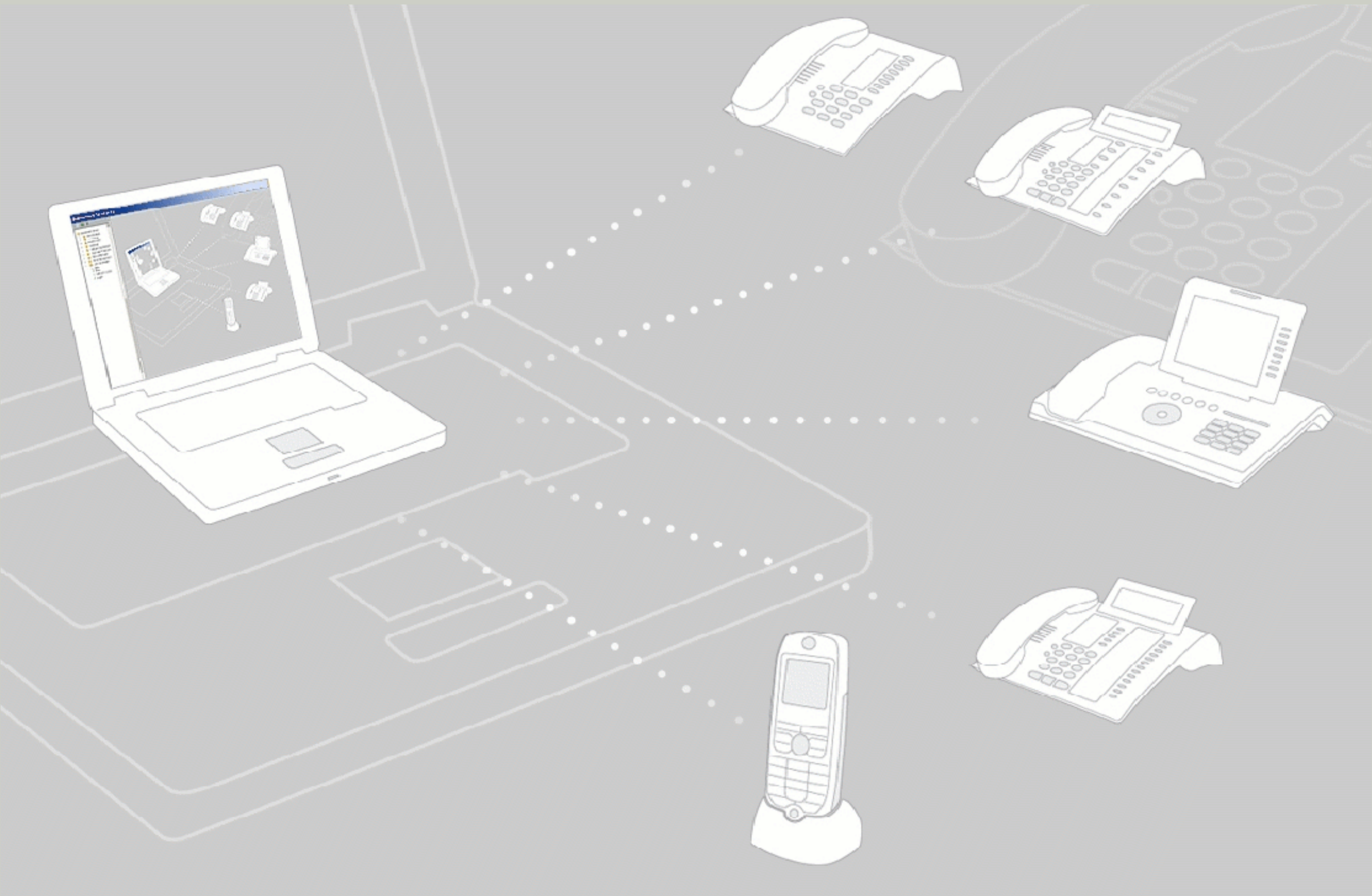
Documentation

OpenScape Deployment Service

Administration and Installation Manual

A31003-S2330-M100-9-76A9



Communication for the open minded

Siemens Enterprise Communications
www.siemens-enterprise.com

SIEMENS

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standard certified by an external certification company.

Reference No.: A31003-S2330-M100-9-76A9

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
OpenScape, OpenStage and HiPath are registered trademarks of Siemens Enterprise Communications GmbH & Co. KG.
All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

Communication for the open minded

Siemens Enterprise Communications
www.siemens-enterprise.com

Contents

1 Introduction

The document describes the OpenScape OpenScape Deployment Service (DLS) client in version **V3R1 (HI-DLS3R1.8xx)** and contains information about initial DLS server configuration.

This manual is also available as online help on the DLS client's interface, see Section 5.3, "Opening the Context-Sensitive Help Function".

For a quick start guide, please read the same-titled Chapter 2.

1.1 Target Group

This manual is intended both for administrators who install and configure the DLS server and for users who carry out configuration and deployment tasks on the DLS client. Users must have prior experience of LAN administration and an in-depth knowledge of IP Device configuration.

For more information on the skills that a DLS administrator must have, see Section 4.1.3, "Personnel Requirements".

1.2 Conventions Used

The following conventions are use for presenting information in this manual:

Convention	Example
`courier`	Input and output Example: enter `LOCAL` as the file name
Italics	Variable Example: *Name* can be up to eight characters long
Bold	Indicates user interface elements Example: Click **OK** Select **Exit** from the **File menu**
Bold	Special emphasis Example: You are **not** permitted to deleted this name
Element	User interface elements with supplementary information
`<Courier>`	Key combinations Example: `<CTRL>+<ALT>+<ESC>`

Table 1-1 Typographic conventions

Convention	Example
>	Menu sequence Example: **File** > **End**
ℹ	Additional information
⚠	Warning on critical aspects of a process

Table 1-1 Typographic conventions

1.3 Constraint Notes

Some of the settings configurable via DLS are available only for particular end devices resp. particular firmware versions. In such cases, an appropriate note is given.

2 Getting Started

This brief guide should enable administrators to quickly start the OpenScape Deployment Service, perform basic configuration, and connect new telephones, without detailed background knowledge.

In order to keep this chapter as short as possible, we have intentionally left the following information out:

- Various application scenarios
  Here only one standard scenario is provided as an example.
- Parameter descriptions
  Here we will only explain what you need to do, not why.
- Background information
  Only the most important information is summarized here.

Detailed information is provided in the rest of the manual, in particular in the chapters:

- Chapter 3: Concept and feature overview
- Chapter 4: Installation of the DLS and additional software components
- Chapter 5: General information about the user interface
- Chapter 6 to Chapter 14: Information on individual parameters
- Chapter 15 and Chapter 16: Practical examples with process descriptions

The following processes are described here:

- Section 2.1, "DLS Installation"
- Section 2.2, "Starting the DLS for the First Time (Single Mode)"
- Section 2.4, "Frequently Used Functions"
- Section 2.5, "Using the Mobility Function"
- Section 2.6, "Security"

2.1 DLS Installation

2.1.1 System Requirements

- Minimum hardware requirements:
  - TAP: CPU with at least 1.4 GHz; at least 512 MB RAM; Ethernet card, 100 Mbit or higher; hard disk drive capacity of 400 MB.
  - Integrated server: CPU with at least 1.8 GHz; at least 1 GB RAM; Ethernet card, 100 Mbit or higher; hard disk drive capacity of 10 GB.
- Operating systems supported: Windows XP Professional; Windows 2000 Server[1] (Service Pack 4); Windows 2000 Professional (Service Pack 4); Windows 2003 Enterprise Edition; Windows 2003 Standard.

2.1.2 Licensing

For configuring mobiles users, using DLS-Nodes in a cluster, database mirroring, the XML push functionality, or location service (IP infrastructure), licenses must be purchased. All further DLS functions are free of cost.

You can use HiPath License Management to load the relevant licenses for this onto the license agent. The license agent can be specified when you install the DLS or later under **Administration** > **Server Licenses**.

The license agent and HiPath License Management are available for download on C-SWS.

Demo licenses are available for test installations and include:
- 10 mobile user licenses (30 days)
- 1 node license (30 days)
- 1 database mirroring license (30 days)
- 1 location service license (30 days)
- 1 XML push license (30 days)

[1] Note the Microsoft license conditions regarding the maximum number of connections allowed. Check whether there are enough CAL (Client Access Licenses) for operating the DLS.

2.1.3 Installing DLS Software

Installation is performed as follows:

1. Download the DLS Software from the SWS-Server and unzip the downloaded file.
2. Click *setup.exe*.
3. Follow the user prompts in the installation shield.

The components required by the DLS, such as the database and web server, are installed if they are not already available on the system.

2.2 Starting the DLS for the First Time (Single Mode)

1. **Starting the program**
   To start the DLS client, go with a Web browser to
   [Server IP address]:18080/DeploymentService/ or
   https://[Server IP address]:10443/DeploymentService/ (encrypted connection via Secure HTTP).

2. **Logging on**
   Log on under the "admin" account with the password set during installation.

3. **Modifying passwords/configuring accounts**
   You must create a separate account in the DLS for each DLS administrator. This is only possible with the default "admin" account. To do this, select **Administration > Account Management** in the menu bar. Click **Search**. If you switch to **Table** view, information is provided on all user IDs in a table overview. You can create a new account with **New**.

4. **Location configuration**
   You can use the location criterion to define groups for terminals that share the same range of IP addresses and/or are connected to certain systems. Proceed as follows for basic configuration of the location:

   Define the IP address range for the location in **Administration** > **Server Configuration** > **Location** > **"IP Ranges" Tab**.

   Enter the IP addresses or host names of the systems (PBX/gateway or SIP server) for the location in **Administration** > **Server Configuration** > **Location** > **"Reg-Addresses" Tab**.

   Additional configuration options are provided under **Administration** > **Server Configuration** > **Location**.

   If you do not define a location, the "Default Location" is assigned for all location-specific parameters.

5. **FTP configuration**

   To load IP phone software and other files to the devices, you will need an FTP server that provides the software images. The DLS supports the configuration and use of unlimited numbers of FTP servers. To enter the access data for an FTP server, go to **Administration > Server Configuration > Configure FTP Server**. Click the action button **New** to create a new FTP server.

   In the **Server ID** field, enter a name for the FTP server you wish to use to transfer IP phone software.

   In the **Hostname** field, enter the network name or the IP address of the FTP server.

   In the field **SW Image Path**, the path to the directory containing the software image files is specified. This path is relative to the root directory of the FTP user ID used by the DLS. If the image files are contained directly in the root directory, enter "./" as your path.

   In the **User** field, enter the user ID that the DLS should use to log on to the FTP server. In the **Password** field, enter the corresponding password.

   You can use **Test** to check if the settings are correct using an FTP connection test. Apply your entries by clicking **Save**.

   You can find a description of all fields and additional information in Section 6.2.4, "FTP Server Configuration".

6. **HTTPS configuration (for OpenStage terminals)**

   OpenStage phones can alternatively use an HTTPS server for downloading files.

   In the **HTTPS Server ID** field, enter a name for the HTTPS server you wish to use to transfer files.

   In the **HTTPS Server URL** field, enter the network name or the IP address of the HTTPS server.

   You can find a description of all fields and additional information in Section 6.2.5, "HTTPS Server Configuration".

7. **Plug & Play/Autoconfiguration**

   DLS provides an option for preconfiguring IP devices to go into operation as soon as they are connected to the network. To do this, the DLS transfers the necessary configuration parameters to the IP device. In the case of IP Devices (IP phones, IP clients, IP Gateways), these parameters include, in particular, phone-number-dependent data for registration at the telephone system. The DLS must receive the system access data before it can incorporate the necessary data from the telephone system in the DLS database. Enter this under **Element Manager** > **Element Manager Configuration**.

   Using profiles, you can create standard configurations for multiple devices. Device profiles are created from templates composed of a collection of settings from individual masks plus information about the devices, gatekeepers, and IP ranges supported by each profile. To perform configuration, select **Profile Management** > **Device Profile**.

   If you want to create individual parameters for a particular device, you can create what is known as a virtual device. To do this, go to **IP Device Management** > **IP Device Configuration** and click **New**. The virtual device is assigned a placeholder beginning with "@"

instead of the device ID and the IP address and E.164 number are set to 0. To assign a physical device, enter either an E.164 number or a real device ID (generally, the MAC address). The 🔧 icon beside the **Device Type** field indicates that the IP device is not yet registered at the DLS. Otherwise, configuration is the same as for a connected, registered device.

> DLS records a device on the basis of the device ID/E.164 number value pair. In all configuration masks, this information is provided in the upper half of the user interface. Make sure that the data displayed here refers to the IP device you wish to configure so that the configuration data can be assigned to the correct IP device.

2.3 Required Workpoint Firmware Installation

If a device is connected for the first time when the DLS is running, it is automatically installed with the latest software available. Auto Deployment is used to upgrade devices that have already been connected. This requires a running FTP server and correct FTP configuration in the DLS (see Section 2.2, "FTP configuration"). The firmware image files must be saved in the directory that was specified as the **SW Image Path** during FTP configuration. They can also be divided into subdirectories.

2.3.1 Creating Software Images Automatically

Once the images are available on the FTP server, the DLS can register these automatically. The files are then assigned information, such as, the matching device type, the software type (SIP or HFA), and the software version. You can activate automatic registration by going to Software **Deployment** > **Manage Software Images** and then clicking **Autocreate...**. Click **Start** in the ensuing dialog window.

2.3.2 Auto Deployment

Software deployment is implemented in accordance with previously defined rules as soon as a new terminal has been registered at the DLS. These rules are defined as follows:

1. Click **New** in the area **Software Deployment > Manage Rules**.
2. Select the device type in the **Device Type** field. Remember, only one rule is permitted per device type.
3. In the field **SW Type**, select the correct software type.
4. If you want the software deployment to be performed using the latest available software, activate **Deploy latest version**.

   If you want the software version you have specified to be installed if the previously installed software is older, activate **Deploy software on an upgrade** and select the required firmware image in the field **SW Image**.

   If you want the software version you have specified to be installed if the previously installed software is newer, activate **Deploy software on a downgrade** and select the required firmware image in the field **SW Image**.

2.3.3 Manual Deployment

1. Go to **Software Deployment > Workpoint Deployment**. In the upper half of the user interface, select the device where you would like to install the software. Click **Deploy**.
2. A window is displayed with a list of all available software. The default setting only allows you to select data that matches the currently-selected device type. Select the required software and click **Deploy**.
3. A dialog opens where you can define when deployment should take place. The check boxes **Enforce deployment if phone is busy** and **Overwrite deployment restrictions** should not be activated. Click **OK** to start deployment.

2.4 Frequently Used Functions

2.4.1 Scan IP Devices

The DLS records IP Devices data during scanning. The IP Devices do not have to be registered at the DLS for this.

1. Go to **IP Devices > IP Device Interaction > Scan IP Devices**. To activate a scan, you need a scanner object. If one has already been created, you can search for it by clicking **Search**. Otherwise, you must create a scanner object. To do so, click **New**. In the field **IP Scanner** in **"IP Ranges" Tab**, enter a name for the object, for example, **Scanner 1**. Next, enter the IP address range to be scanned. Click the icon to do this. Enter appropriate values in the fields that are now active (**IP Address from** and **IP address to**). The **Port** field contains the default setting 8085; this is the default port for HTTP with IP phones. If you click **Save** now, the scanner object is ready for use.

> In the default setting, the DSL sends an ICMP ping to each IP address of the area to be scanned. If the network does not support ICMP pings, the check box **Allow ICMP-Pings** under **IP Devices** > **IP Device Interaction** > **Scan IP Devices** > **"Configuration" Tab** must be deactivated.

2. Click **Scan IP Devices** to activate scanning.

For more information on this subject, see Section 7.4.4, "Scan IP Devices".

2.4.2 Configuring Parameters: Example Key Layout

Configuring parameters for individual IP Devices is demonstrated below using the key layout. The function and text of a function key are to be configured. The example function in this case is the mobility key, which a user can use to log on to the telephone.

1. Go to **IP Devices > IP Phone Configuration > Keysets/Keylayout**. Click **Search** and then select the device in **Table** view. For more information on the settings in the **Keysets** tab, see Section 7.1.19.1, ""Keysets" Tab".
2. To create a new entry, go to the **Destinations** tab and click the icon. A new row is displayed in the table.
3. As the key function **Mobility** is on the first level, select "1st **Level** " in the Level column.
4. In the **Key number** column, select the key to which the new function should be assigned. For more information, see Section 7.1.19.2, ""Destinations" Tab".
5. Select "Mobility" in the **Key function** column.
6. You can now enter a key label in the final column. This is only displayed with optiPoint 420 telephones that provide automatic key labeling.

Complete the action by pressing **Save**.

2.4.3 Jobs

All actions that can be performed on IP Devices using DLS, such as, configuring the key layout, are managed by the DLS as jobs.

Using job control, you can view information on individual jobs, and cancel, delete or reactivate jobs. To do so, go to **Job Coordination > Job Control**.

Essentially jobs can be started either immediately or later at a specific, predefined time. For example, in order to perform the actions described in Section 2.4.2, "Configuring Parameters: Example Key Layout" at a specific time, perform all the steps described except the final **Save** action. Then, in the top right field **Job ID**, enter an arbitrary job ID and click the 📅 icon beside the field **Execution Time** to define when the action should be executed. Once this has been completed, activate the job with **Save**.

For further information on job coordination, see Section 14, "Job Coordination".

2.5 Using the Mobility Function

With the Mobility function, call numbers can be assigned to specific persons instead of devices. As well as their call number, users can transfer their personal settings, such as their key layout, from one device to another. To enable this, users must log on to a device that has been activated for this purpose with their call number and a password. As a result of logging on, the call number of the device and all other user data is replaced with the data of the new user. Following logoff, the device is reassigned its original number and user data.

In order to use the mobility function, a mobile user profile must be created. This profile is identified by a call number and password. There are two possibilities here: creation by adding or creation by migrating a basic profile. The second option is described below.

1. A prerequisite for using the mobility function is that the workpoint is activated for mobile user logon. To do so, go to **IP Devices > IP Phone Configuration > SIP Mobility**, and in the **"SIP Mobility" Tab**, activate the option **"**Device available for Mobile User**"**. Activation takes a few seconds and is carried out in the background.

2. Go to **Mobile Users > SIP Mobile User Interaction > SIP Mobile User**. If you now select "Mobility enabled Device" in the **User Type** field and then click **Search**, a list of all devices available for a mobile user is shown in **Table** view.

3. Click on **Migration to Mobile User**. After this, a dialog window appears.

4. Now, in the field **New Basic E.164**, enter a new basic callnumber for the end device currently selected, whose basic profile is to be migrated. This call number must be registered with the SIP server. A new basic call number is necessary so that the end device remains ready to use. Further on, a virtual device must exist which provides the required Plug&Play data (see Section 15.5.2.2, "Creating Plug&Play Data"). As soon as the migration has succeeded, the previous basic call number is assigned to the mobile user. The call number of a mobile user is also referred to as mobility ID.

5. In the field **Basic Mobile User Profile**, a new profile for the basic user (the basic call number) must be entered. The mobile user adopts the data and the call number of the end device, these data automatically constituting his new individual profile. If you search for the mobile user after this action is completed, the mobile user’s call number is displayed with a prefixed "@". This is a placeholder for his individual profile.
6. Start the migration via **Start Migration**.
7. Now, enter a new password for the mobile user in the field Mobile User Password (the default password is "000000"). Finally, confirm by clicking **Save**.

2.6 Security

2.6.1 Encryption

The data traffic within the telephone system can be secured using the encrypted Secure Real-time Protocol (SRTP). The devices, which communicate with each other via encryption, are in an SRTP Security Domain. In this domain, non-secure clients are not permitted. In order to create an SRTP Security Domain, all components of the telephone system must have a shared key or a Pre-Shared Secret (PSS). Only the DLS can generate and distribute this PSS.

The device must be prepared as follows for encryption:

Go to **IP Devices > IP Phone Configuration > Gateway/Server**. The **"Gateway (HFA) / SIP Server" Tab** contains the field **H.235 Security Mode**. Here, **Full** must be activated. Enter the **Subscriber Password**.

Key distribution is activated as follows:

1. Go to **Voice over IP Security V1 > Key Distribution**. In the **Distribute to** list, select the gateways that should receive a key.
2. Click **Change Security Mode**. A dialog window is displayed where you can define when the key should be distributed and activated. Confirm with **OK**.

Keys are automatically verified and distributed as soon as a new and appropriately prepared device is registered.

For more information on key distribution, see Section 16.11.1, "Initially Configuring a PSS".

2.6.2 Certificates

Certificates enable secure authentication between servers and clients. They can be implemented for the following server-client scenarios:

- WebServer Certificates for web-based Management (WBM of IP Phones/IP Gateways)
- Certificate for IEEE 802.1x/EAP-TLS authentication (IP Phones only)
- TLS-based Signaling Encryption (all device types)
- additional Server Applications for IP Phones (e.g. LDAPS)

DLS can be used for certificate administration.

