis	America/Inuvik	America/St_Barthelemy
America/Argentina/Tucuman	America/Iqaluit	America/St_Johns
America/Argentina/Ushuaia	America/Jamaica	America/St_Kitts
America/Aruba	America/Jujuy	America/St_Lucia
America/Asuncion	America/Juneau	America/St_Thomas
America/Atikokan	America/Kentucky/Louisville	America/St_Vincent
America/Atka	America/Kentucky/Monticello	America/Swift_Current
America/Bahia	America/Knox_IN	America/Tegucigalpa
America/Bahia_Banderas	America/Kralendijk	America/Thule
America/Barbados	America/La_Paz	America/Thunder_Bay

Table Continued

America/Belem	America/Lima	America/Tijuana
America/Belize	America/Los_Angeles	America/Toronto
America/Blanc-Sablon	America/Louisville	America/Tortola
America/Boa_Vista	America/Lower_Princes	America/Vancouver
America/Bogota	America/Maceio	America/Virgin
America/Boise	America/Managua	America/Whitehorse
America/Buenos_Aires	America/Manaus	America/Winnipeg
America/Cambridge_Bay	America/Marigot	America/Yakutat
America/Campo_Grande	America/Martinique	America/Yellowknife
America/Cancun	America/Matamoros	Brazil/Acre
America/Caracas	America/Mazatlan	Brazil/DeNoronha
America/Catamarca	America/Mendoza	Brazil/East
America/Cayenne	America/Menominee	Brazil/West
America/Cayman	America/Merida	Canada/Atlantic
America/Chicago	America/Metlakatla	Canada/Central
America/Chihuahua	America/Mexico_City	Canada/Eastern
America/Coral_Harbour	America/Miquelon	Canada/East-Saskatchewan
America/Cordoba	America/Moncton	Canada/Mountain
America/Costa_Rica	America/Monterrey	Canada/Newfoundland
America/Creston	America/Montevideo	Canada/Pacific
America/Cuiaba	America/Montreal	Canada/Saskatchewan
America/Curacao	America/Montserrat	Canada/Yukon
America/Danmarkshavn	America/Nassau	Chile/Continental
America/Dawson	America/New_York	Chile/EasterIsland
America/Dawson_Creek	America/Nipigon	Cuba
America/Denver	America/Nome	Jamaica
America/Detroit	America/Noronha	Mexico/BajaNorte
America/Dominica	America/North_Dakota/Beulah	Mexico/BajaSur
America/Edmonton	America/North_Dakota/Center	Mexico/General
America/Eirunepe	America/North_Dakota/New_Salem	US/Alaska
America/El_Salvador	America/Ojinaga	US/Aleutian
America/Ensenada	America/Panama	US/Arizona
America/Fort_Wayne	America/Pangnirtung	US/Central
America/Fortaleza	America/Paramaribo	US/Eastern
America/Glace_Bay	America/Phoenix	US/East-Indiana
America/Godthab	America/Port_of_Spain	US/Indiana-Starke

Table Continued

America/Goose_Bay	America/Port-au-Prince	US/Michigan
America/Grand_Turk	America/Porto_Acre	US/Mountain
America/Grenada	America/Porto_Velho	US/Pacific
America/Guadeloupe	America/Puerto_Rico	US/Pacific-New

Asia time zone settings

IMPORTANT:
Time zones must be entered exactly as they appear.

The following table provides the Asian time zone settings that are supported by the Onboard Administrator.

Asia/Aden	Asia/Dhaka	Asia/Khandyga	Asia/Qyzylorda	Asia/Ulaanbaatar
Asia/Almaty	Asia/Dili	Asia/Kolkata	Asia/Rangoon	Asia/Ulan_Bator
Asia/Amman	Asia/Dubai	Asia/Krasnoyarsk	Asia/Riyadh	Asia/Urumqi
Asia/Anadyr	Asia/Dushanbe	Asia/Kuala_Lumpur	Asia/Riyadh87	Asia/Ust-Nera
Asia/Aqtau	Asia/Gaza	Asia/Kuching	Asia/Riyadh88	Asia/Vientiane
Asia/Aqtobe	Asia/Harbin	Asia/Kuwait	Asia/Riyadh89	Asia/Vladivostok
Asia/Ashgabat	Asia/Hebron	Asia/Macao	Asia/Saigon	Asia/Yakutsk
Asia/Ashkhabad	Asia/Ho_Chi_Minh	Asia/Macau	Asia/Sakhalin	Asia/Yekaterinburg
Asia/Baghdad	Asia/Hong_Kong	Asia/Magadan	Asia/Samarkand	Asia/Yerevan
Asia/Bahrain	Asia/Hovd	Asia/Makassar	Asia/Seoul	Hongkong
Asia/Baku	Asia/Irkutsk	Asia/Manila	Asia/Shanghai	Iran
Asia/Bangkok	Asia/Istanbul	Asia/Muscat	Asia/Singapore	Israel
Asia/Beirut	Asia/Jakarta	Asia/Nicosia	Asia/Taipei	Japan
Asia/Bishkek	Asia/Jayapura	Asia/Novokuznetsk	Asia/Tashkent	Mideast/Riyadh87
Asia/Brunei	Asia/Jerusalem	Asia/Novosibirsk	Asia/Tbilisi	Mideast/Riyadh88
Asia/Choibalsan	Asia/Kabul	Asia/Omsk	Asia/Tehran	Mideast/Riyadh89
Asia/Chongqing	Asia/Kamchatka	Asia/Oral	Asia/Tel_Aviv	PRC
Asia/Chungking	Asia/Karachi	Asia/Phnom_Penh	Asia/Thimbu	ROC
Asia/Colombo	Asia/Kashgar	Asia/Pontianak	Asia/Thimphu	ROK
Asia/Dacca	Asia/Kathmandu	Asia/Pyongyang	Asia/Tokyo	Singapore
Asia/Damascus	Asia/Katmandu	Asia/Qatar	Asia/ Ujung_Pandang	Turkey

Oceanic time zone settings

IMPORTANT:
Time zones must be entered exactly as they appear.

The following table provides the Oceanic time zone settings that are supported by the Onboard Administrator.

Atlantic/Azores	Australia/Melbourne	Kwajalein	Pacific/Marquesas
Atlantic/Bermuda	Australia/North	NZ	Pacific/Midway
Atlantic/Canary	Australia/NSW	NZ-CHAT	Pacific/Nauru
Atlantic/Cape_Verde	Australia/Perth	Pacific/Apia	Pacific/Niue
Atlantic/Faeroe	Australia/Queensland	Pacific/Auckland	Pacific/Norfolk
Atlantic/Jan_Mayen	Australia/South	Pacific/Chatham	Pacific/Noumea
Atlantic/Madeira	Australia/Sydney	Pacific/Chuuk	Pacific/Pago_Pago
Atlantic/Reykjavik	Australia/Tasmania	Pacific/Easter	Pacific/Palau
Atlantic/South_Georgia	Australia/Victoria	Pacific/Efate	Pacific/Pitcairn
Atlantic/St_Helena	Australia/West	Pacific/Enderbury	Pacific/Pohnpei
Atlantic/Stanley	Australia/Yancowinna	Pacific/Fakaofo	Pacific/Ponape
Australia/ACT	Iceland	Pacific/Fiji	Pacific/Port_Moresby
Australia/Adelaide	Indian/Antananarivo	Pacific/Funafuti	Pacific/Rarotonga
Australia/Brisbane	Indian/Chagos	Pacific/Galapagos	Pacific/Saipan
Australia/Broken_Hill	Indian/Christmas	Pacific/Gambier	Pacific/Samoa
Australia/Canberra	Indian/Cocos	Pacific/Guadalcanal	Pacific/Tahiti
Australia/Currie	Indian/Comoro	Pacific/Guam	Pacific/Tarawa
Australia/Darwin	Indian/Kerguelen	Pacific/Honolulu	Pacific/Tongatapu
Australia/Eucla	Indian/Mahe	Pacific/Johnston	Pacific/Truk
Australia/Hobart	Indian/Maldives	Pacific/Kiritimati	Pacific/Wake
Australia/LHI	Indian/Mauritius	Pacific/Kosrae	Pacific/Wallis
Australia/Lindeman	Indian/Mayotte	Pacific/Kwajalein	Pacific/Yap
Australia/Lord_Howe	Indian/Reunion	Pacific/Majuro	US/Hawaii
—	—	—	US/Samoa