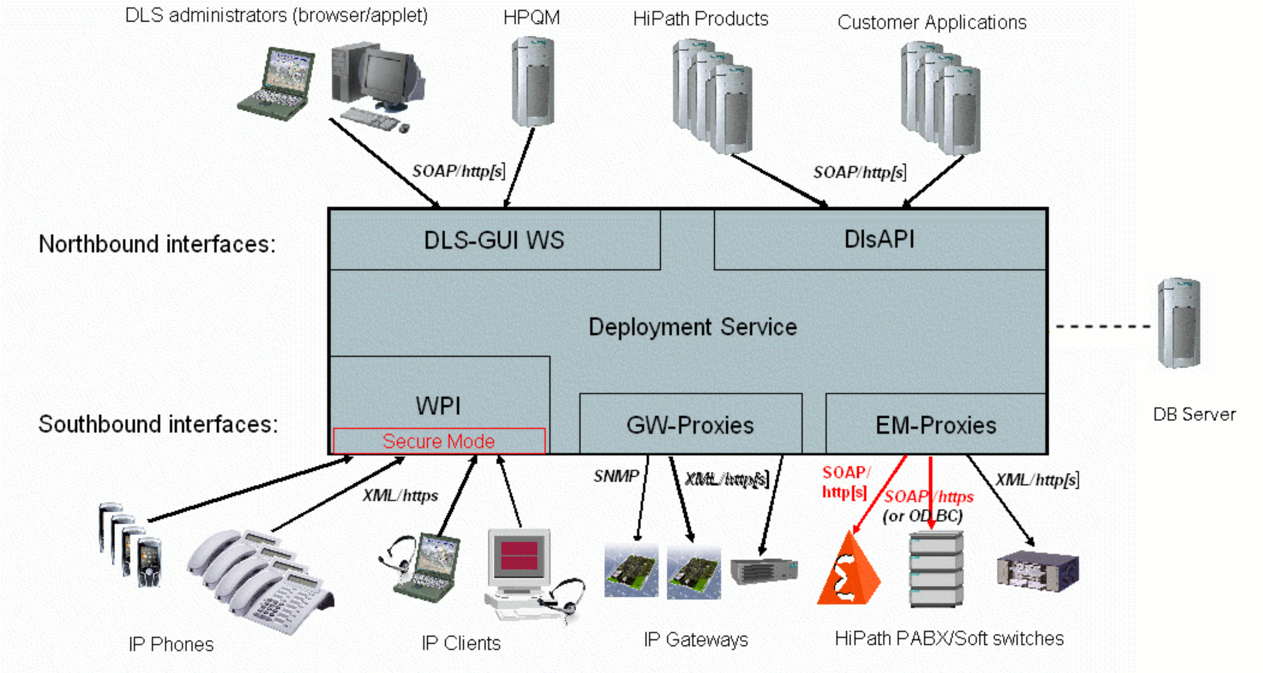
For more information, see Section 16.12, "Security: Administering Certificates".

3 Concept and Features

3.1 Overview

The Deployment Service (DLS) is a HiPath Management application for administering workpoints (IP phones and IP client installations) in both HiPath and non-HiPath networks. The DLS database can be exported to a separate server (optional).

The following overview shows possible components that can work together with the DLS in a network.



We recommend that you use a DHCP server in the DLS environment to

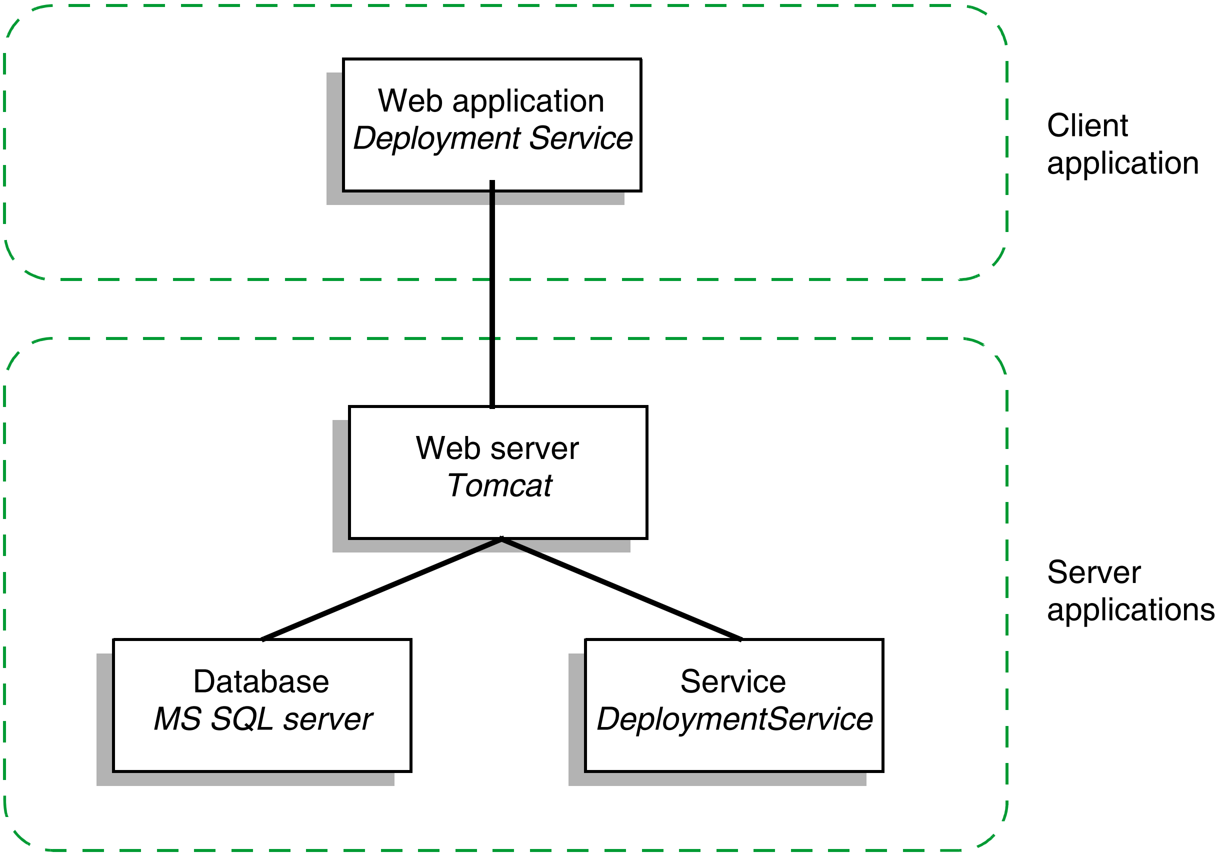
- support plug&play and
- ensure the authenticity of the DLS server.

Setting up the DHCP server should be one of the first tasks you perform, if possible, even before you install the workpoints.

Only one DLS server is allowed per DHCP domain at the customer facility.

3.2 Deployment Service Components

The following overview shows the components that are involved in operation of the Deployment Service on the server and client sides.



The client applications can be executed both on a client PC that can be reached in the IP network and on the server PC itself.

When server and client are being used separately, ensure that the operating system times are synchronized.

3.3 Operating Fundamentals

Before you can configure IP Devices with the DLS, you must first collate all IP Device data following initial DLS startup. This means that the IP Device configuration data first has to be incorporated in the DLS server database.
The IP Devices do this by registering at the DLS and transmitting this data to the DLS.

The IP Devices data is read out by

- scanning the IP Devices with DLS, see Section 7.4.4, "Scan IP Devices"
  (recommended if there are already a number of IP Devices operating after the initial DLS startup)

  or by
- plugging the LAN connector or power supply into the IP Device
  (recommended if putting separate additional IP Devices into operation).

All actions performed with the DLS, for example, an IP Device software update or a modification of the configuration data, are logged in the DLS.

Job coordination helps you in this process. This allows you to see the status of each action and to determine the cause if there is an error. For more information, see Section 14, "Job Coordination".

3.4 Area of Application

> Please refer to the Release Notes or Sales Release for the appropriate version for information on current supports/restrictions.

You can administer the following IP Devices with the DLS:

IP Device	HFA Version	SIP Version
AC-Win 2Q IP	all versions	all versions
AC-Win MQ IP	all versions	all versions
HG1500		
HG3500		
HG3575		
HOOEE (HiPath OpenOffice EntryEdition)	all versions	all versions
HOOME (HiPath OpenOffice MediumEdition)	from V1.0	from V1.0
HP2K V2.0	from V2.0	from V2.0
optiClient 130	from V5.0 onwards	V2.0
Siemens OpenScape Desktop Client	all versions	all versions
optiPoint 400 economy	from V5.0 onwards	-
optiPoint 400 standard	from V5.0 onwards	-
optiPoint 410 entry	from V5.0 onwards	from V4.1 onwards
optiPoint 410 economy	from V5.0 onwards	from V4.1 onwards
optiPoint 410 economy plus	from V5.0 onwards	from V4.1 onwards
optiPoint 410 standard	from V5.0 onwards	from V4.1 onwards
optiPoint 410 advance	from V5.0 onwards	from V4.1 onwards
optiPoint 420 economy	from V5.0 onwards	from V4.1 onwards
optiPoint 420 economy plus	from V5.0 onwards	from V4.1 onwards
optiPoint 420 standard	from V5.0 onwards	from V4.1 onwards
optiPoint 420 advance	from V5.0 onwards	from V4.1 onwards
optiPoint 600 office	all versions	-

Table 3-1 IP Devices / versions supported

IP Device	HFA Version	SIP Version
optiPoint WL2 professional S	-	V1.0 (50/70)
optiPoint WL2 professional	V1.0 (50)	-
OpenStage 15	all versions	all versions
OpenStage 20E	all versions	all versions
OpenStage 20	all versions	all versions
OpenStage 40	all versions	all versions
OpenStage 60	all versions	all versions
OpenStage 80	all versions	all versions

Table 3-1 IP Devices / versions supported

On the following device types, the mobility function is available in SIP V6.0 or later: optiPoint 410 economy, optiPoint 410 economy plus, optiPoint 410 standard, optiPoint 410 advance, optiPoint 420 economy, optiPoint 420 economy plus, optiPoint 420 standard, optiPoint 420 advance.
On the following device types, the mobility function is available in all versions: OpenStage 20E, OpenStage 20, OpenStage 40, OpenStage 60, OpenStage 80.

Administration is possible for various communication platforms. Both HiPath and non-HiPath platforms are supported:

Platform	P&P connection	Plug &play	QDC connection	QDC	SRTP connection	SRTP
OpenOffice EE V1.0	standalone	no	no	no	no	no
OpenScape Office MX/LX	standalone	no	no	no	no	no
HiPath 3000/5000 <V5.0	standalone	no	no	no	no	no
HiPath 3000/5000 V5.0	HG1500	yes	HG1500	yes	no	no
HiPath 3000/5000 V6.0	HG1500	yes	HG1500	yes	HG1500	yes
HiPath 3000/5000 V7.0	HG1500	yes	HG1500	yes	HG1500	yes
HiPath 4000 V1.0	Assistant	yes	no	no	no	no
HiPath 4000 V2.0	Assistant	yes	HG3530/50/ 70/75	yes	no	no
HiPath 4000 V3.0	Assistant	yes	HG3530/50/ 70/75	yes	HG3530/50	yes
HiPath 4000 V4.0 / V5	Assistant	yes	HG3500/75	yes	HG3500/75	yes
HiPath 4000 V6[1]	Assistant	yes	HG3500/75	yes	HG3500/75	yes
OpenScape Voice V3.1	SOAP I/F H8000	yes	no	no	no	no
OpenScape Voice V3.1	Assistant	yes	no	no	no	no
OpenScape Voice V4.0	SOAP I/F H8000	yes	no	no	no	no
OpenScape Voice V4.0	Assistant	yes	no	no	no	no
OpenScape Voice V4.1	Assistant	yes	no	no	no	no
HiPath DX V9	DX WebPro	yes	no	no	no	no
HiPath RG2700 V1.0	not relevant	no	RG2700	yes	no	no

Table 3-2 Communication platforms supported

[1] Parameter settings for HiPath 4000 are also valid for HiPath 4000 V6, except as noted otherwise.

> ⓘ If SIP IP phones are connected to the platforms HiPath 3000 and HiPath 4000, some features are not available. Please deactivate these at the IP Device, so that they are not visible resp. selectable by the user.
>
> For more information on this, see Section 7.1.4.4, ""Availability" Tab".

3.5 Overview of Software and File Types

The following table displays how DLS maps file extensions to file types in standard configuration.

> ℹ The administrator can define the extensions as desired in the `file_map.xml` file found under `DeploymentService\Tomcat5\webapps\DeploymentService\WEB-INF\classes`.
> To return to the standard configuration copy and rename `default_file_map.xml` to `file_map.xml`.

Object type (name in the DLS)	File extension	Example	Contents
Software objects			
Software image	*.img	opera_bind.img	OpenStage firmware
Software image	*.app	optiPoint410std-V5.0.0.app	DLS-compatible optiPoint firmware ("new format")
Software image (old)	*.app	vxWorks.app	non-compatible optiPoint firmware ("old format")
Software image	*.exe	setup.exe	PC software installation
Firmware (Netboot)	*.fli	vxWorks.fli	Software image for transfer via Netboot server
		netboot308.fli	Netboot firmware
File objects			
LDAP Template	*.ldap	ldap_temp.ldap	LDAP Template for optiPoint and OpenStage 40/60/80
	*.txt	ldap_temp.txt	LDAP template for OpenStage 40/60/80

Table 3-3 Software and file types supported

Music on hold [1][2]	*.moh	opti410.moh	Audio file in proprietary format for optiPoint and OpenStage.
	*.wav	music.wav	Audio file in WAV format for OpenStage. Recommended Specifications: Audio format: PCM Bitrate: 16 kB/sec Sampling rate: 8 kHz Quantization level: 16 bit
	*.mp3	music.mp3	Audio file in WAV format for OpenStage 60/80.
	*.mid	music.mid	MIDI-Datei for OpenStage.
Screen Saver[2]	*.jpg	screenPic1.jpg	Image file for the OpenStage 60/80 screensaver. Resolution: OpenStage 60: 320x240 OpenStage 80: 640x480
	*.png	screenPic1.png	
INCA Firmware	*.h86	inca.h86	INCA firmware for optiPoint 600 office
JAVA Midlet	*.jad	?	Java application
-	*.jar[3]	?	Java archive
Logo file[2]	?	?	
	*.jpg		Image file for a logo on OpenStage. Recommended specifications for OpenStage 60: Width: 240 px Height: 70 px Resolution: 70,55 dpi Recommended specifications for OpenStage 80: Width: 480 px Height: 148 px Resolution: 124,5 dpi
	*.png		
System and Ringtone[1] -	*.xml	?	System and ringing tones
	*.wav	?	
	*.mp3	?	
	*.mid	?	
	*.app	bootrom.app	Boot loader for the optiPoint 600 office
-	?	?	New/other applications
-	?	?	DSM firmware
-	*.csv	?	For ENB import and export
Dongle Keys	*.key	dongle.key	Dongle Keys for OpenStage Remote Test Tool

Table 3-3 Software and file types supported

[1] Only for SIP versions.

[2] Ringtones and music on hold files must not exceed 1MB in size, while screensavers/logos should not be larger than 300kB.

[3] Only in combination with a *.jad file.

3.6 The Most Important Features

Security:

DLS provides extensive functions that guarantee a high level of security for VoIP communication. The following is an overview of the most important elements:

- PSS generation and distribution within an SRTP security domain (password identification).
  See Section 16.11, "Security: Pre-Shared Secret for SRTP Security Domains".
- Import and distribution of individual certificates for secure authentication.
  See Section 16.12, "Security: Administering Certificates".
- Secure mode can be configured for mutual authentication between the workpoint and the DLS.
  Area: **IP Devices** > **IP Device Management** > **IP Device Configuration** > **"DLS Connectivity" Tab**.
- Minimum password length specification for user, administration, and screenlock passwords as well as for the SNMP community string.
  Area: **IP Devices** > **IP Phone Configuration** > **Security Settings** > **"Passwords" Tab**.
- Systematic deactivation of workpoint services (for example, WBM interface).
  Area: **IP Devices** > **IP Phone Configuration** > **Security Settings** > **"Enabled Services (NW Stack)" Tab**.

Mobility for SIP IP phones:

DLS is a tool that supports the mobility feature on SIP IP phones and permits the configuration and administration of Mobile Users. You can use these options to migrate existing workpoints and implement mobile user standards.

For basic information on mobility in DLS, see Section 3.7, "DLS Mobility - General Information".

Software deployment:

DLS is a user-friendly tool for upgrading software on all workpoints available or on a definable number of workpoints.

For more information, see .

Inventory data management:

The DLS is the central inventory data manager. Inventory data describes the hardware configuration and capacity of the workpoint and includes information on items, such as, add-on devices or adapters available.

Inventory data can be exported over the CSV interface.

Plug&play function:

The DLS supports plug&play. Plug&play means that the IP phone is ready to work as soon as it is plugged into the network - no user intervention required. Ideally, the workpoint automatically downloads all necessary software and configuration data and can be used after a few minutes.

For more information, see Section 15.5, "Workpoint Autoconfiguration (Plug&Play)".

User interface:

The DLS has a Java-supported, Web-based user interface, and runs on an Internet browser.

For information on browser requirements, see .

Configuration Management:

Configuration Management is the DLS's central tool for displaying and administering workpoint parameters in a HiPath environment. It can be operated either at the customer facility or by Service (via remote administration).

Workpoints can also be restarted with the Reset function.

Additional functions:

The following basic functions are supported:

- Import/Export:
  This function is particularly useful during the initial configuration of the DLS, and can also be used in later operation for backing up configuration data.
  The Import/Export function is a user-friendly tool for transmitting a DLS configuration from one DLS installation to another.
- Access protection:
  Access to the DLS is password-protected.

- Error and activity logging and trace function.
- Support for the configuration of QDC features for HG3550 V2.0, HG1500, RG2700, and HiPath HG3530/70/75 (over SNMP proxy).
  The SNMP proxy is installed together with the DLS during startup and start automatically (runs as a local "DeploymentServiceSNMPProxy" service).

3.6.1 Capacity Limits and Restrictions

- You can only use the plug&play functionality in DLS if there is a DHCP/DNS infrastructure in the network and this has been configured for working with the DLS (see Section 15.5, "Workpoint Autoconfiguration (Plug&Play)").
- You can only install one DLS per domain in the network.
- The DLS user interface is available in German and English.

3.6.2 Ports Used

The DLS Release Notes contain an overview of the ports used by the DLS.

3.7 DLS Mobility - General Information

You can use the mobility feature in DLS to carry out the following functions (for definitions of these terms, see below):

- Create, refresh and delete Mobile Users
- Create user profiles for Mobile Users.
- Modify Mobile Profile parameters
- Migrate Basic Profiles to Mobile Profiles
- Log Mobile User on or off and monitor activities.
- Archive mobile users.

For additional information on operation, refer to Section 16.13, "Configuring and Administrating Mobility".

3.7.1 Mobility Definitions

The following terms are frequently used in connection with mobility in this document:

Term	**Definition**
Mobility Function	This function enables Mobile Users to log on to a Mobility Phone and operate it with their personal settings.
Mobility Phone	A phone that supports the Mobility Function. In other words, Mobile Users can log on to this kind of phone and operate it with their personal settings.
Mobility ID	Phone number of the Mobile User. The Mobility ID and password are used for authentication when logging on to a Mobility Phone.
Basic User	Phone number and user data of a Mobility Phone if there are no mobile users logged on.
Mobile User	A user who can log on to a random Mobility Phone and operate it with his or her personal settings.
User Data Profile	This is a configurable user data (sub)set, depending on the scope of the associated templates. The parameters are not device-specific.
Device Profile	User-independent telephone parameters. These parameters are entirely device-specific (dependent on the telephone used).
Mobile User Archive	Can be created to save mobile user data.

Table 3-4 Definition of mobility terms

3.7.2 Using Mobility

Mobility grants appropriately configured users access to their individual settings on all telephones that support the mobility function. Transferable parameters include user-specific configurations (for example, authorizations) and user-defined settings (for example, language settings).

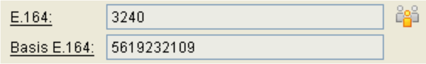
To use this function, just press the "Mobility" function key on a Mobility Phone (or use the corresponding telephone menu), and log on as a Mobile User with your call number (Mobility ID) and user password.

After logging on, Mobile Users can make and receive calls via Mobility Phones and can always be reached at their personal number. Outgoing calls are also made using these numbers.

Mobile Users can log off a phone either locally at the phone or remotely via Web-based Management (WBM) or DLS ("forced logoff").

3.7.3 Mobility ID

These two call numbers are displayed as **E.164** and **Basic E.164** in the area **IP Devices** > **IP Phone Configuration** in the DLS client.



E.164: 3240

Basis E.164: 5619232109

E.164 is the Mobile User's call number (Mobility ID) and **Basic E.164** is the Mobility Phone call number when no Mobile Users are currently logged on.
The smiley to the right of the **E.164** field indicates that a Mobile User is currently logged on.

3.7.4 Configuring Mobility

The Mobility Function can only be configured for a phone via DLS. To configure this function, the telephone must be released by activating the Mobility function.

> The "Mobility" function can only be assigned to a key on the actual telephone; keys on connected optiPoint key modules or optiPoint self labeling key modules cannot be used.

A Mobile User can be created in two ways:

- **Creating a Mobile User by adding a number**
  A new Mobile User is generated by assigning a new call number together with a password. The remaining parameters are assigned to the Mobile User from a User Data Profile. When the mobile user is logged on, only device-specific parameters are retained in the telephone.
- **Creating a Mobile User by migrating a number**
  The telephone's existing call number becomes the Mobility ID and the telephone is assigned a new basic number. The mobile user accepts the telephone's parameters. Use this option, for example, if you want to change an existing workstation into a mobile workstation. You can then continue to use the existing number to contact the user at the mobile workstation, providing he or she is logged on to a Mobility Phone.

For more information on configuring the Mobility Function for SIP IP phones, see Section 16.13, "Configuring and Administrating Mobility".

3.7.5 Profile Concept in DLS

For more information on this, refer to the profile descriptions in Section 3.7, "DLS Mobility - General Information".

3.7.5.1 Difference between Device Profile and User Data Profile

The following examples of parameters and the profiles they belong to highlight the difference between Device Profiles and User Data Profiles.

The parameters in the example are displayed in the following DLS client area:
IP Devices > **IP Phone Configuration** > **Miscellaneous** > **"Country & Language" Tab**

Parameter	Profile	Definition
IP address	Device Profile	The IP address is connected to a physical phone, regardless of who is logged on to the phone. This makes it part of the Device Profile.
Layout	User Data Profile	The Mobile User should be able to use a telephone's key layout with any Mobility Phone. This makes it part of the User Data Profile.
QoS parameters	Device Profile	QoS parameters are location-specific and therefore part of the Device Profile.
Language	User Data Profile	Once a language is configured on a phone, it should be available to a Mobile User on every Mobility Phone. This makes it part of the User Data Profile.

Table 3-5 Sample parameters with profile classification

A User Data Profile can be either a Basic Profile or a Mobile Profile, Section 3.7.5.2, "Parameter Configuration Availability".

3.7.5.2 Parameter Configuration Availability

Device Profile parameters can always be modified in the **IP Phone Configuration** area. Device Profile parameters are not Mobile User data. As a result, they are not available in the **SIP Mobile User Configuration** area.

Different configuration options are available in the DLS client depending on whether the Mobility Function is configured on a phone and, if so, whether a Mobile User is logged on.

This section only deals with the Basic Profile and Mobile Profile, as the Device Profile is always available in the **IP Phone Configuration** area and never in the **SIP Mobile User Configuration** area.

Status	**Parameters under:** **IP Phone Configuration**	**Parameters under:** **SIP Mobile User Configuration**
No Mobility Phone	All profiles can be modified	Not available
Mobility Phone, Mobile User is not logged on	Basic Profile: can be modified Mobile Profile: not available	Basic Profile: can be modified Mobile Profile: can be modified. Both profiles are visible as two objects in the DLS.
Mobility Phone, Mobile User is logged on	Basic Profile: not available Mobile Profile: read-only.	Basic Profile: can be modified (changes transferred to phone after Mobile User logoff). Mobile Profile: can be modified

Table 3-6 Parameter availability in DLS

Please note the different parameter displays in the **IP Phone Configuration** and **SIP Mobile User Configuration** areas:

- In the **IP Phone Configuration** area, a *single* object (displayed in **Object** view or as a row in **Table** view) always corresponds to a physical SIP IP phone (mobility-enabled or standard).
- In the **SIP Mobile User Configuration** area, two different object types exist:
  - an object for the Mobility Phone and
  - an object for the Mobile User.

4 Installation and Initial Configuration

There are multiple variants for DLS installation and operation:

- **Single node operation with local database:** DLS server and DLS database are located on the same machine. For the database, Microsoft SQL Server 2005/2008 is used. The software is included.
- **Single node operation with remote database:** The DLS database is located on another machine.
- **Multi node operation (cluster):** The DLS server is running in a distributed way on multiple machines. The DLS database is hosted on another machine or on one of the DLS node machines.

In addition, if a remote database is used, database mirroring is possible (mode for enhanced data security / high availability). Mirroring can be carried out in a synchronous manner, that is, main database and mirror database are refreshed simultaneously, or in an asynchronous manner. With asynchronous mirroring, the mirror database is updated after the transaction on the main database has occured.

The following chapters are arranged in order of their relevance for a particular DLS installation variant.

Variant	Chapter
Single Node with local database	● Section 4.5.1, "Single Node Operation With Local Database"
Single Node with remote database	● Section 4.2, "Install MS SQL Server for Remote Database" ● Section 4.5.2, "Single Node Operation With Remote Or Customer Specific Database"
Multi node / cluster	● Section 4.1.5, "Infrastructure For Cluster Operation" ● Section 4.2, "Install MS SQL Server for Remote Database" ● Section 4.3, "Configure the Network Load Balancer" ● Section 4.5.3, "Multi Node Operation"
Enhanced database security / High availability through database mirroring	● Section 4.6, "SQL Database Mirroring Setup"

4.1 Requirements

4.1.1 General Server Requirements

For information on the hardware needed, see Section 2.1.1, "System Requirements".

The DLS server runs on the German or English version of one of the following operating systems:

- Windows XP Professional (Service Pack 3)
- Windows 2000 Server[1] (Service Pack 4)
- Windows 2000 Professional (Service Pack 4)
- Windows Server 2003 Enterprise Edition (Service Pack 2)
- Windows Server 2003 Standard Edition (Service Pack 2)
- Windows Server 2008 (Service Pack 2)
- Windows Server 2008 R2 x64

> ℹ For larger-scale installations, particularly for cluster operation, a server operating system is required.

> ℹ If you plan to use the SQL server shipped with the DLS, please ensure that the database directory is not located in a partition with the ’compressed’ property.

The DLS client runs as Java applet in a web browser. Required are:

- Microsoft Internet Explorer 6.0 or higher or Firefox 2.0 or higher (Netscape is not supported).
- When Windows 2000 is used: DirectX (V9.x or higher).
- Java PlugIn

4.1.2 General Client PC Requirements

The PC on which the DLS client runs should provide the following hardware features:

- Space on hard disk: no special requirements.
- CPU Pentium IV with at least 1.4 GHz clock speed.
- At least 512 MB RAM.
- Network device with 10 Mbit, 100 Mbit or more or modem.
- Screen resolution: at least 1024 × 768 pixels with at least 16-bit color depth.

[1] Note the Microsoft license conditions regarding the maximum number of connections allowed. Check whether there are enough CAL (Client Access Licenses) for operating the DLS.

4.1.3 Personnel Requirements

Remote Service Engineer (RSE):

- Sound knowledge of LAN technology and IP networks.
- Sound knowledge of the IP Devices supported by the DLS (see Section 3.4).
- For multi node (cluster): sound knowledge of Microsoft operating systems and MS SQL Server 2005/2008.

Field Service Engineer (FSE)

- Sound knowledge of the IP Devices supported by the DLS (see Section 3.4).
- Basic knowledge of LAN technology, IP networks, and the operating systems supported.
- For multi node (cluster): sound knowledge of Microsoft operating systems and MS SQL Server 2005/2008.

4.1.4 DLS Availability

For more information on DLS licensing resp. specific DLS functionalities, see Section 2.1.2, "Licensing".

For service, additional installation options are available:

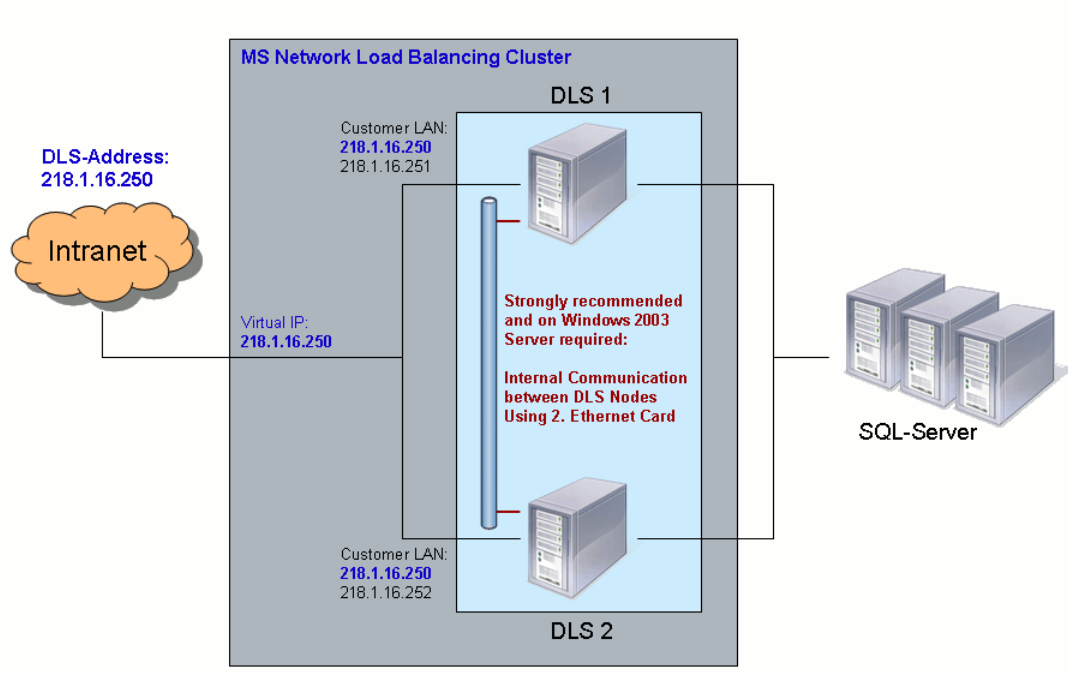
- For DLS installation at the customer facility (for example, HiPath SPA Server), the software can be acquired from C-SWS using RCC.
- Installation in service can take place as follows:
  – In the international market, you can also use the C-SWS for installation on the service laptop.

4.1.5 Infrastructure For Cluster Operation

A DLS cluster consists of up to 4 DLS nodes and up to 3 SQL servers. DLS nodes and SQL server may share common hardware, but the use of separate machines is recommended. From the end devices' point of view, the DLS nodes constitute a cluster with one virtual IP address, which is provided by the Windows Network Load Balancing Manager. The Network Load Balancer runs as a service on all DLS nodes and forwards the requests to the DLS nodes. For communication between the individual DLS nodes, all DLS nodes need a secondary IP address, and thus an additional network card.

> The nodes administered by the NLB must not be configured by DHCP.

The DLS database operates as a remote database on one or more machines, depending on whether database mirroring is desired or not. However, the DLS will connect to only one machine. It is also possible to operate both DLS server and database server on one and the same machine.



4.2 Install MS SQL Server for Remote Database

A simple way to increase the capacity and efficiency of the DLS lies in employing Microsoft SQL Server 2008 Enterprise Edition. This way, you can avoid the limitation to 4 GB which comes along with the Microsoft SQL Server 2008 Express Edition included in the DLS software package.

It is recommended to install the SQL server on a separate machine. Please ensure that the database directory is not located in a partition with the ’compressed’ property.

The communication between DLS node and SQL server proceeds in clear text. Therefore, it is necessary to take appropriate security measures.

For the DLS, Microsoft SQL Server 2005 as well as Microsoft SQL Server 2008 can be used. In the following, both versions are described.

As, for the configuration of database mirroring, the individual SQL servers are addressed via FQDNs (Fully Qualified Domain Names) , DNS names must be available at least for all SQL servers. Therefore, either a DNS server (recommended), or a name assignment for all participating machines by means of Windows workgroups. You can find the configuration files in which IP addresses and workgroup names are assigned to each other in:

`C:\Windows\system32\drivers\etc\hosts`

For database mirroring, Microsoft SQL Server 2008 Enterprise Edition expects names in one of these formats:

`<hostname>.<domain>` (DNS)

or

`<hostname>.<workgroup>` (Windows Workgroup)

The Windows 2008 R2 Server operating system already contains a DNS server; please refer to the correspondant documentation.

Please ensure that system time is synchronous on all machines. This is the case when Windows 2008 Server is used, as the system time will be provided here.

The installation described here is required when the DLS database is to operate on a separate machine. For operating DLS server and database on the same machine in a single node solution, no special installation is required, as this is handled by the DLS installation routine (see the installation description in the DLS software package). With multi node solutions, a separate database installation is definitely necessary, even if database and DLS reside on the same machine.

Microsoft SQL Server 2008 Enterprise Edition, which is required for multi node solutions, is not provided with the DLS software package, and must therefore be purchased separately.

You can find further information on the Microsoft SQL server in:
Ray Rankins u. a. (1987): Microsoft SQL Server 2005 Unleashed. SAMS Verlag, ISBN: 0-672-32824-0; Ray Rankins u. a. (2009): Microsoft SQL Server 2008 Unleashed. SAMS Verlag, ISBN-10: 0672330563.

1. Account for DLS and Database

   Alternative A: Local user.

   On the machine designated for database hosting, create a local administrator account. For this purpose, e. g. "dls".

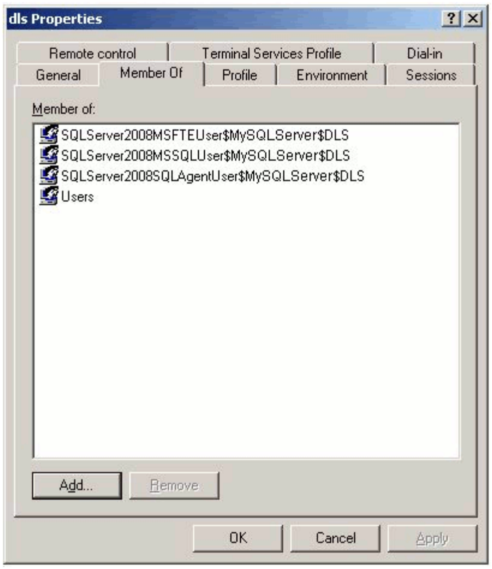
   Alternative B: Using Active Directory.

   Use a domain account existing in your Active Directory or create a new account for database access.

   Alternatives A and B: Add the account to the group of local administrators.

   If a database with mirroring is to be used, the same account must be used on each database server.

   If the access rights for the user "dls" shall be reduced to a minimum, it is recommended to use the setting shown in the following example, instead of assigning the user to the administrators group. In the example, "MySQLServer" is the name of the SQL server. A FQDN (Fully Qualified Domain Name) can be used here.



Member of:

SQLServer2008MSFTEUser$MySQLServer$DLS
SQLServer2008MSSQLUser$MySQLServer$DLS
SQLServer2008SQLAgentUser$MySQLServer$DLS
Users

As in the course of the installation, a stored procedure must be set up in the master database, this user should have the "sysadmin" role during installation. After the installation, the role for the server can be changed to "public", and the role for the database can be changed to "db_owner". A role for executing stored procedures can be created and assigned as follows:

```
CREATE ROLE db_executor
GRANT EXECUTE TO db_executor
EXEC sp_addrolemember 'db_executor', 'dlsservice'
```

2. Database Directory

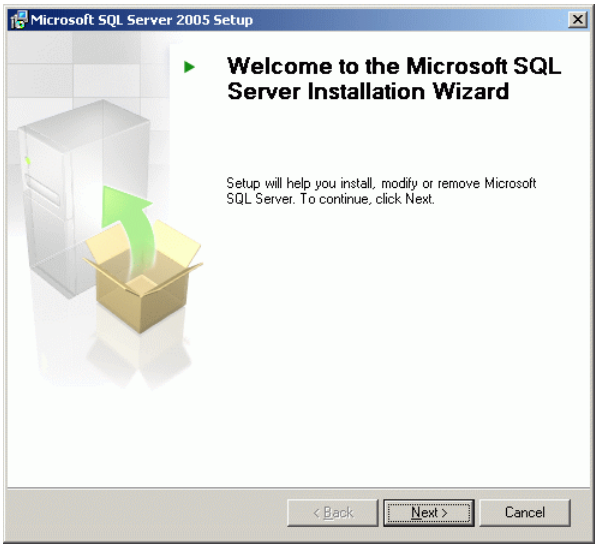
   On the database server, create a database directory, e. g. `D:\DATA\DLSDB`. This directory will be needed for the DLS installation later on.

   For mirroring, the same local path must be given both on the main server and on the mirroring server.

   The further installation steps are described separatedly for Microsoft SQL Server 2005 and Microsoft SQL Server 2008.

4.2.1 Microsoft SQL Server 2005

1. Open the setup program and click on **Next**.

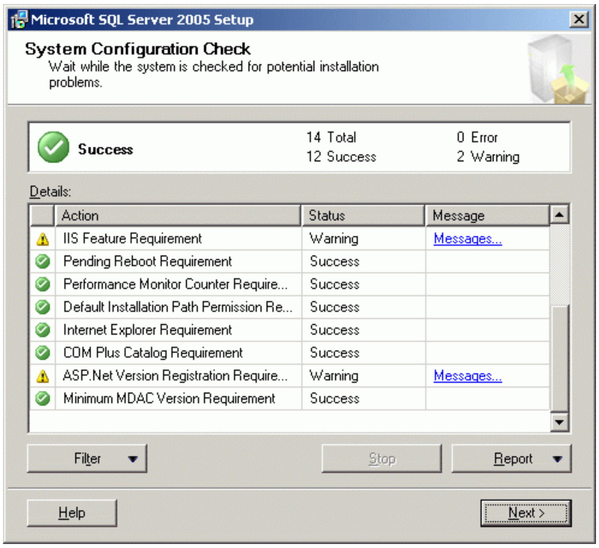


Microsoft SQL Server 2005 Setup

Welcome to the Microsoft SQL Server Installation Wizard

Setup will help you install, modify or remove Microsoft SQL Server. To continue, click Next.

2. The system configuration is analyzed. In case you receive warnings in relation with the components IIS (Internet Information Server) or ASP.Net, you can ignore these.



Microsoft SQL Server 2005 Setup

System Configuration Check
Wait while the system is checked for potential installation problems.

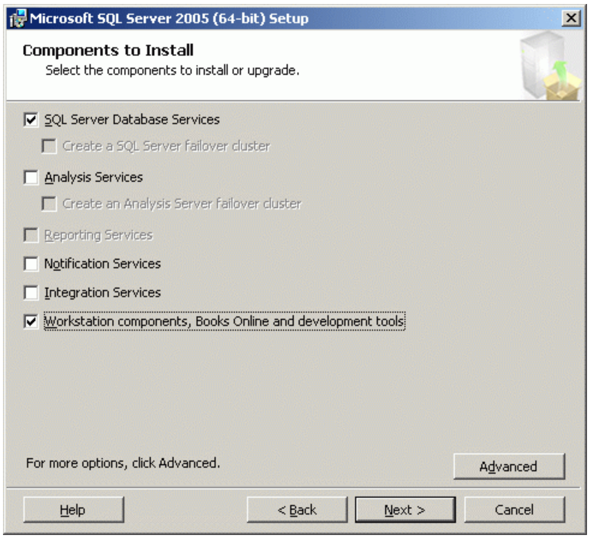
✓ **Success** — 14 Total, 12 Success, 0 Error, 2 Warning

Details:

	Action	Status	Message
⚠	IIS Feature Requirement	Warning	Messages...
✓	Pending Reboot Requirement	Success	
✓	Performance Monitor Counter Require...	Success	
✓	Default Installation Path Permission Re...	Success	
✓	Internet Explorer Requirement	Success	
✓	COM Plus Catalog Requirement	Success	
⚠	ASP.Net Version Registration Require...	Warning	Messages...
✓	Minimum MDAC Version Requirement	Success	

Click on **Next**.

3. Select the components **SQL Server Database Services** and **Workstation components...**. The latter component enables controlling the database mirroring via user interface.



Microsoft SQL Server 2005 (64-bit) Setup

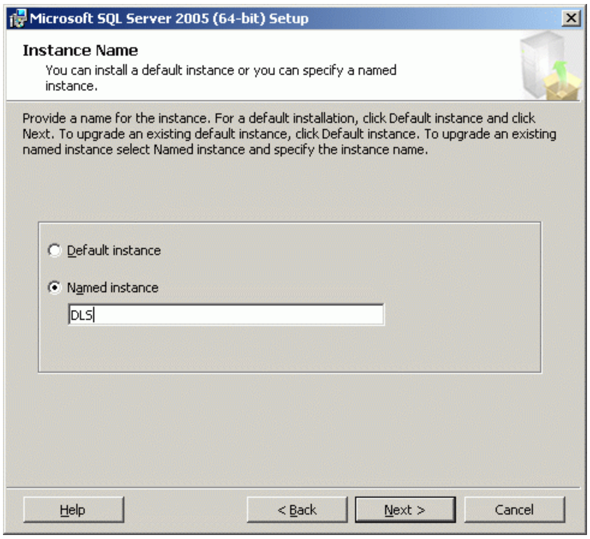
Components to Install
Select the components to install or upgrade.

☑ SQL Server Database Services
  □ Create a SQL Server failover cluster
□ Analysis Services
  □ Create an Analysis Server failover cluster
□ Reporting Services
□ Notification Services
□ Integration Services
☑ Workstation components, Books Online and development tools

For more options, click Advanced.

Click on **Next**.

4. Provide an instance name, which is the same for all SQL server, e. g. "DLS".



Microsoft SQL Server 2005 (64-bit) Setup

Instance Name

You can install a default instance or you can specify a named instance.

Provide a name for the instance. For a default installation, click Default instance and click Next. To upgrade an existing default instance, click Default instance. To upgrade an existing named instance select Named instance and specify the instance name.

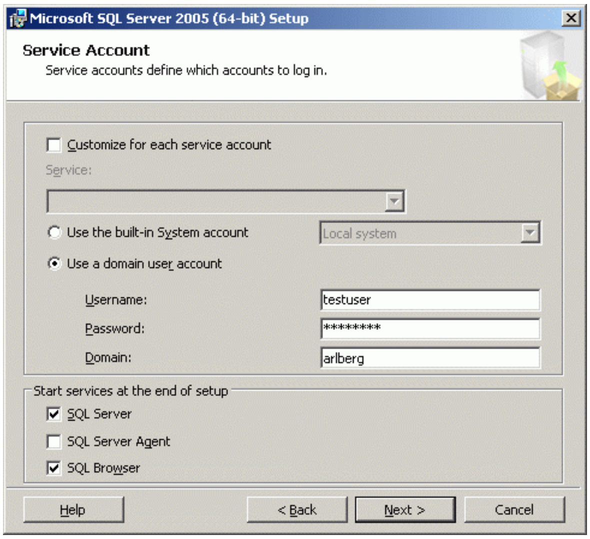
○ Default instance

● Named instance

DLS

Click on **Next**.