Europe time zone settings

IMPORTANT:
Time zones must be entered exactly as they appear.

The following table provides the European time zone settings that are supported by the Onboard Administrator.

Eire	Europe/Kaliningrad	Europe/Sarajevo
Europe/Amsterdam	Europe/Kiev	Europe/Simferopol
Europe/Andorra	Europe/Lisbon	Europe/Skopje
Europe/Athens	Europe/Ljubljana	Europe/Sofia
Europe/Belfast	Europe/London	Europe/Stockholm
Europe/Belgrade	Europe/Luxembourg	Europe/Tallinn

Table Continued

Europe/Berlin	Europe/Madrid	Europe/Tirane
Europe/Bratislava	Europe/Malta	Europe/Tiraspol
Europe/Brussels	Europe/Mariehamn	Europe/Uzhgorod
Europe/Bucharest	Europe/Minsk	Europe/Vaduz
Europe/Budapest	Europe/Monaco	Europe/Vatican
Europe/Busingen	Europe/Moscow	Europe/Vienna
Europe/Chisinau	Europe/Nicosia	Europe/Vilnius
Europe/Copenhagen	Europe/Oslo	Europe/Volgograd
Europe/Dublin	Europe/Paris	Europe/Warsaw
Europe/Gibraltar	Europe/Podgorica	Europe/Zagreb
Europe/Guernsey	Europe/Prague	Europe/Zaporozhye
Europe/Helsinki	Europe/Riga	Europe/Zurich
Europe/Isle_of_Man	Europe/Rome	GB
Europe/Istanbul	Europe/Samara	GB-Eire
Europe/Jersey	Europe/San_Marino	Poland
—	—	Portugal

Polar time zone settings

IMPORTANT:
Time zones must be entered exactly as they appear.

The following table provides the Polar time zone settings that are supported by the Onboard Administrator.

Antarctica/Casey	Antarctica/Mawson	Antarctica/South_Pole
Antarctica/Davis	Antarctica/McMurdo	Antarctica/Syowa
Antarctica/DumontDUrville	Antarctica/Palmer	Antarctica/Vostok
Antarctica/Macquarie	Antarctica/Rothera	Arctic/Longyearbyen