5. In the **Service Account** screen, select the option **Use a domain user account**. Then, in the fields **Username** and **Password**, enter the data of that user which is used by the DLS nodes to connect to the database. This user must be a member of the adminstrator group. In the **Domain** field, enter the DNS domain that is assigned to the subnet in which the DLS nodes and the database server reside. Under **Start services at the end of setup**, activate **SQL Server** and **SQL Browser**.



Microsoft SQL Server 2005 (64-bit) Setup

Service Account

Service accounts define which accounts to log in.

□ Customize for each service account

Service:

○ Use the built-in System account — Local system

● Use a domain user account

Username: testuser

Password: ********

Domain: arlberg

Start services at the end of setup

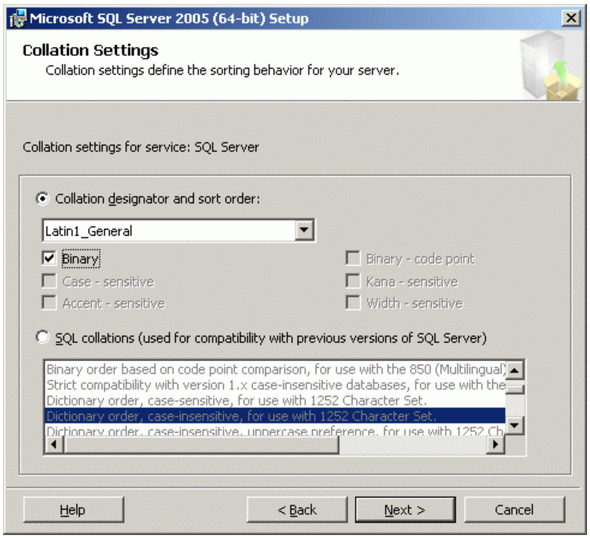
☑ SQL Server

□ SQL Server Agent

☑ SQL Browser

Click on **Next**.

6. Configure the appropriate sorting behaviour. For this purpose, activate the option **Collation designator and sort order** and choose **Latin1_General**. Activate the **Binary** option and click on **Next**.


Microsoft SQL Server 2005 (64-bit) Setup

Collation Settings
Collation settings define the sorting behavior for your server.

Collation settings for service: SQL Server

● Collation designator and sort order:

Latin1_General

☑ Binary
□ Case - sensitive
□ Accent - sensitive
□ Binary - code point
□ Kana - sensitive
□ Width - sensitive

○ SQL collations (used for compatibility with previous versions of SQL Server)

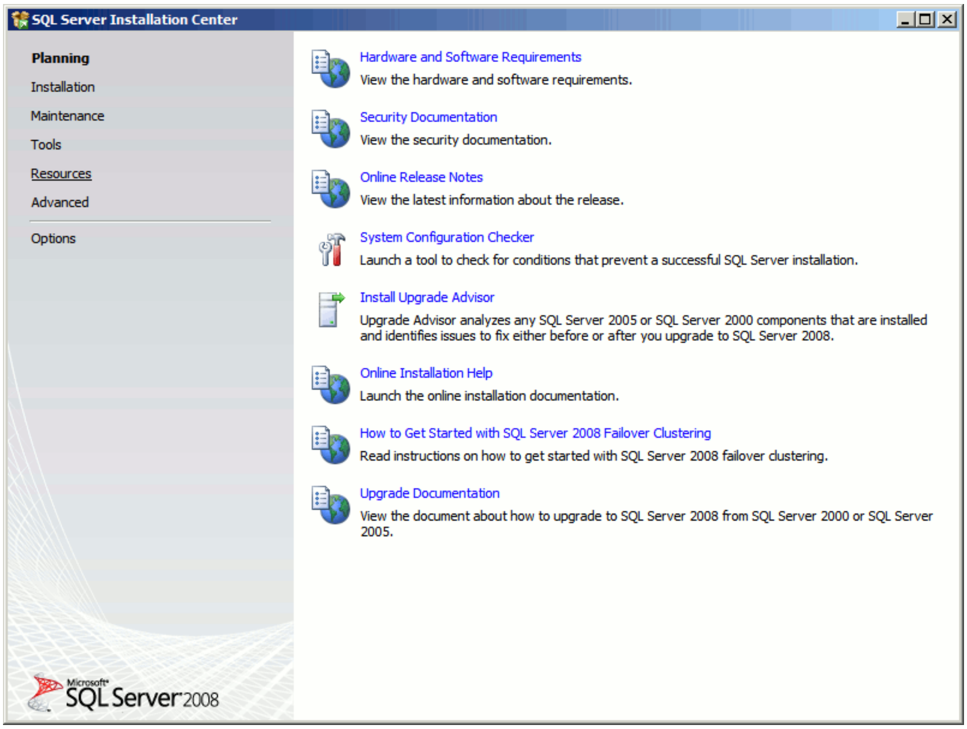
Binary order based on code point comparison, for use with the 850 (Multilingual)
Strict compatibility with version 1.x case-insensitive databases, for use with the
Dictionary order, case-sensitive, for use with 1252 Character Set.
Dictionary order, case-insensitive, for use with 1252 Character Set.
Dictionary order, case-insensitive, uppercase preference, for use with 1252 Ch

7. The installation of Microsoft SQL Server 2005 in its basic version is completed. Now, continue with the installation of Service Pack 1 for Microsoft SQL Server 2005. For this purpose, start the setup program and follow the instructions.

8. It is recommended to install Service Pack 2 for Microsoft SQL Server 2005 as well. For this purpose, start the setup program and follow the instructions.

4.2.2 Microsoft SQL Server 2008

1. Open the setup program and choose **Installation**.



Hardware and Software Requirements
View the hardware and software requirements.

Security Documentation
View the security documentation.

Online Release Notes
View the latest information about the release.

System Configuration Checker
Launch a tool to check for conditions that prevent a successful SQL Server installation.

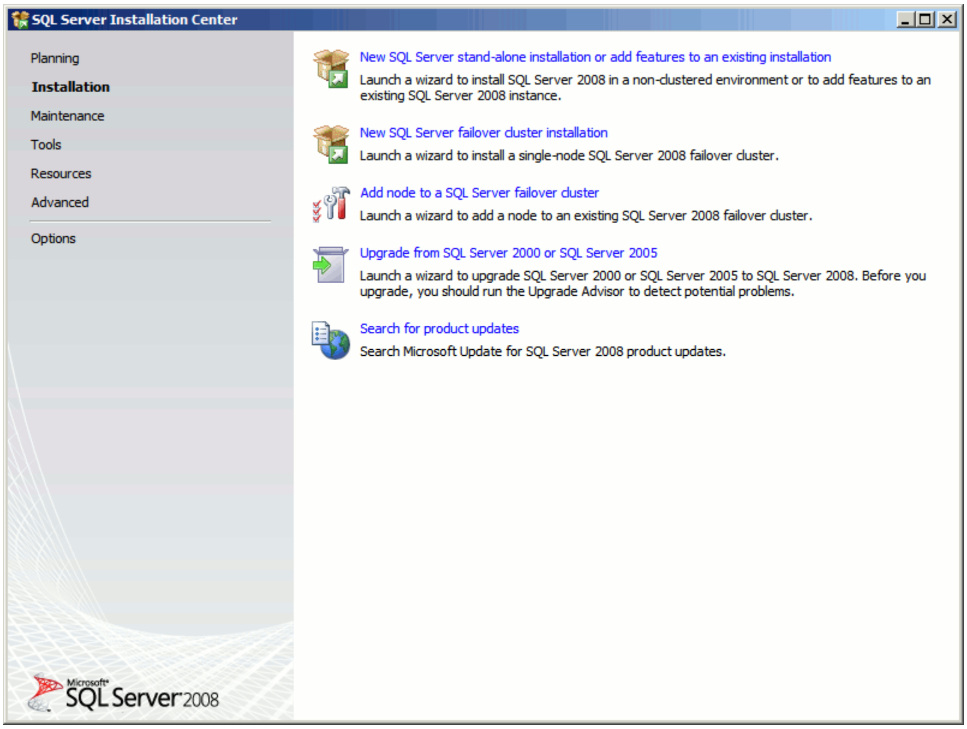
Install Upgrade Advisor
Upgrade Advisor analyzes any SQL Server 2005 or SQL Server 2000 components that are installed and identifies issues to fix either before or after you upgrade to SQL Server 2008.

Online Installation Help
Launch the online installation documentation.

How to Get Started with SQL Server 2008 Failover Clustering
Read instructions on how to get started with SQL Server 2008 failover clustering.

Upgrade Documentation
View the document about how to upgrade to SQL Server 2008 from SQL Server 2000 or SQL Server 2005.

2. Choose **New Server stand alone installation or add features to an existing installation**.



New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2008 in a non-clustered environment or to add features to an existing SQL Server 2008 instance.

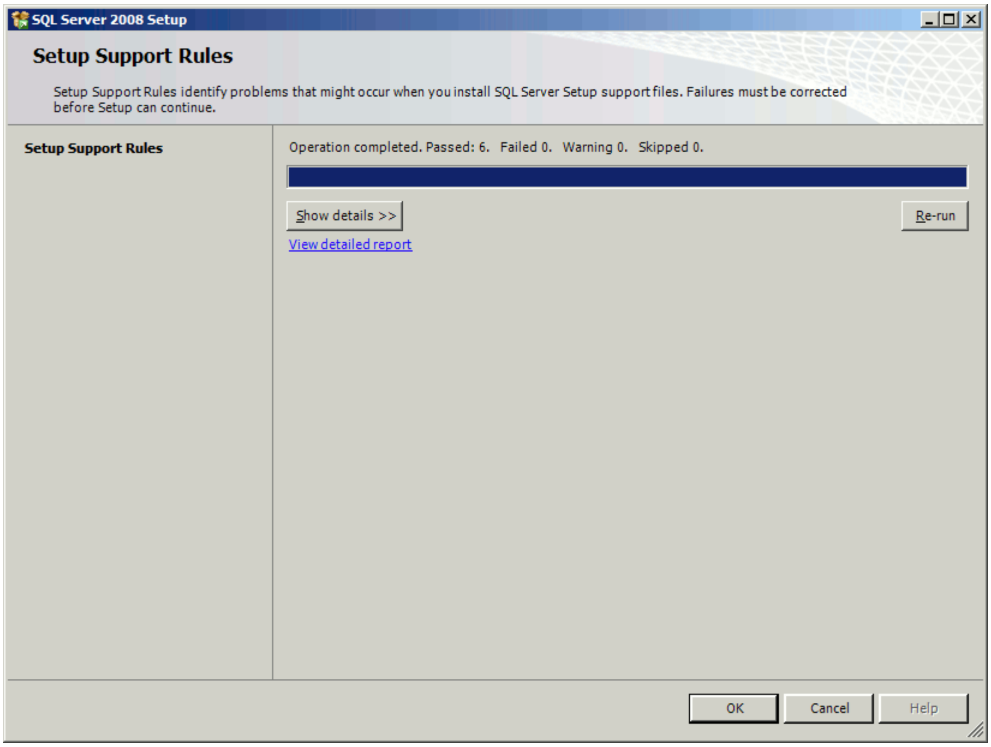
New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2008 failover cluster.

Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2008 failover cluster.

Upgrade from SQL Server 2000 or SQL Server 2005
Launch a wizard to upgrade SQL Server 2000 or SQL Server 2005 to SQL Server 2008. Before you upgrade, you should run the Upgrade Advisor to detect potential problems.

Search for product updates
Search Microsoft Update for SQL Server 2008 product updates.

3. The installation program checks the installation requirements. If the check has been successful, click **OK**.

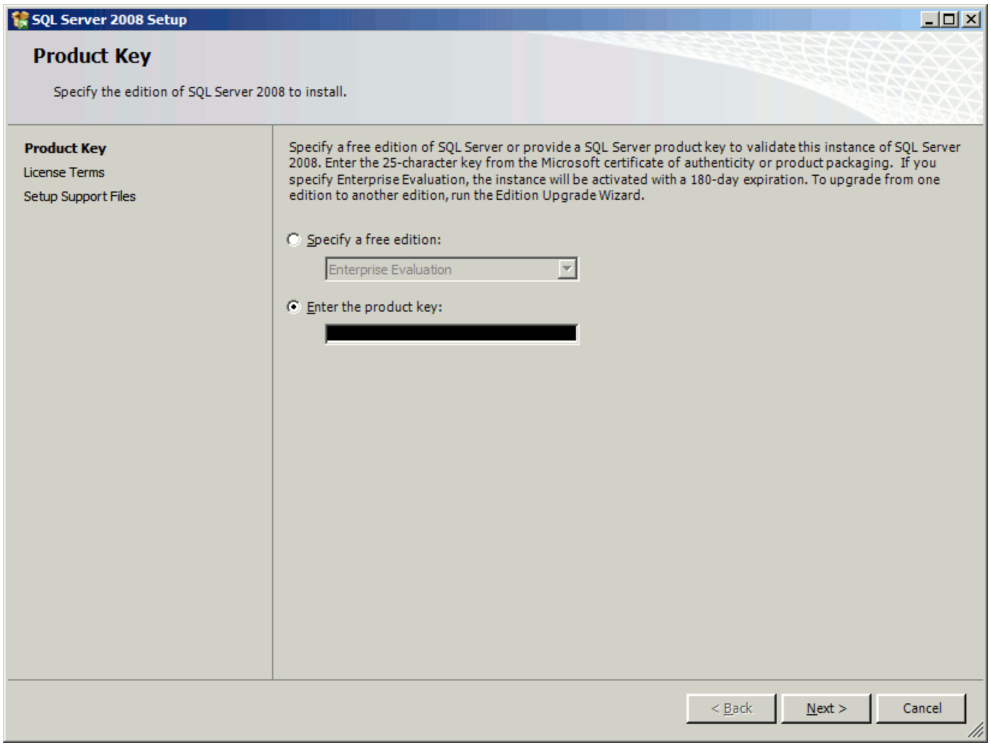

SQL Server 2008 Setup

Setup Support Rules

Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

Operation completed. Passed: 6. Failed 0. Warning 0. Skipped 0.

4. Enter the product key.


SQL Server 2008 Setup

Product Key

Specify the edition of SQL Server 2008 to install.

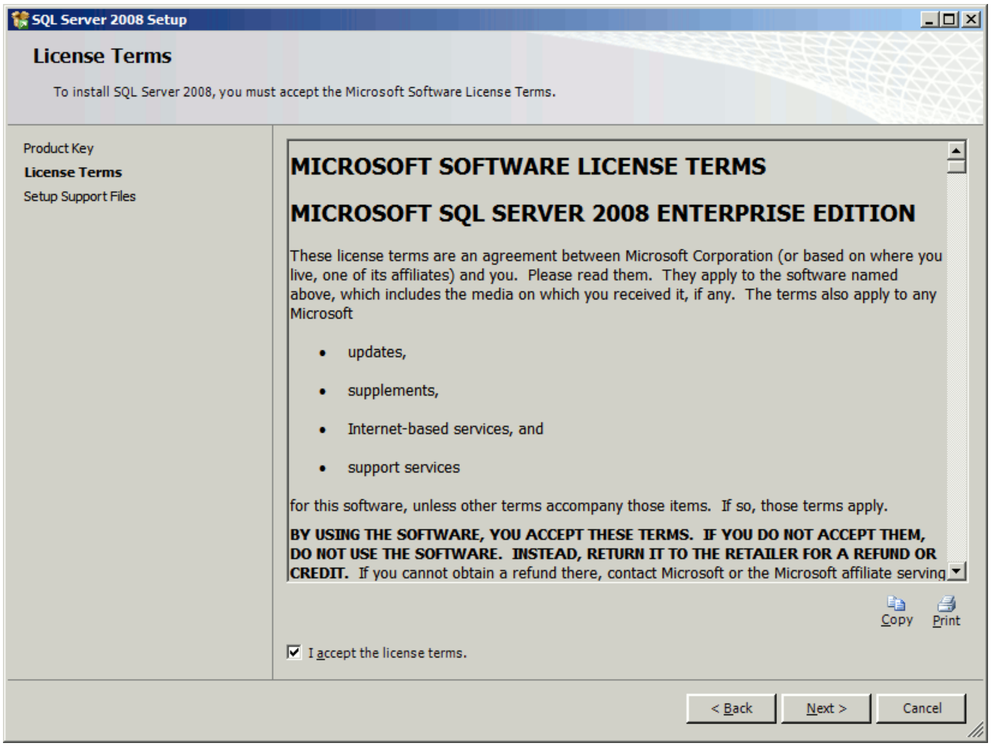
Specify a free edition of SQL Server or provide a SQL Server product key to validate this instance of SQL Server 2008. Enter the 25-character key from the Microsoft certificate of authenticity or product packaging. If you specify Enterprise Evaluation, the instance will be activated with a 180-day expiration. To upgrade from one edition to another edition, run the Edition Upgrade Wizard.

○ Specify a free edition: Enterprise Evaluation

● Enter the product key: [redacted]

Click **Next**.

5. Accept the license terms.



License Terms

To install SQL Server 2008, you must accept the Microsoft Software License Terms.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2008 ENTERPRISE EDITION

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

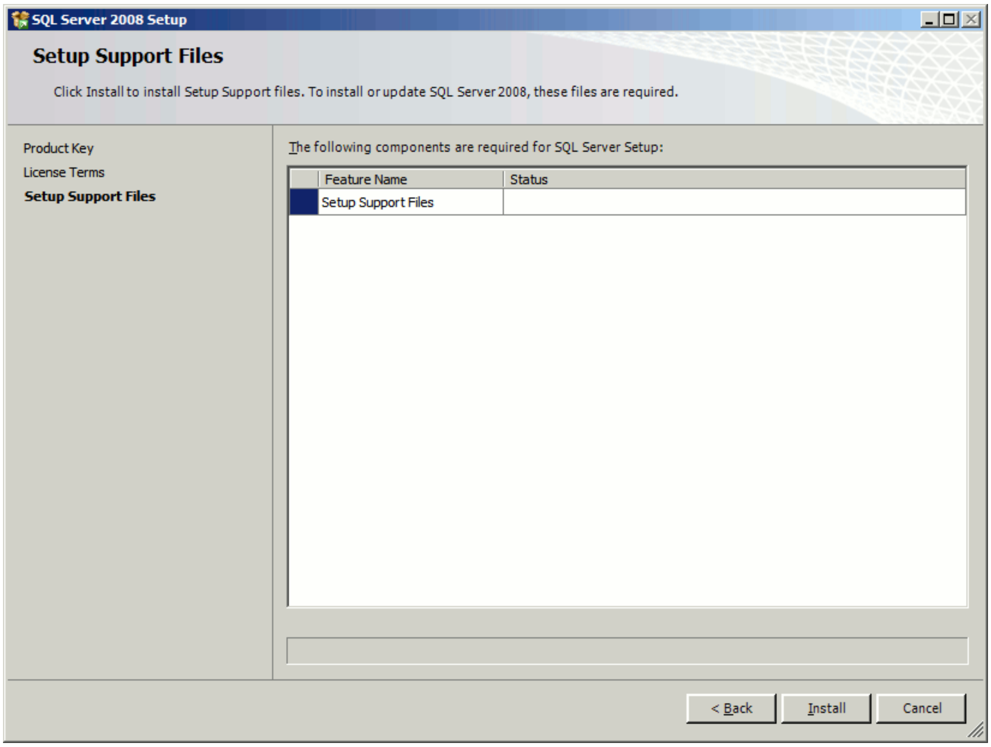
for this software, unless other terms accompany those items. If so, those terms apply.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE. INSTEAD, RETURN IT TO THE RETAILER FOR A REFUND OR CREDIT. If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving

☑ I accept the license terms.

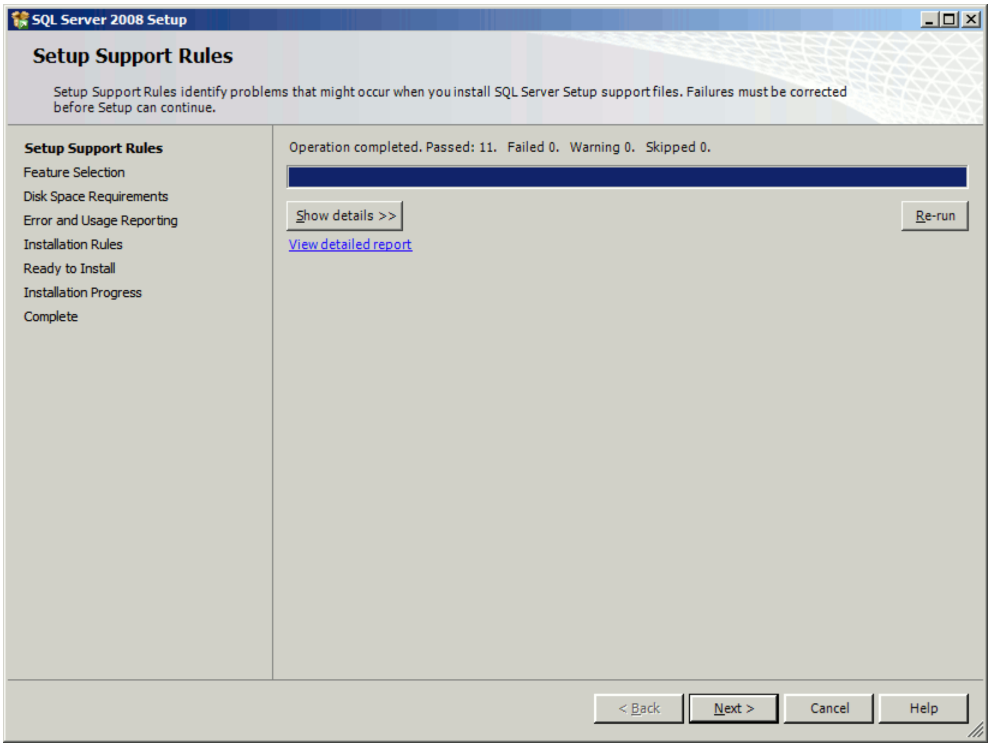
Click **Next**.

6. With **Install**, confirm the installation of the support files required for setup .



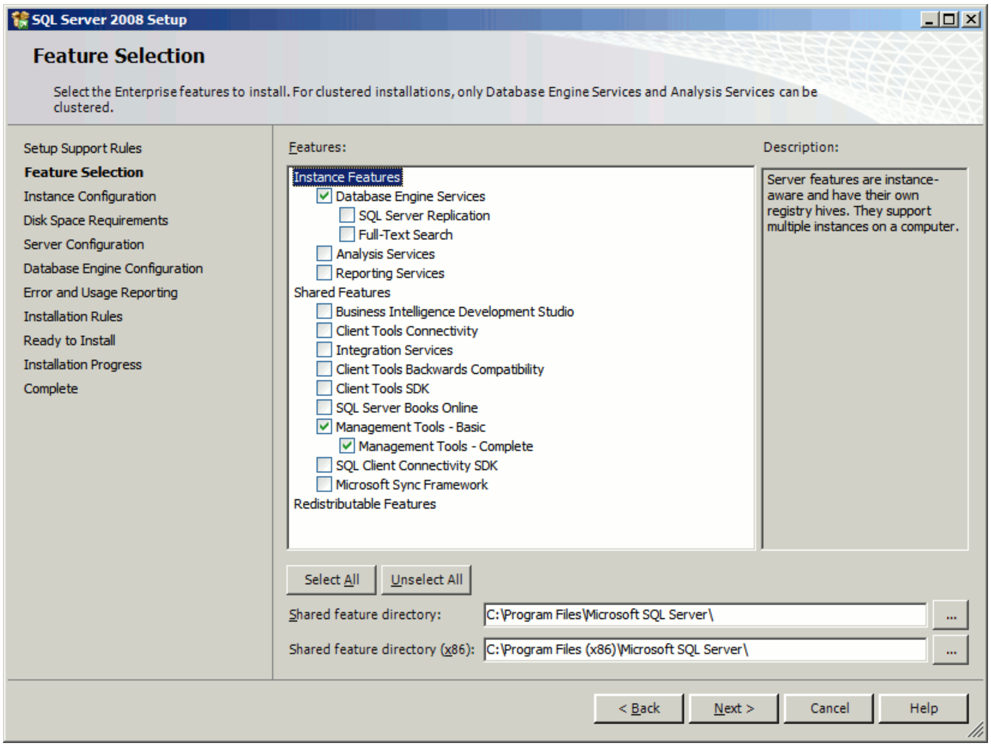
SQL Server 2008 Setup
Setup Support Files
Click Install to install Setup Support files. To install or update SQL Server 2008, these files are required.
Product Key
License Terms
Setup Support Files
The following components are required for SQL Server Setup:
Feature Name
Status
Setup Support Files
< Back
Install
Cancel

7. If the installation of the setup files has been successful, click **Next**.



SQL Server 2008 Setup
Setup Support Rules
Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.
Setup Support Rules
Feature Selection
Disk Space Requirements
Error and Usage Reporting
Installation Rules
Ready to Install
Installation Progress
Complete
Operation completed. Passed: 11. Failed 0. Warning 0. Skipped 0.
Show details >>
Re-run
View detailed report
< Back
Next >
Cancel
Help

8. Select the following features for installation: **Database Engine Services**, **Management Tools - Basic**, **Management Tools - Complete**.



Feature Selection

Select the Enterprise features to install. For clustered installations, only Database Engine Services and Analysis Services can be clustered.

- Setup Support Rules
- **Feature Selection**
- Instance Configuration
- Disk Space Requirements
- Server Configuration
- Database Engine Configuration
- Error and Usage Reporting
- Installation Rules
- Ready to Install
- Installation Progress
- Complete

Features:

Instance Features
- ☑ Database Engine Services
  - ☐ SQL Server Replication
  - ☐ Full-Text Search
- ☐ Analysis Services
- ☐ Reporting Services

Shared Features
- ☐ Business Intelligence Development Studio
- ☐ Client Tools Connectivity
- ☐ Integration Services
- ☐ Client Tools Backwards Compatibility
- ☐ Client Tools SDK
- ☐ SQL Server Books Online
- ☑ Management Tools - Basic
  - ☑ Management Tools - Complete
- ☐ SQL Client Connectivity SDK
- ☐ Microsoft Sync Framework

Redistributable Features

Description:

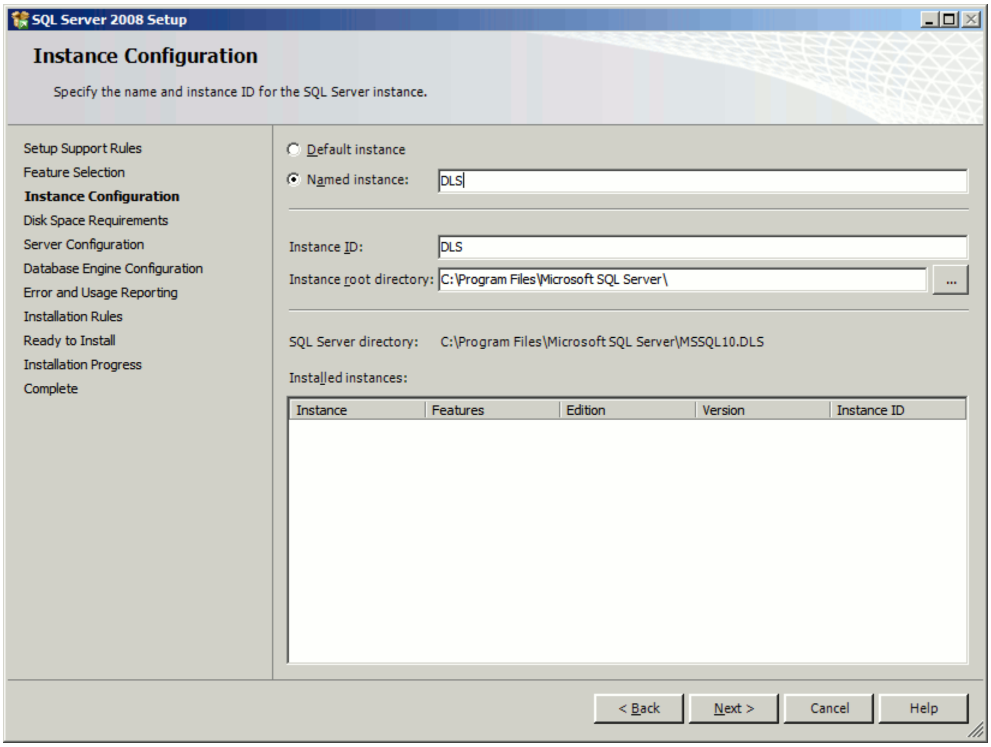
Server features are instance-aware and have their own registry hives. They support multiple instances on a computer.

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

Click **Next**.

9. Now configure the SQL server instance which is used for the DLS. For this, select **Named instance** and assign an instance name, for instance, "DLS". In **Instance root directory**, enter the root directory.



○ Default instance
● Named instance: DLS

Instance ID: DLS
Instance root directory: C:\Program Files\Microsoft SQL Server\

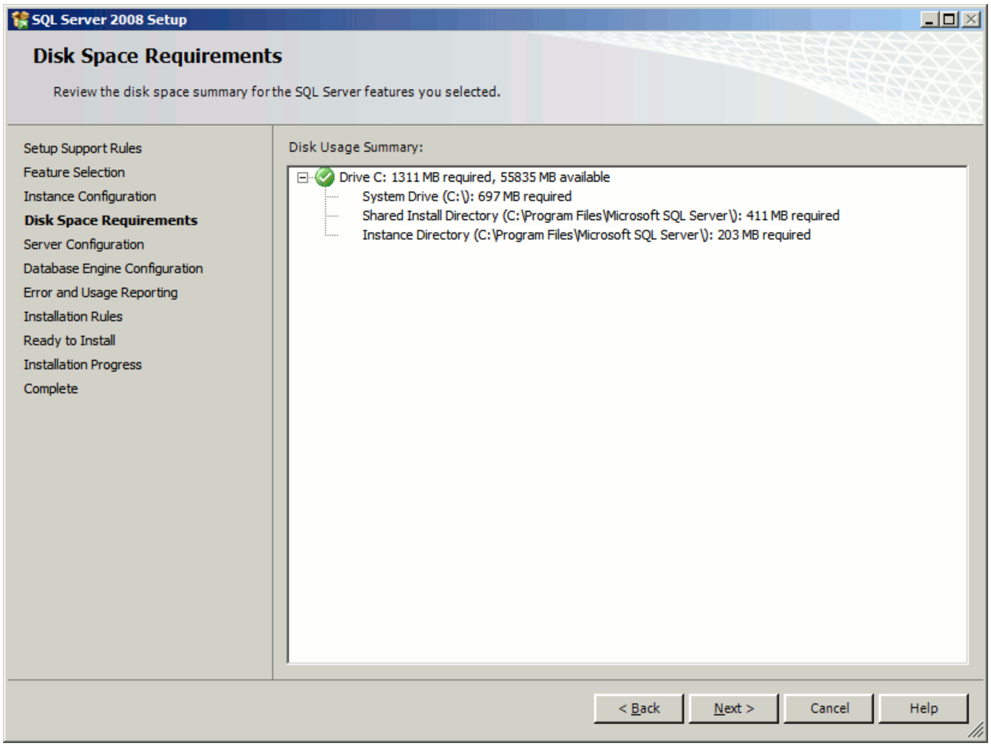
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL10.DLS

Installed instances:

Instance	Features	Edition	Version	Instance ID

Click **Next**.

10. The required disk space is displayed. Click **Next**.



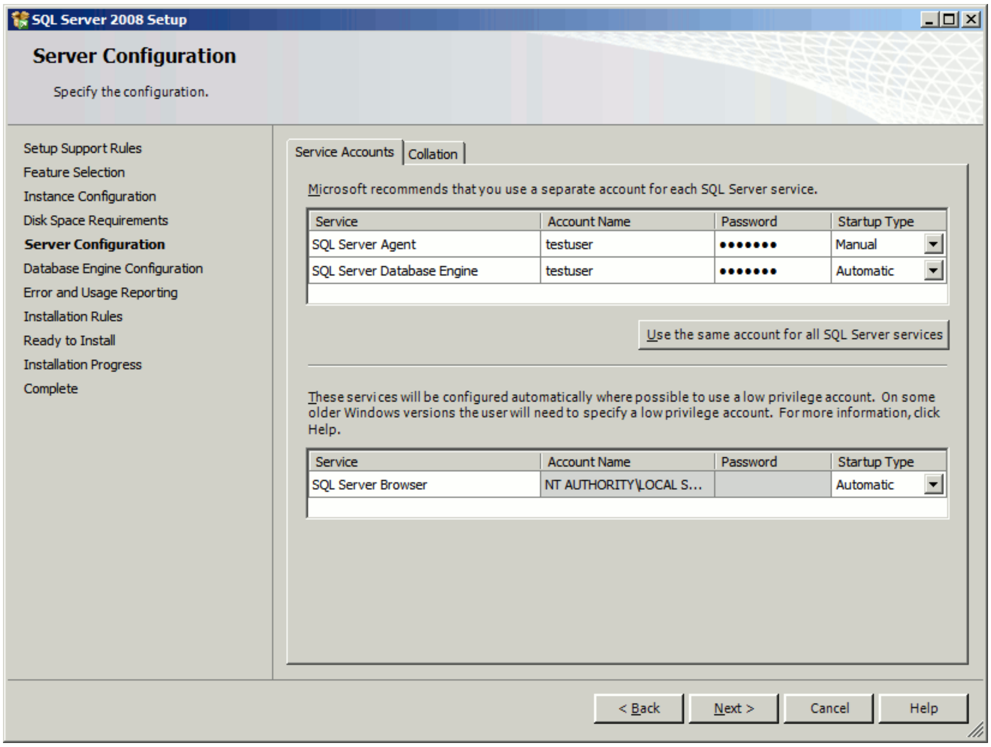
Disk Space Requirements

Review the disk space summary for the SQL Server features you selected.

Disk Usage Summary:

- ✓ Drive C: 1311 MB required, 55835 MB available
  - System Drive (C:\): 697 MB required
  - Shared Install Directory (C:\Program Files\Microsoft SQL Server\): 411 MB required
  - Instance Directory (C:\Program Files\Microsoft SQL Server\): 203 MB required

11. In the **Service Account** tab, for the services **SQL Server Agent** and **SQL Server Database Engine**, enter the data of that user which the DLS nodes utilize for connecting to the database. This user must be part of the administrators group. In Startup Type, select "Manual" for the **SQL Server Agent**, and "Automatic" for the **SQL Server Database Engine**.



Server Configuration

Specify the configuration.

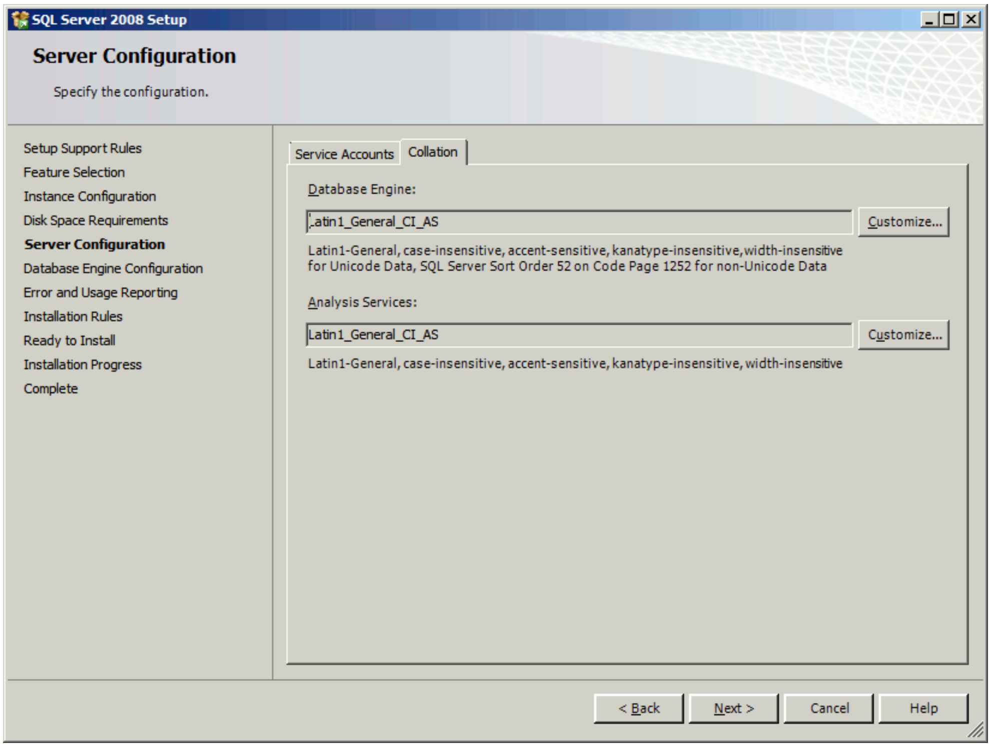
Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent	testuser	•••••••	Manual
SQL Server Database Engine	testuser	•••••••	Automatic

These services will be configured automatically where possible to use a low privilege account. On some older Windows versions the user will need to specify a low privilege account. For more information, click Help.

Service	Account Name	Password	Startup Type
SQL Server Browser	NT AUTHORITY\LOCAL S...		Automatic

12. Determine an appropriate sorting behaviour. For **Database Engine**, click **Customize**.



Database Engine:

Latin1_General_CI_AS

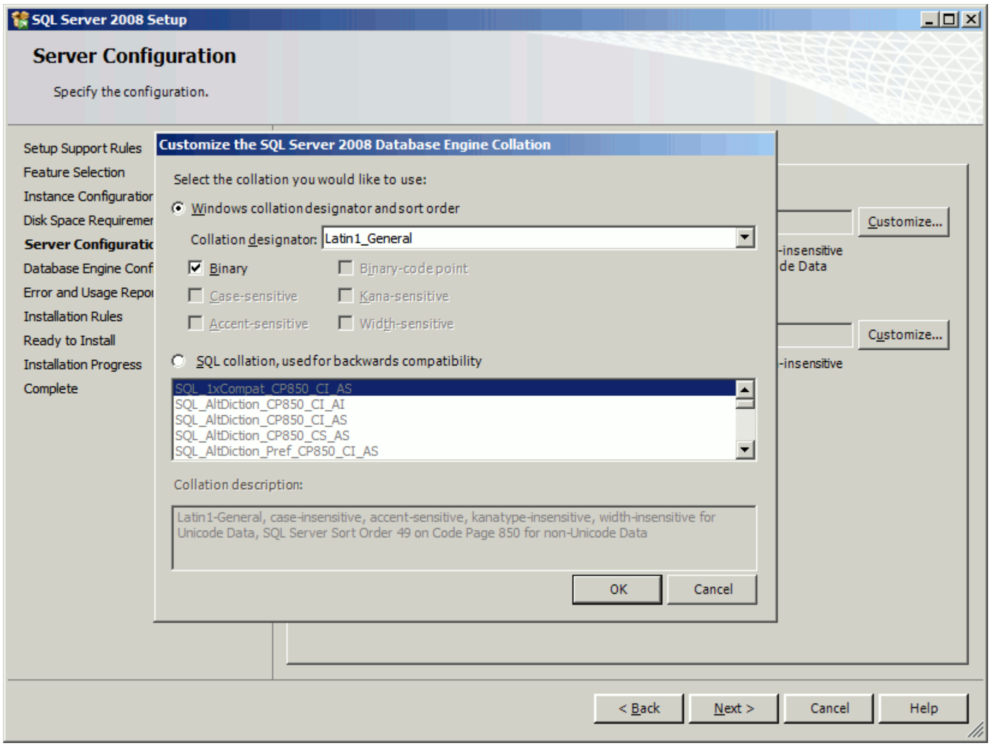
Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode Data

Analysis Services:

Latin1_General_CI_AS

Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive

13. For the collation, select **Windows collation designator and sort order**. Under **Collation designator**, select "Latin1_General". Ensure that the **Binary** option is activated.



SQL Server 2008 Setup

Server Configuration

Specify the configuration.

Setup Support Rules
Feature Selection
Instance Configuratior
Disk Space Requiremer
Server Configuratic
Database Engine Conf
Error and Usage Repoi
Installation Rules
Ready to Install
Installation Progress
Complete

Customize the SQL Server 2008 Database Engine Collation

Select the collation you would like to use:

● Windows collation designator and sort order

Collation designator: Latin1_General

☑ Binary ☐ Binary-code point
☐ Case-sensitive ☐ Kana-sensitive
☐ Accent-sensitive ☐ Width-sensitive

○ SQL collation, used for backwards compatibility

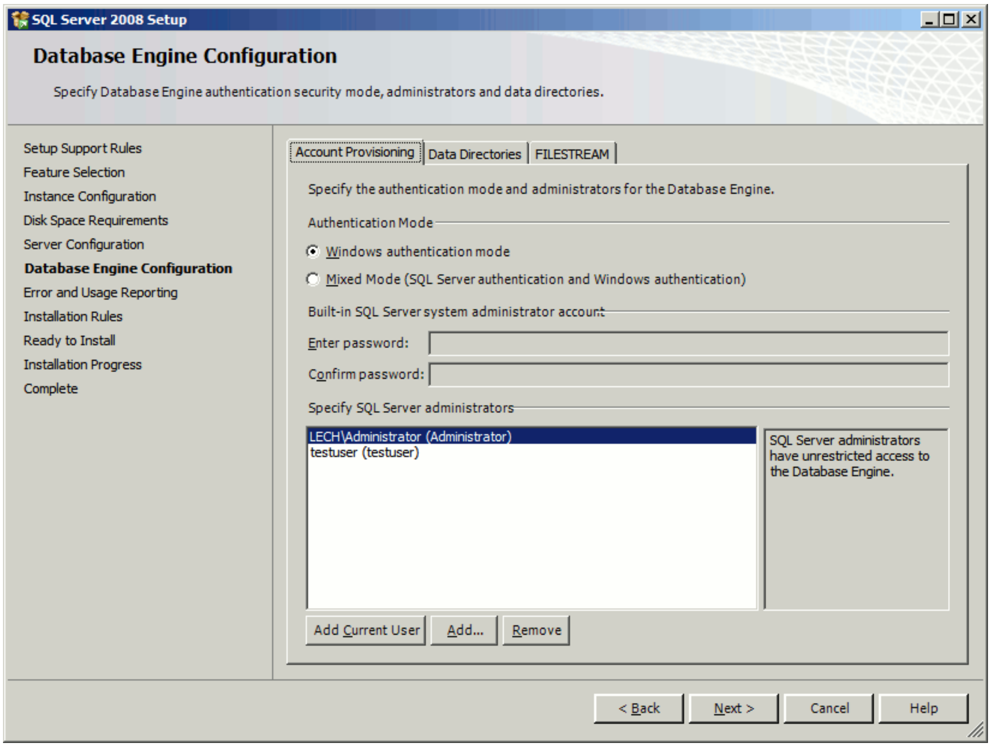
SQL_1xCompat_CP850_CI_AS
SQL_AltDiction_CP850_CI_AI
SQL_AltDiction_CP850_CI_AS
SQL_AltDiction_CP850_CS_AS
SQL_AltDiction_Pref_CP850_CI_AS

Collation description:

Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 49 on Code Page 850 for non-Unicode Data

Confirm with **OK** and click **Next**.