Acronyms and abbreviations

CA

certificate authority

CRL

certificate revocation list

CSR

certificate signing request

DC

domain controller

DCC

device control channel

DHCP

Dynamic Host Configuration Protocol

DN

distinguished name

DNS

domain name system

EBIPA

Enclosure Bay IP Addressing

EDPC

Enclosure Dynamic Power Capping

EEPROM

electrical erasable programmable read only memory

EFM

Enclosure Firmware Management

ext2

second extended file system

FAT32

File Allocation Table with cluster values represented by 32-bit numbers

FIPS

Federal Information Processing Standard

FQDN

Fully Qualified Domain Name

FRU

field replaceable unit

GC

global catalog

HPESC

Hewlett Packard Enterprise Support Center

HTTPS

hypertext transfer protocol secure sockets

I2C

inter-integrated circuit

iLO

Integrated Lights-Out

KVM

keyboard, video, and mouse

LDAP

Lightweight Directory Access Protocol

LOM

LAN on Motherboard

MAC

Media Access Control

MMC

Microsoft Management Console

NTP

network time protocol

NVRAM

nonvolatile memory

PCI

payment card industry

PCIe

Peripheral Component Interconnect Express

PEM

Privacy Enhanced Mail

PIC

peripheral interface controller

PIN

Personal Identification Number

PKCS

Public-Key Cryptography Standards

PXE

preboot execution environment

RBSU

ROM-Based Setup Utility

RIBCL

Remote Insight Board Command Language

RPM

Red Hat Package Manager

RSA

Rivest, Shamir, and Adelman public encryption key

SAM

Security Account Manager

SAS

serial attached SCSI

SLAAC

stateless address autoconfiguration

SOAP

Simple Object Access Protocol

SSH

Secure Shell

SSL

Secure Sockets Layer

SUV

serial, USB, video

TFA

Two-Factor Authentication

TFTP

Trivial File Transfer Protocol

TLS

Transport Layer Security

TPM

Trusted Platform Module

UEFI

Unified Extensible Firmware Interface

UID

unit identification

VC

Virtual Connect

VCM

Virtual Connect Manager

VLAN

virtual local-area network

VM

Virtual Machine

VSP

virtual serial port

CAC

Common Access Card

DOD

United States Department of Defense

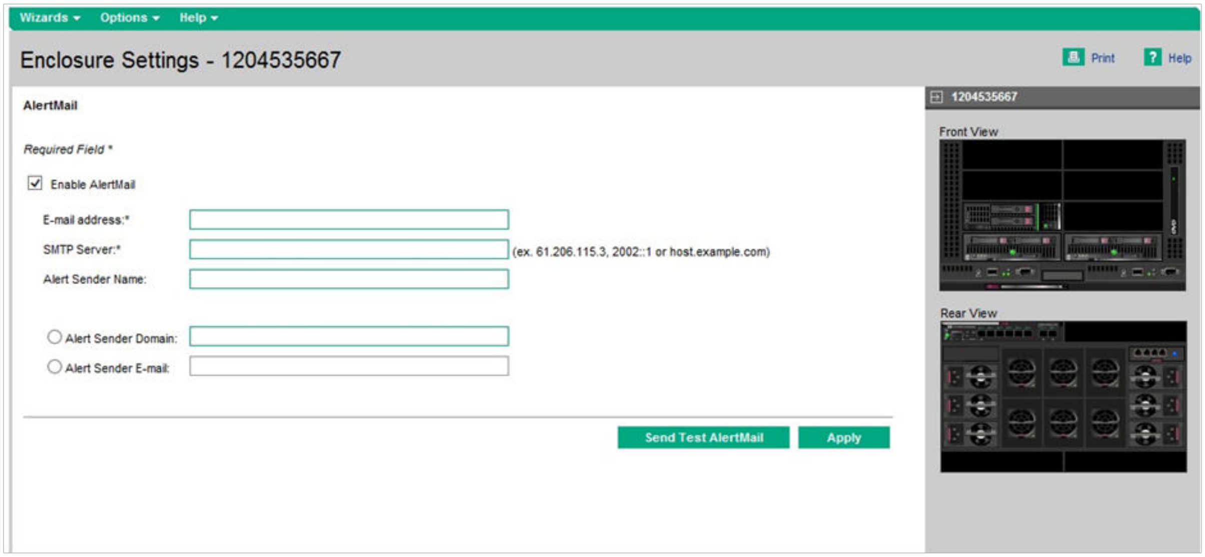
OCSP

Online Certificate Status Protocol

AlertMail

AlertMail enables users to receive system events by e-mail instead of using SNMP traps. AlertMail is completely independent from SNMP, and both can be enabled at the same time. AlertMail uses standard SMTP commands to communicate with an SMTP-capable mail server. The “reply to” address for each e-mail sent by AlertMail will be <Enclosure Name>@<Alert Sender Domain>. To enable the AlertMail feature, select the **Enable AlertMail** check box.

To test the AlertMail function, ensure that the email address, alert sender domain, and SMTP server settings are correct. Select **Send Test AlertMail**. To confirm the test completed successfully, verify the recipient email account.