14. In the **Account Provisioning** tab, under **Authentication Mode**, select **Windows authentication mode**. Under **Specify SQL Server administrators**, use **Add...** to add the administrator of the database machine as well as the user account which the DLS nodes utilize for connecting to the database.



SQL Server 2008 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

● Windows authentication mode

○ Mixed Mode (SQL Server authentication and Windows authentication)

Built-in SQL Server system administrator account

Enter password:

Confirm password:

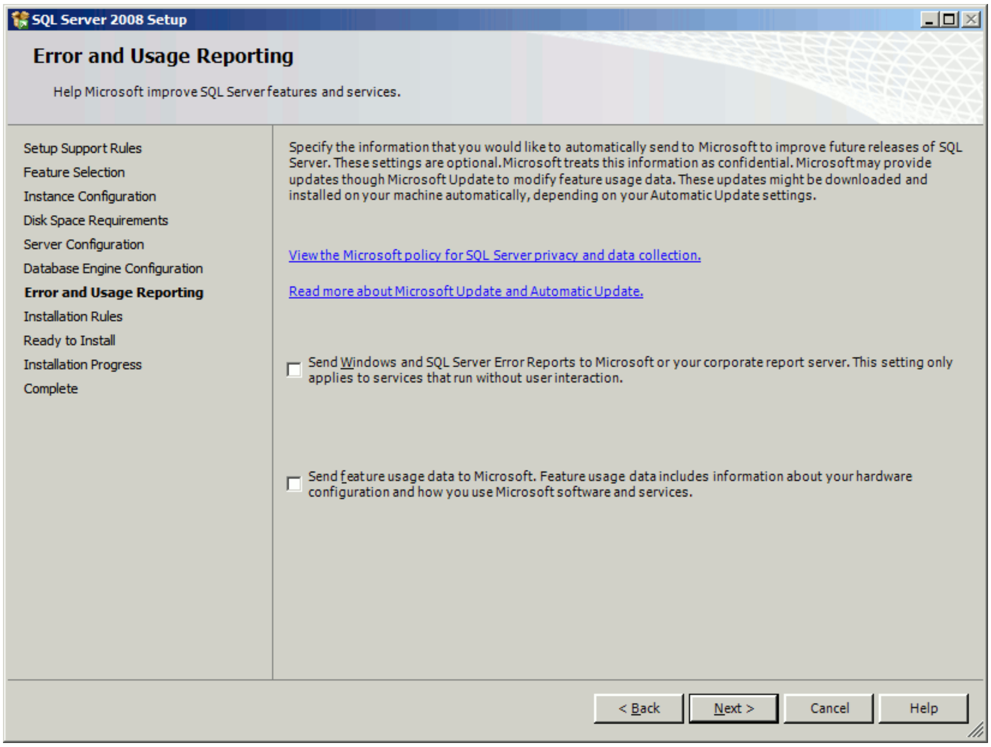
Specify SQL Server administrators

LECH\Administrator (Administrator)
testuser (testuser)

SQL Server administrators have unrestricted access to the Database Engine.

Click **Next**.

15. If you wish, activate the automatic sending of information about the SQL server operation to Microsoft.



Error and Usage Reporting

Help Microsoft improve SQL Server features and services.

Specify the information that you would like to automatically send to Microsoft to improve future releases of SQL Server. These settings are optional. Microsoft treats this information as confidential. Microsoft may provide updates though Microsoft Update to modify feature usage data. These updates might be downloaded and installed on your machine automatically, depending on your Automatic Update settings.

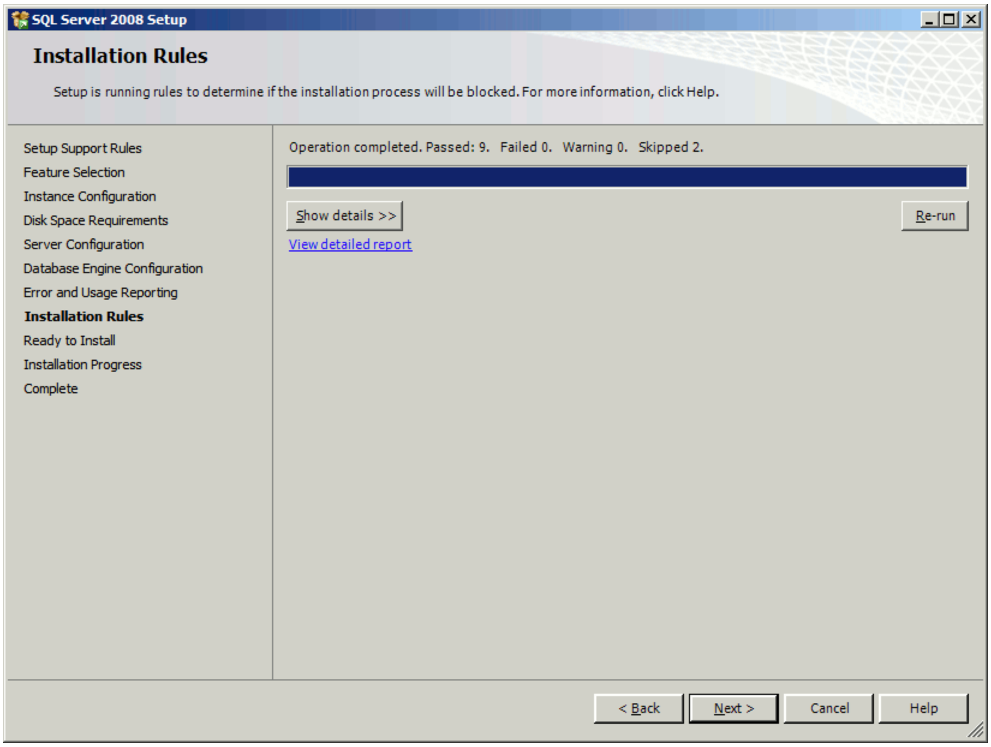
View the Microsoft policy for SQL Server privacy and data collection.

Read more about Microsoft Update and Automatic Update.

□ Send Windows and SQL Server Error Reports to Microsoft or your corporate report server. This setting only applies to services that run without user interaction.

□ Send feature usage data to Microsoft. Feature usage data includes information about your hardware configuration and how you use Microsoft software and services.

16. The installation program checks if the installation can be accomplished without problems.

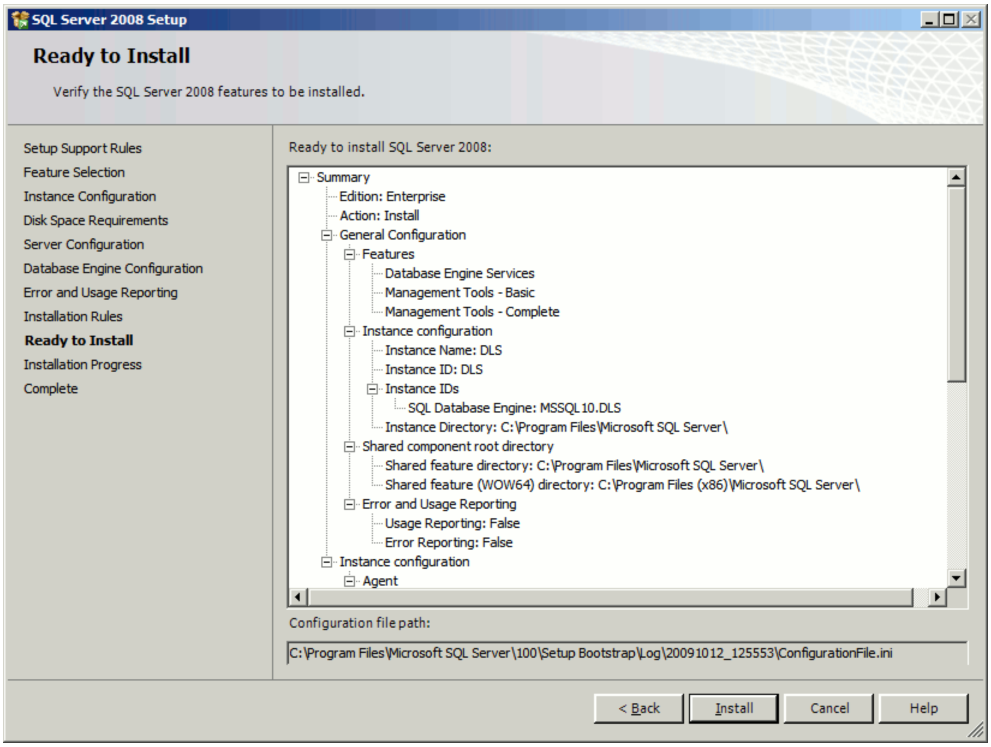


Setup is running rules to determine if the installation process will be blocked. For more information, click Help.

Operation completed. Passed: 9. Failed 0. Warning 0. Skipped 2.

If the check has been successful, click **Next**.

17. The components and configurations which are scheduled for installation are displayed.



Ready to Install

Verify the SQL Server 2008 features to be installed.

Ready to install SQL Server 2008:

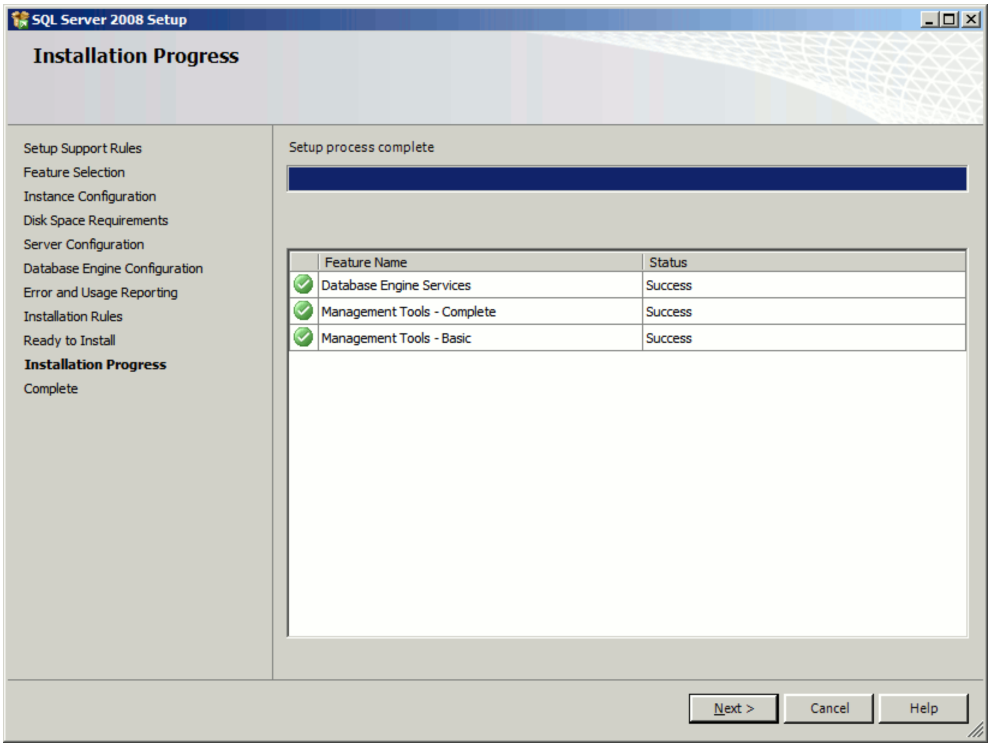
```
Summary
  Edition: Enterprise
  Action: Install
  General Configuration
    Features
      Database Engine Services
      Management Tools - Basic
      Management Tools - Complete
    Instance configuration
      Instance Name: DLS
      Instance ID: DLS
      Instance IDs
        SQL Database Engine: MSSQL10.DLS
      Instance Directory: C:\Program Files\Microsoft SQL Server\
    Shared component root directory
      Shared feature directory: C:\Program Files\Microsoft SQL Server\
      Shared feature (WOW64) directory: C:\Program Files (x86)\Microsoft SQL Server\
    Error and Usage Reporting
      Usage Reporting: False
      Error Reporting: False
  Instance configuration
    Agent
```

Configuration file path:

C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20091012_125553\ConfigurationFile.ini

If the settings are as desired, click **Next**.

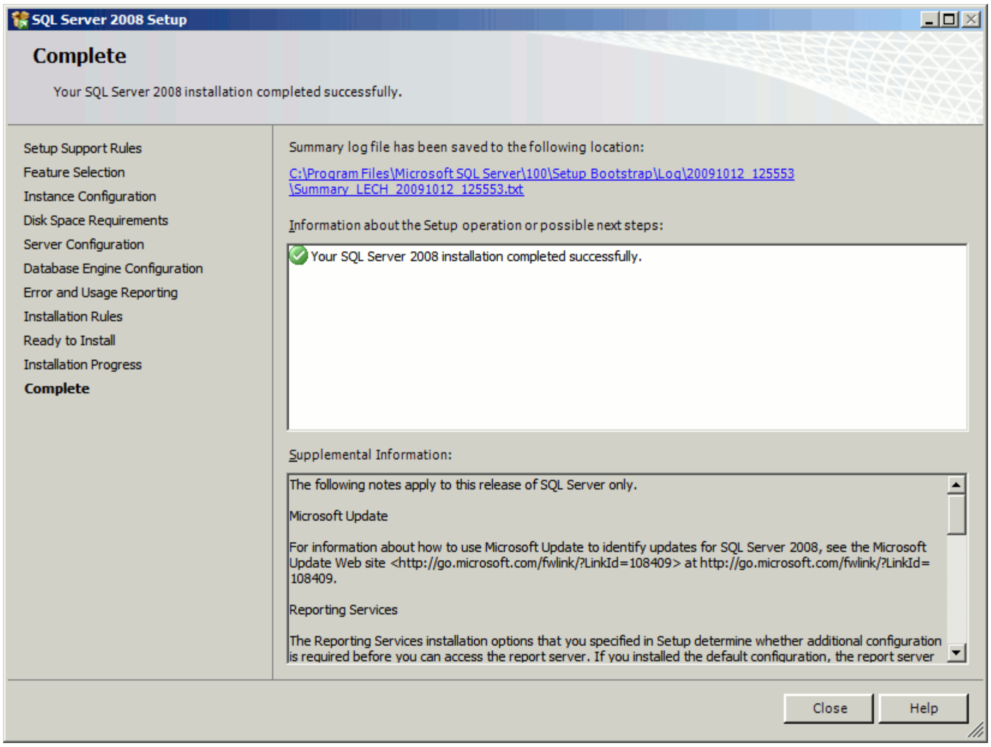
18. If the installation has been successful, click **Next**.



Setup process complete

	Feature Name	Status
✓	Database Engine Services	Success
✓	Management Tools - Complete	Success
✓	Management Tools - Basic	Success

19. Now you can exit the installation program by clicking on **Close**.



Complete

Your SQL Server 2008 installation completed successfully.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20091012_125553\Summary_LECH_20091012_125553.txt

Information about the Setup operation or possible next steps:

✓ Your SQL Server 2008 installation completed successfully.

Supplemental Information:

The following notes apply to this release of SQL Server only.

Microsoft Update

For information about how to use Microsoft Update to identify updates for SQL Server 2008, see the Microsoft Update Web site <http://go.microsoft.com/fwlink/?LinkId=108409> at http://go.microsoft.com/fwlink/?LinkId=108409.

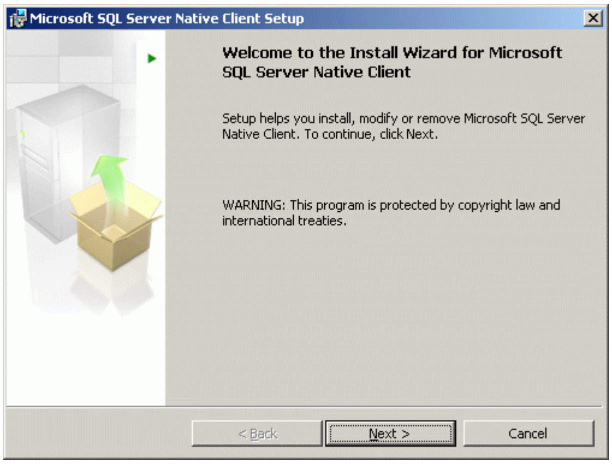
Reporting Services

The Reporting Services installation options that you specified in Setup determine whether additional configuration is required before you can access the report server. If you installed the default configuration, the report server

4.2.3 SQL Native Client - When a Remote Database is Used

A Microsoft SQL Native Client installation is required when a Microsoft SQL database, perhaps from a former DLS installation, does not yet exist. If the operating system is a 32 bit variant, the Native Client is installed by the DLS installation routine. When a 64 bit system is used, the installation must be executed separately.

1. Start the setup program.



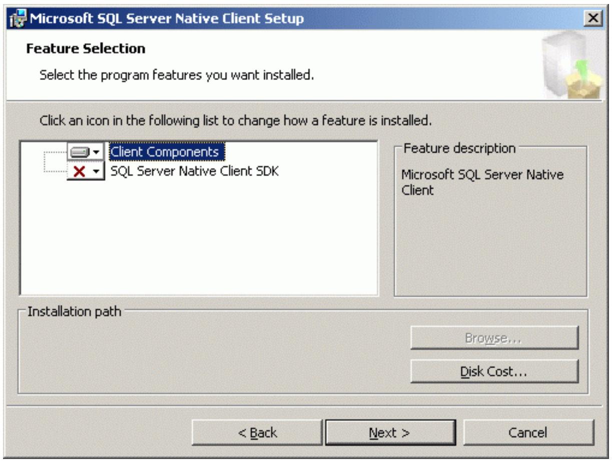
Microsoft SQL Server Native Client Setup

Welcome to the Install Wizard for Microsoft SQL Server Native Client

Setup helps you install, modify or remove Microsoft SQL Server Native Client. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. Follow the instructions in the particular screens and click **Next**. In the **Feature Selection** screen, select **SQL Server Native Client SDK**.



Microsoft SQL Server Native Client Setup

Feature Selection

Select the program features you want installed.

Click an icon in the following list to change how a feature is installed.

Client Components
SQL Server Native Client SDK

Feature description

Microsoft SQL Server Native Client

Installation path

3. Continue the installation until it is completed.

4.2.4 Change Service Password

If a password change should be necessary, go to

`<Installationsverzeichnis>\Tomcat5\webapps\DeploymentService\database`

and execute `dlsSetServicePW.bat <new password>`.

After this, change the password for the service 'DeploymentService' on each DLS node.

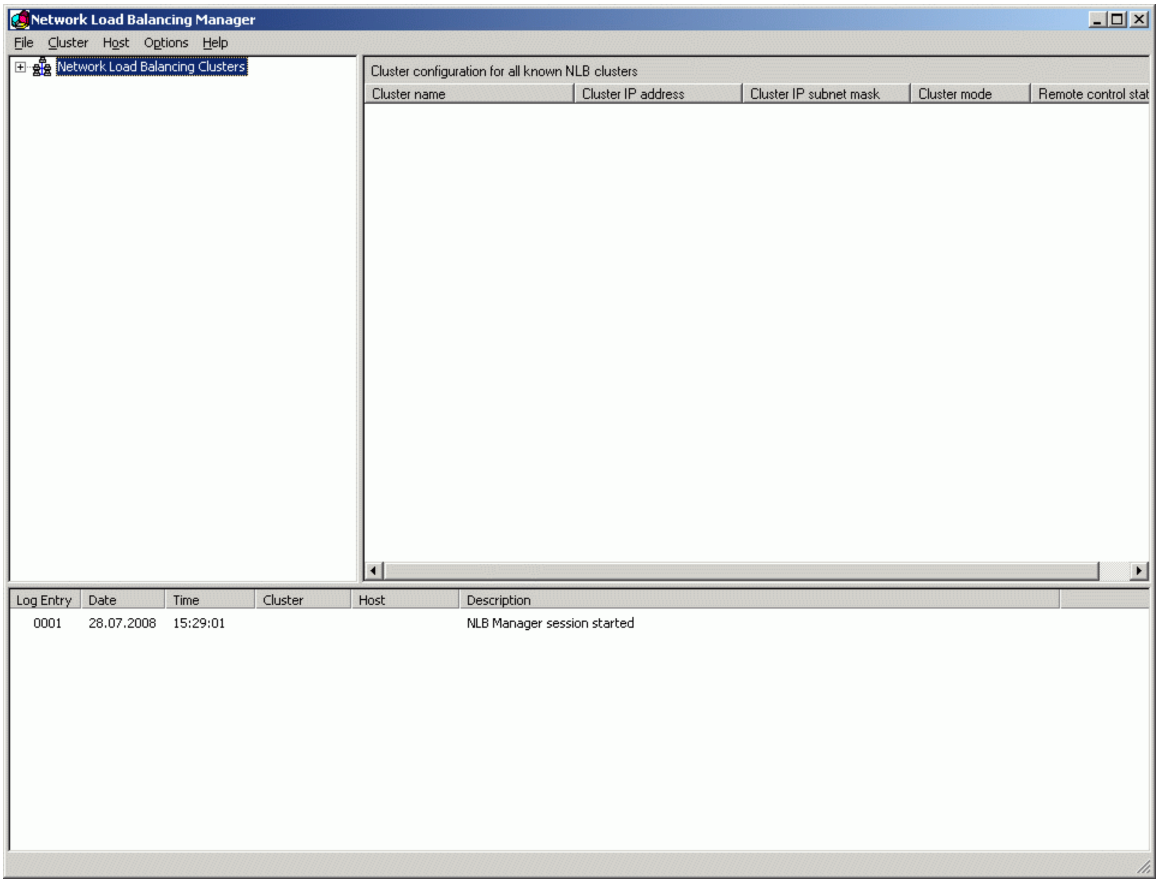
4.3 Configure the Network Load Balancer

For cluster operation, a network load balancer is required. A description of the Network Load Balancer, as included in Windows Server 2003/2008, will follow. (Alternatively, any other network load balancer may be used, as long as it has the same functionality.)

4.3.1 Network Load Balancer for Windows Server 2003

> Some configuration steps may take up to 1 minute or so. In such cases, wait until the step is completed, and do not input anything.

1. On one of the node machines, call **Start** > **Administrative Tools** > **Network Load Balancer Manager**. Thereby, the service is activated on all node machines, which is necessary for cluster operation.
2. A tripartite configuration screen opens. To build a new cluster, go to **Cluster** > **New** in the menu or use the right-hand mouse key to call the context menu and select **New Cluster**.

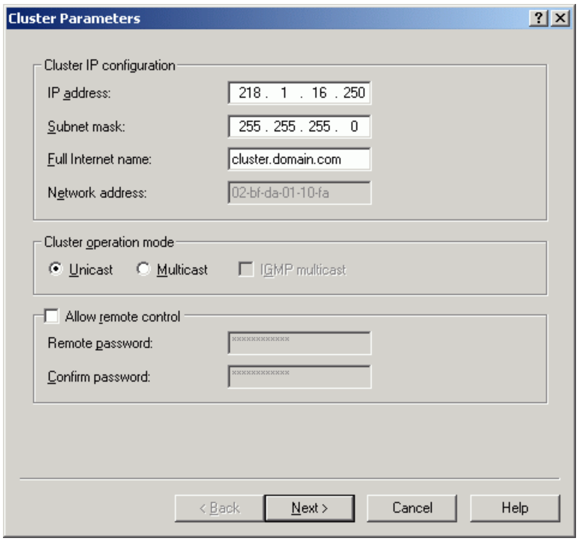

Network Load Balancing Manager
File Cluster Host Options Help
Network Load Balancing Clusters
Cluster configuration for all known NLB clusters

Cluster name	Cluster IP address	Cluster IP subnet mask	Cluster mode	Remote control stat

Log Entry	Date	Time	Cluster	Host	Description
0001	28.07.2008	15:29:01			NLB Manager session started

3. In the **Cluster Parameters** screen enter the following parameters:

- **IP address**: Address under which the DLS cluster can be reached ("virtual IP address").
- **Subnet mask**: Subnet mask for the cluster.
- **Full internet name**: DNS name under which the DLS cluster is reachable from outside.
- **Cluster operation mode**: Select **Unicast**. With this setting, all network interfaces in the outer network will be assigned the same MAC address. Thus, inbound data packets are initially received by all node machines and then filtered by the network load balancer.
- **Allow remote control**: Enable the remote control and provide a strong password to prevent abuse. Remember this password in order to communicate it to the DLS (see Section 4.5.3.1, "First Node", Step 15).



Cluster Parameters

Cluster IP configuration

IP address: 218 . 1 . 16 . 250

Subnet mask: 255 . 255 . 255 . 0

Full Internet name: cluster.domain.com

Network address: 02-bf-da-01-10-fa

Cluster operation mode

● Unicast ○ Multicast □ IGMP multicast

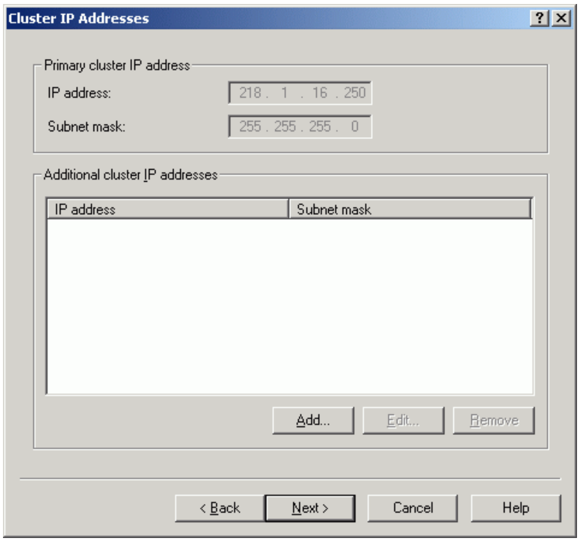
□ Allow remote control

Remote password: ************

Confirm password: ************

Click on **Next**.

4. Now the new cluster can be populated with IP addresses. In the **Cluster IP Addresses screen**, click on **Add**.



Cluster IP Addresses

Primary cluster IP address

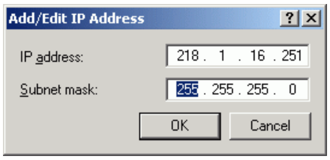
IP address: 218 . 1 . 16 . 250

Subnet mask: 255 . 255 . 255 . 0

Additional cluster IP addresses

IP address	Subnet mask

5. The screen **Add/Edit IP Address** appears, in which you enter the IP address and subnet mask of the first node machine.



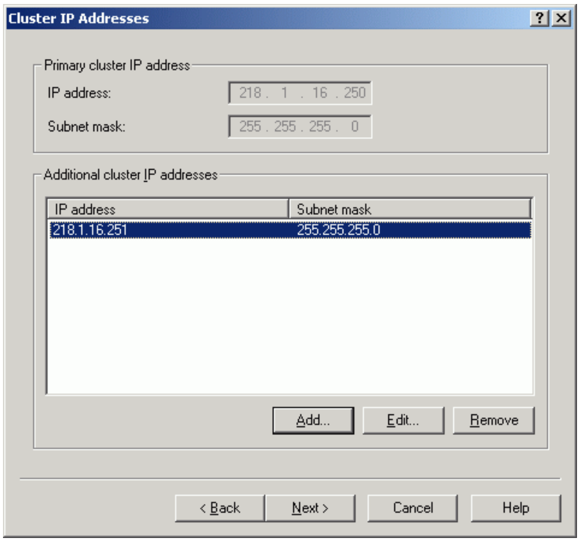
Add/Edit IP Address

IP address: 218 . 1 . 16 . 251

Subnet mask: 255 . 255 . 255 . 0

After this, click on **OK**.

6. You get back to the **Cluster IP Adresses** screen. The newly entered machine now appears under **Additional cluster IP adresses**.



Cluster IP Addresses

Primary cluster IP address

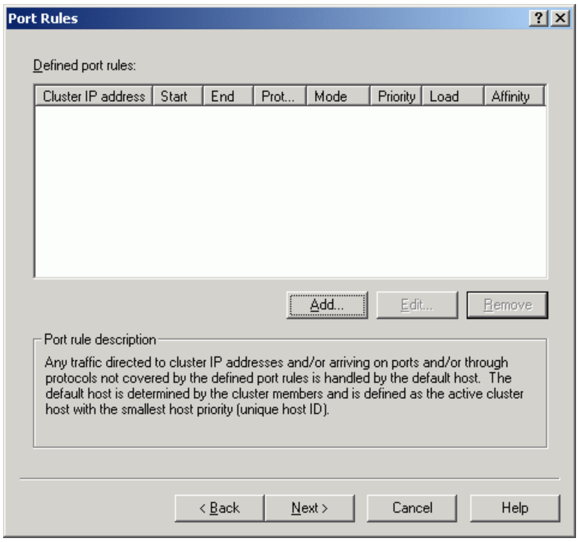
IP address: 218 . 1 . 16 . 250

Subnet mask: 255 . 255 . 255 . 0

Additional cluster IP addresses

IP address	Subnet mask
218.1.16.251	255.255.255.0

7. Click on **Next**. In the **Port Rules** screen, you set the rules for those ports over which the DLS cluster communicates with the outside world. In case there are some port rules already, remove these with **Remove**.



Port Rules

Defined port rules:

Cluster IP address	Start	End	Prot...	Mode	Priority	Load	Affinity

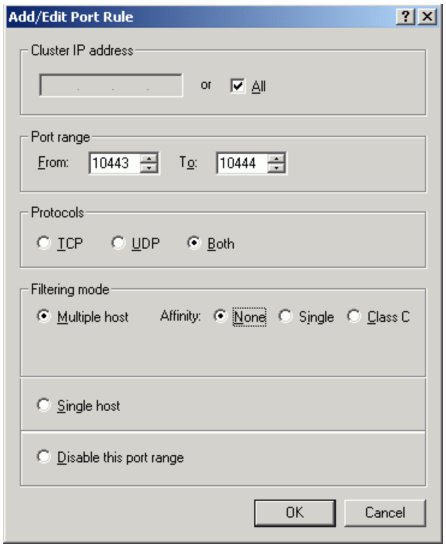
Port rule description

Any traffic directed to cluster IP addresses and/or arriving on ports and/or through protocols not covered by the defined port rules is handled by the default host. The default host is determined by the cluster members and is defined as the active cluster host with the smallest host priority (unique host ID).

Click on **Add**.

8. The screen **Add/Edit Port Rule** opens. Enter the parameters for the ports resp. port ranges, as appropriate. Under **Cluster IP address**, enter **All** in order to assign the rule to all IP addresses within the cluster. Under **Affinity**, select **None**. With this setting, it is possible that consecutive requests from one and the same IP address are handled by different nodes. Thus it is ensured that the loads are distributed equally.

The following screenshot shows the settings for the ports 10443 and 10444. (For the functions of these ports, please see step 9.)



Add/Edit Port Rule

Cluster IP address: or ☑ All

Port range: From: 10443 To: 10444

Protocols: ○ TCP ○ UDP ● Both

Filtering mode: ● Multiple host Affinity: ● None ○ Single ○ Class C

○ Single host

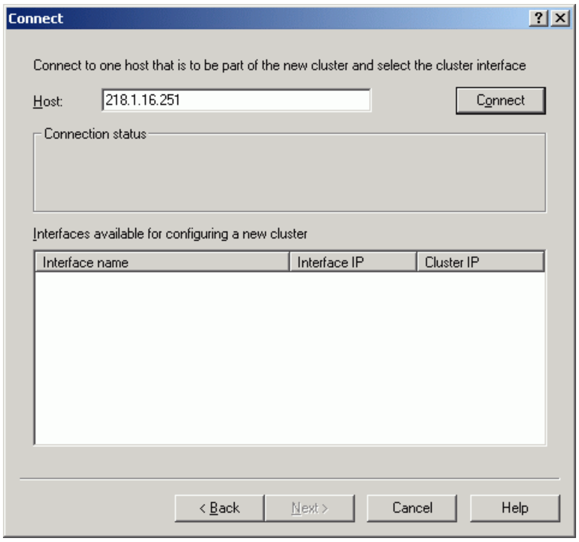
○ Disable this port range

9. Enter the rules for the remaining ports, as described in steps 7 and 8. In the following, the ports elementary for the DLS are listed (in the Release Notes, you can find a list of all DLS ports).

   - 10443: Receives data from the graphical user interface, that is, from the web browser, when HTTPS is used.
   - 10444: Receives data over HTTPS from the DlsAPI, which is the web service interface of the DLS.
   - 18080: Receives data from the graphical user interface, that is, from the web browser, when HTTP is used.
   - 18443: Receives data from the end devices (HTTP and HTTPS).
   - 18444: Receives data from the end devices when a secure connection between DLS and end device is established (secure mode).

   When you have entered all port rules, click on **Next**.

10. Now the individual node machines are interconnected to form a cluster. In the **Connect** screen, in the **Host** field, enter the IP address of the first node machine.



Connect

Connect to one host that is to be part of the new cluster and select the cluster interface

Host: 218.1.16.251

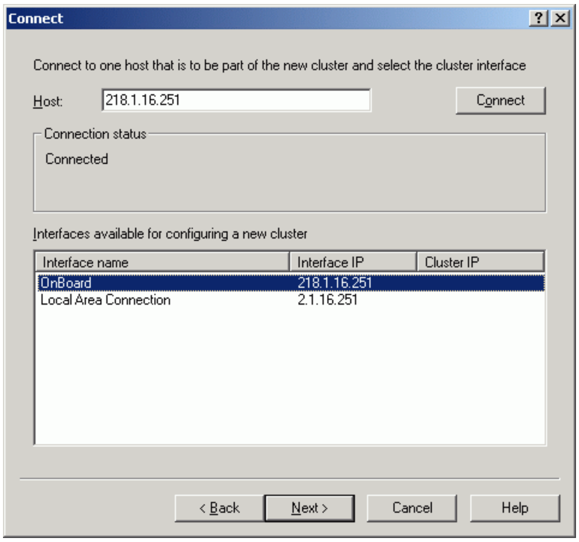
Connection status

Interfaces available for configuring a new cluster

Interface name	Interface IP	Cluster IP

Afterwards, click on **Connect**.

11. Under **Interfaces available for configuring a new cluster** you find all network interfaces of the newly added machine now. To get to the **Host Parameters** screen, mark that network card that resides in the outward network.



Connect

Connect to one host that is to be part of the new cluster and select the cluster interface

Host: 218.1.16.251

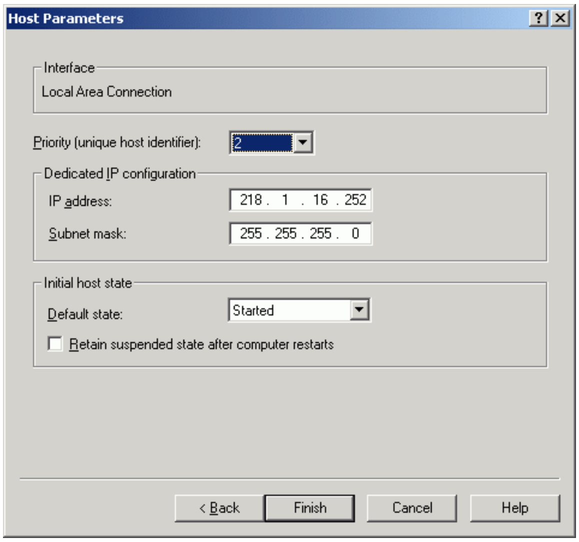
Connection status
Connected

Interfaces available for configuring a new cluster

Interface name	Interface IP	Cluster IP
OnBoard	218.1.16.251	
Local Area Connection	2.1.16.251	

Afterwards, click on **Next**.

12. In the field **Priority**, a pre-defined value is displayed, which is a mere numeration and does not imply a prioritization. The **IP address** field contains the IP address of the network interface.



Host Parameters

Interface
Local Area Connection

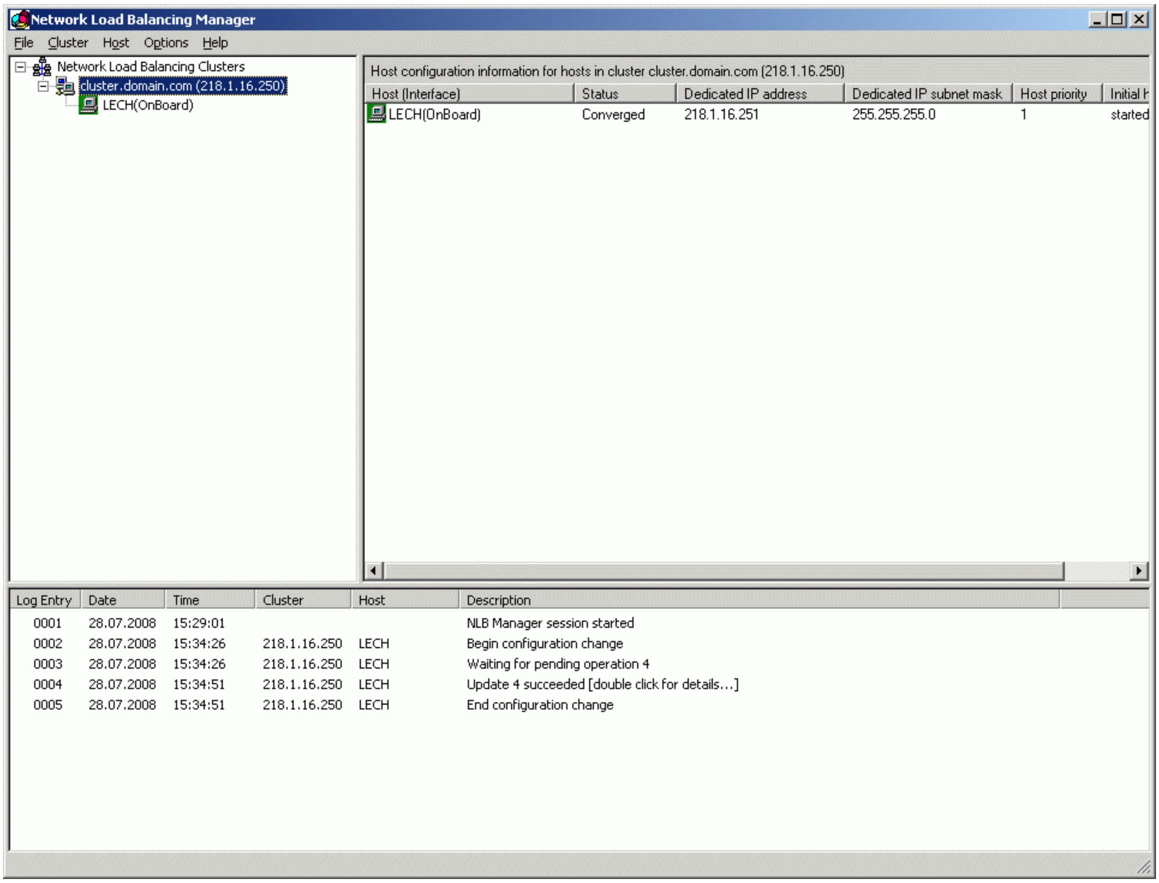
Priority (unique host identifier): 2

Dedicated IP configuration
IP address: 218 . 1 . 16 . 252
Subnet mask: 255 . 255 . 255 . 0

Initial host state
Default state: Started
□ Retain suspended state after computer restarts

When all values are correct, click on **Finish**. The process of adding a node to the cluster may take 1-2 minutes.

13. You get to the main screen of the **Network Load Balancing Manager**, where the cluster in its current composition is displayed. When the addition of the node machine has been successful, the **Status** is set to **Converged**.


Network Load Balancing Manager
File Cluster Host Options Help
Network Load Balancing Clusters
cluster.domain.com (218.1.16.250)
LECH(OnBoard)

Host configuration information for hosts in cluster cluster.domain.com (218.1.16.250)

Host (Interface)	Status	Dedicated IP address	Dedicated IP subnet mask	Host priority	Initial h
LECH(OnBoard)	Converged	218.1.16.251	255.255.255.0	1	started

```
Log Entry  Date        Time      Cluster       Host  Description
0001       28.07.2008  15:29:01                      NLB Manager session started
0002       28.07.2008  15:34:26  218.1.16.250  LECH  Begin configuration change
0003       28.07.2008  15:34:26  218.1.16.250  LECH  Waiting for pending operation 4
0004       28.07.2008  15:34:51  218.1.16.250  LECH  Update 4 succeeded [double click for details...]
0005       28.07.2008  15:34:51  218.1.16.250  LECH  End configuration change
```

In the **Cluster** menu, go to **Add Host** or use the right-hand mouse key to call the context menu and then go to **Add Host to Cluster** in order to add another node machine.