Enclosure Settings - 1204535667

AlertMail

*Required Field **

☑ Enable AlertMail

E-mail address:*

SMTP Server:* (ex. 61.206.115.3, 2002::1 or host.example.com)

Alert Sender Name:

○ Alert Sender Domain:

○ Alert Sender E-mail:

NOTE:

The Alert Sender Domain might not be needed. This field depends on the mail server setup.

Field	Possible value	Description
E-Mail address	<account>@<domain>	A valid email address for the administrator or other designated individual receiving the alert mail
SMTP Server	• IPv4 address—###.###.###.### where ### ranges from 0 to 255 • IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. • DNS name—1 to 64 characters including all alphanumeric characters and the dash (-)	An IPv4 address, IPv6 address, or the DNS name for the SMTP server
Alert Sender Name	A character string including all alphanumeric characters, the dash (-), the underscore (_), and space. The field is optional with a limit of 40 characters.	Onboard Administrator name
Alert Sender Domain	A character string including all alphanumeric characters, the dash (-), and the period (.)	The domain in which the Onboard Administrator resides. Mutually exclusive with Sender Email.
Alert Sender E-mail	<account>@<domain>	Sender's valid email address for the administrator or other designated individual receiving the alert mail.

1. Select the **Enable AlertMail** checkbox to enable the AlertMail feature.
2. Enter values for the e-mail address, alert sender domain, and SMTP server.
3. Click **Apply** to save settings.

AlertMail, if enabled, sends alerts by e-mail for the following events:

- Enclosure status change
- Enclosure information change
- Fan status change
- Fan inserted
- Fan removed
- Power supply status
- Power supply inserted
- Power supply removed
- Power supply overload
- Blade inserted
- Blade removed
- Blade status
- Blade thermal condition
- Blade fault
- Blade information change
- Tray status change
- Tray reset

- Switch connect
- Switch disconnect

All e-mails have the following header:

From: Enclosure ENCLOSURE-NAME <enclosure-name@serverdomain>

Date: Date in standard format

Subject: HP AlertMail-SEQ: <SEVERITY> SUBJECT

To: RECEIVER MAILBOX

Where SEVERITY is one of the following (from highest to lowest):

- # FATAL
- # CRITICAL
- # WARNING MAJOR
- # WARNING MINOR
- # WARNING
- # NORMAL

Each subject line contains a unique sequence number to easily identify the order of events in case the mail server distributes them in the wrong order. Sequence numbers range from 0 to 999 and start again at 0.

The mail body is used to give more detailed information regarding the event issued. It also contains information on what the user should do to correct any issue and what the current enclosure status is.

> **NOTE:**
>
> The enclosure status is displayed as the status at the time the event was processed which can cause the status to show up as OK in an e-mail saying a Fan has Failed, if the user has already replaced the fan at the time the event was sent out by AlertMail.

Sample e-mail

Subject: HP AlertMail-010: (CRITICAL) Power Supply #1: Failed

Date: Wed, 23 Apr 2006 15:02:22 +0200

From: Enclosure EM-00508BEBA571 <EM-00508BEBA571@hp.com>

To: user@domain

X-OS: HP BladeSystem Enclosure Manager

X-Priority: 1

Content-Type: text/plain; charset=us-ascii

EVENT (26 May 07:09): Power Supply #1 Status has changed to: Failed.

Enclosure, EM-00508BEBA571, has detected that a power supply in bay 1 has changed from status OK to Failed.

The power supply should be replaced with the appropriate spare part. You can ensure that the center wall assembly is operating correctly by swapping the two power supplies. Make sure that there are no bent pins on the power supply connectors before reinserting and that each power supply is fully seated.

An amber LED on the power supply indicates either an over-voltage, over-temperature, or loss of AC power has occurred. A blinking LED on the power supply indicates a current limit condition.

Enclosure Status: Degraded

Enclosure Management URL: https://16.181.75.213/

- PLEASE DO NOT REPLY TO THIS EMAIL -