14. For the next as well as for all further node machines proceed as described in step 10 to 12.

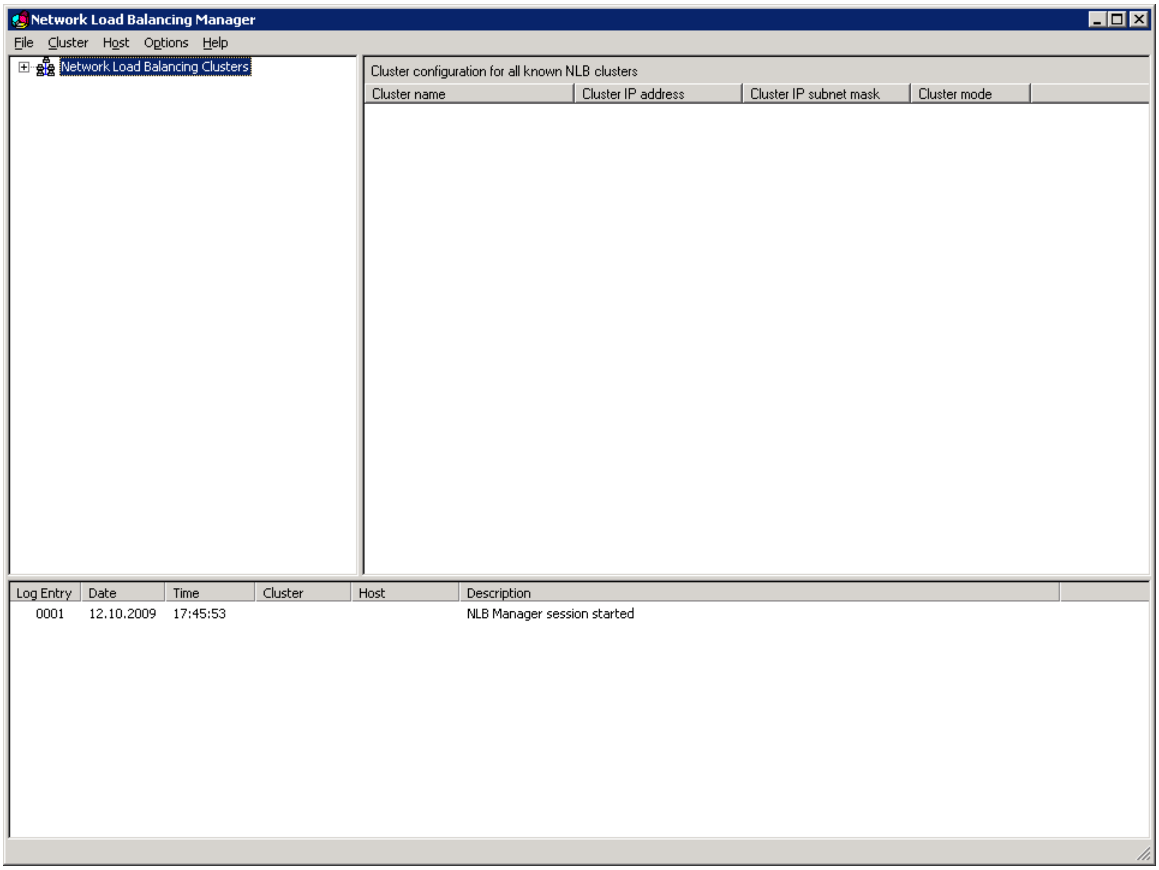
> In case you do not obtain a current view of the cluster after configuring the host parameters, press the control key F5 on your computer. If you see error messages, close the NLB Manager, restart it and connect to the cluster once more.
> If further problems should occur, please consult the relevant documentation for the Microsoft Network Load Balancer.

4.3.2 Network Load Balancer for Windows Server 2008

Some configuration steps may take up to 1 minute or so. In such cases, wait until the step is completed, and do not input anything.

1. On one of the node machines, call **Start** > **Administrative Tools** > **Network Load Balancer Manager**. Thereby, the service is activated on all node machines, which is necessary for cluster operation.

2. A tripartite configuration screen opens. To build a new cluster, go to **Cluster** > **New** in the menu or use the right-hand mouse key to call the context menu and select **New Cluster**.

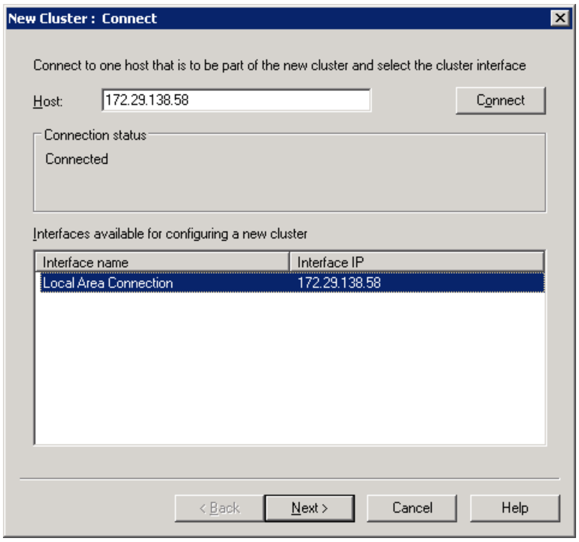

Network Load Balancing Manager
File
Cluster
Host
Options
Help
Network Load Balancing Clusters

Cluster configuration for all known NLB clusters

Cluster name	Cluster IP address	Cluster IP subnet mask	Cluster mode

Log Entry	Date	Time	Cluster	Host	Description
0001	12.10.2009	17:45:53			NLB Manager session started

3. In the **New Cluster: Connect** screen, in the **Host** field, enter the IP address of the first node machine.



New Cluster : Connect

Connect to one host that is to be part of the new cluster and select the cluster interface

Host: 172.29.138.58

Connection status

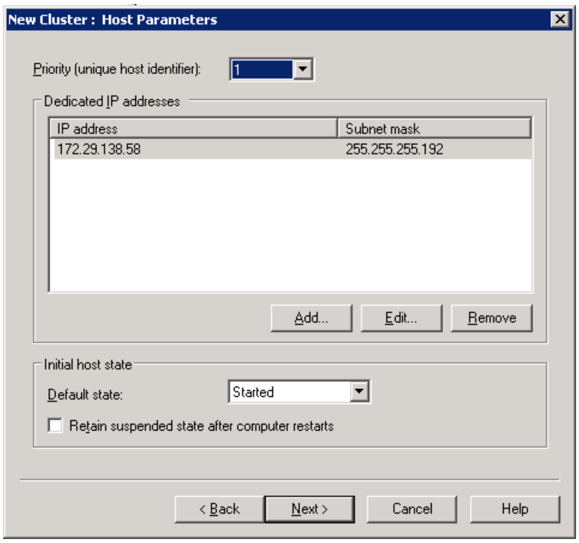
Connected

Interfaces available for configuring a new cluster

Interface name	Interface IP
Local Area Connection	172.29.138.58

Afterwards, click on **Connect**.

4. You are in the **New Cluster: Host Parameters** screen now. In the field **Priority**, a predefined value is displayed, which is a mere numeration and does not imply a prioritization. The IP address field contains the IP address of the network interface.



New Cluster : Host Parameters

Priority (unique host identifier): 1

Dedicated IP addresses

IP address	Subnet mask
172.29.138.58	255.255.255.192

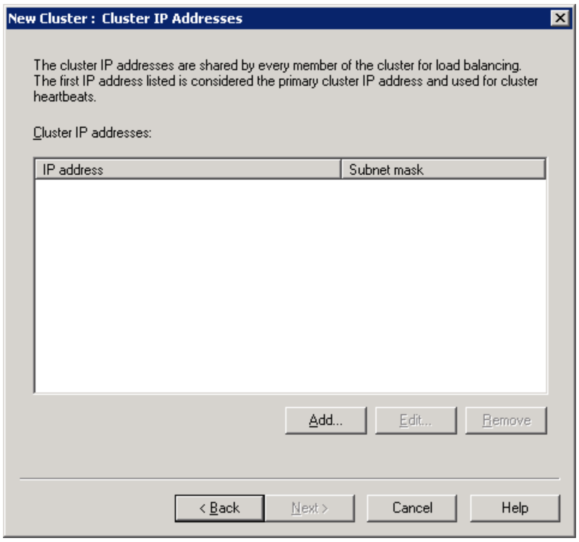
Initial host state

Default state: Started

□ Retain suspended state after computer restarts

When all values are correct, click on **Finish**. The process of adding a node to the cluster may take 1-2 minutes.

5. In the screen **New cluster: Cluster IP Addresses**, the common addresses of the cluster are provided. Click on **Add**.



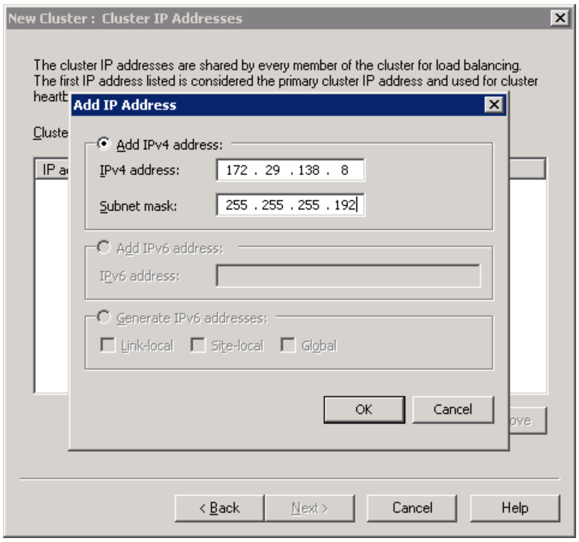
New Cluster : Cluster IP Addresses

The cluster IP addresses are shared by every member of the cluster for load balancing. The first IP address listed is considered the primary cluster IP address and used for cluster heartbeats.

Cluster IP addresses:

IP address	Subnet mask

6. In the dialog window **Add IP Address**, in **IPv4 address**, enter the IP address at which the cluster shall be reachable. In the **Subnet mask** field, enter the corresponding subnet mask.



New Cluster : Cluster IP Addresses

Add IP Address

● Add IPv4 address:

IPv4 address: 172 . 29 . 138 . 8

Subnet mask: 255 . 255 . 255 . 192

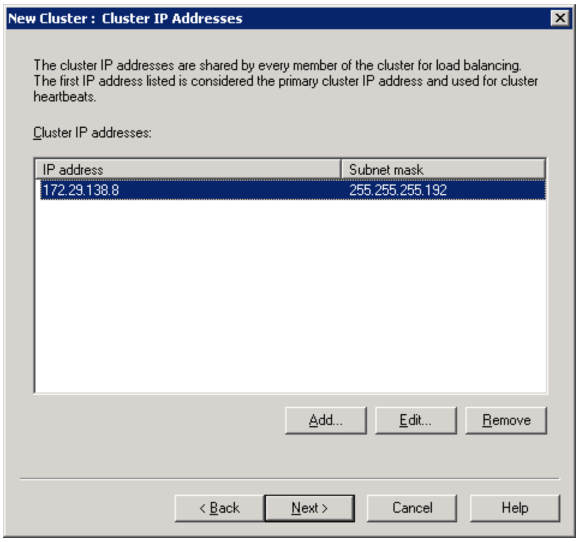
○ Add IPv6 address:

IPv6 address:

○ Generate IPv6 addresses:

□ Link-local □ Site-local □ Global

7. In the screen **New Cluster: Cluster IP Addresses**, the address of the cluster appears now.


New Cluster : Cluster IP Addresses

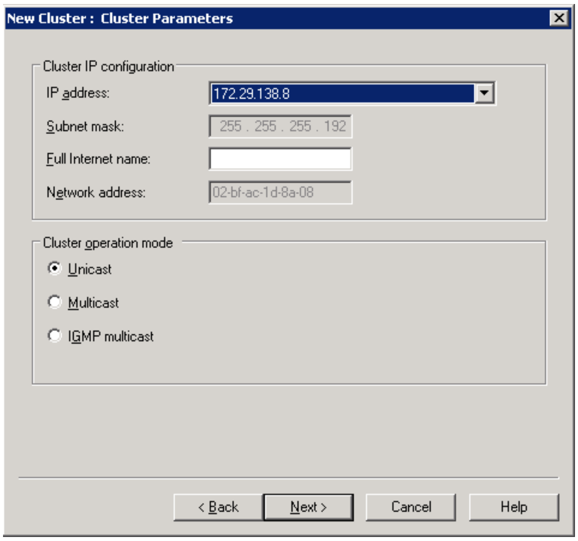
The cluster IP addresses are shared by every member of the cluster for load balancing. The first IP address listed is considered the primary cluster IP address and used for cluster heartbeats.

Cluster IP addresses:

IP address	Subnet mask
172.29.138.8	255.255.255.192

Click on **Next**.

8. You are in the **New Cluster: Cluster Parameters** screen now. If the cluster shall be reachable via DNS name, enter it in **Full Internet name**, e. g. `cluster.domain.com`. In the field **Cluster operation mode**, select **Unicast**. With this setting, all network interfaces in the outer network will be assigned the same MAC address. Thus, inbound data packets are initially received by all node machines and then filtered by the network load balancer.


New Cluster : Cluster Parameters

Cluster IP configuration

IP address: 172.29.138.8

Subnet mask: 255 . 255 . 255 . 192

Full Internet name:

Network address: 02-bf-ac-1d-8a-08

Cluster operation mode

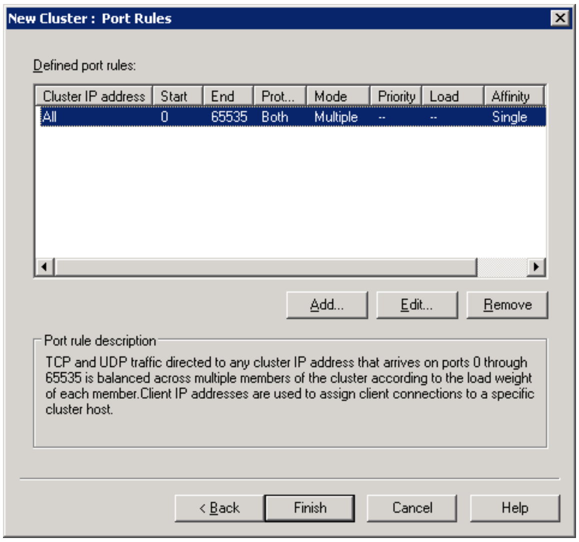
● Unicast

○ Multicast

○ IGMP multicast

Click on **Next**.

9. In the **New Cluster: Port Rules** screen, you set the rules for those ports over which the DLS cluster communicates with the outside world. In case there are some port rules already, remove these with **Remove**.



New Cluster : Port Rules

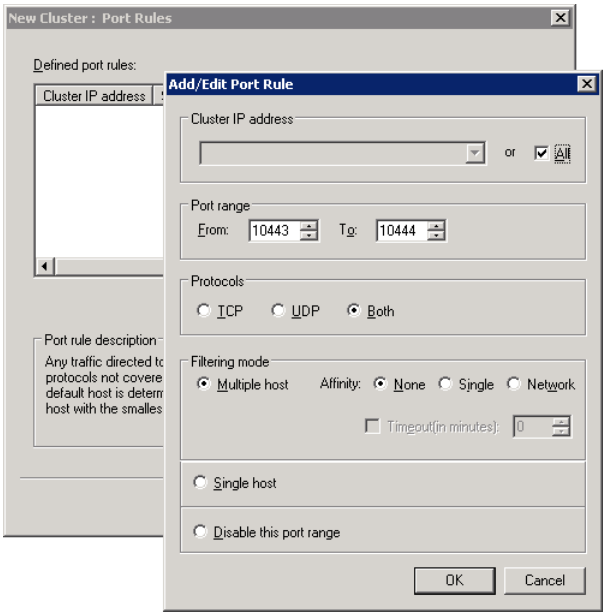
Defined port rules:

Cluster IP address	Start	End	Prot...	Mode	Priority	Load	Affinity
All	0	65535	Both	Multiple	--	--	Single

Port rule description
TCP and UDP traffic directed to any cluster IP address that arrives on ports 0 through 65535 is balanced across multiple members of the cluster according to the load weight of each member.Client IP addresses are used to assign client connections to a specific cluster host.

Click on **Add**.

10. The dialog window **Add/Edit Port Rule** opens. Enter the parameters for the ports resp. port ranges, as appropriate. Under **Cluster IP address**, enter **All** in order to assign the rule to all IP addresses within the cluster. Under **Affinity**, select **None**. With this setting, it is possible that consecutive requests from one and the same IP address are handled by different nodes. Thus it is ensured that the loads are distributed equally. The following screenshot shows the settings for the ports 10443 and 10444. The functions of these ports are described in step 11.



Add/Edit Port Rule

Cluster IP address: or ☑ All

Port range: From: 10443 To: 10444

Protocols: ○ TCP ○ UDP ● Both

Filtering mode: ● Multiple host Affinity: ● None ○ Single ○ Network

□ Timeout(in minutes): 0

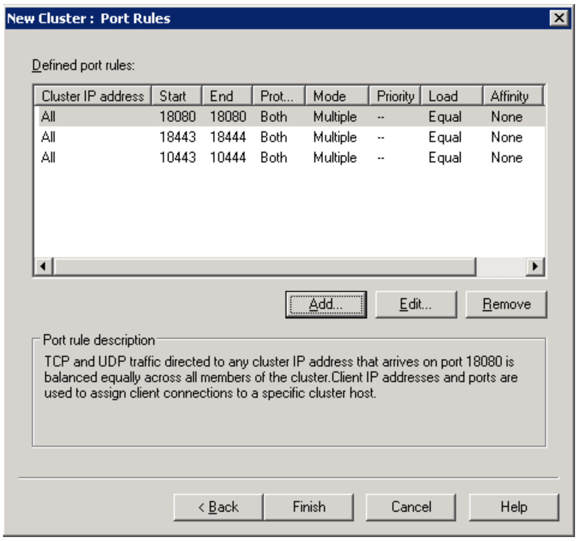
○ Single host

○ Disable this port range

11. Enter the rules for the remaining ports, as described in steps 9 and 10. In the following, the ports elementary for the DLS are listed (in the Release Notes, you can find a list of all DLS ports).

    - 10443: Receives data from the graphical user interface, that is, from the web browser, when HTTPS is used.
    - 10444: Receives data over HTTPS from the DlsAPI, which is the web service interface of the DLS.
    - 18080: Receives data from the graphical user interface, that is, from the web browser, when HTTP is used.
    - 18443: Receives data from the end devices (HTTP and HTTPS).
    - 18444: Receives data from the end devices when a secure connection between DLS and end device is established (secure mode).

12. When you have entered all port rules, click on **Finish**.



New Cluster : Port Rules

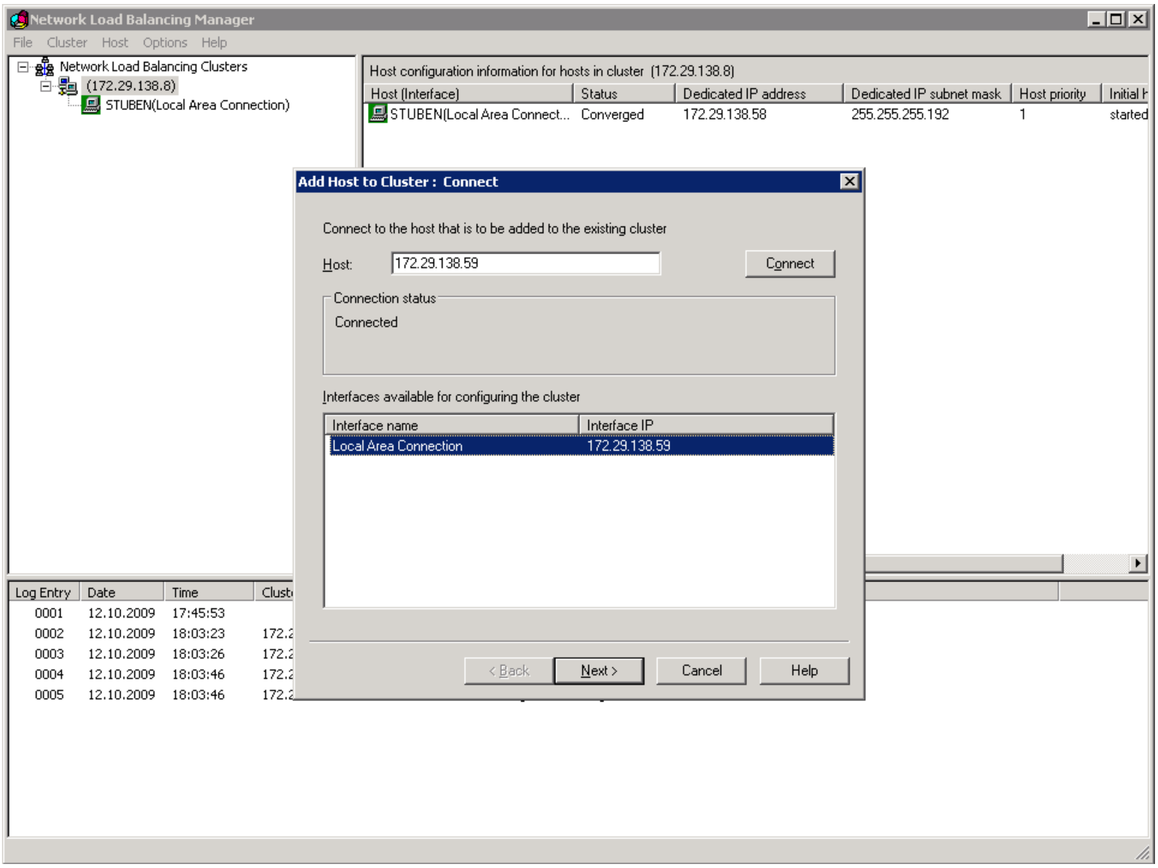
Defined port rules:

Cluster IP address	Start	End	Prot...	Mode	Priority	Load	Affinity
All	18080	18080	Both	Multiple	--	Equal	None
All	18443	18444	Both	Multiple	--	Equal	None
All	10443	10444	Both	Multiple	--	Equal	None

Port rule description

TCP and UDP traffic directed to any cluster IP address that arrives on port 18080 is balanced equally across all members of the cluster.Client IP addresses and ports are used to assign client connections to a specific cluster host.

13. You get to the main screen of the Network Load Balancing Manager again, where the cluster in its current composition is displayed. When the addition of the node machine has been successful, the **Status** is set to **Converged**. In the **Cluster** menu, go to **Add Host** or use the right-hand mouse key to call the context menu and then go to **Add Host to Cluster** in order to add another node machine.


Network Load Balancing Manager
File Cluster Host Options Help
Network Load Balancing Clusters
(172.29.138.8)
STUBEN(Local Area Connection)
Add Host to Cluster : Connect
Connect
< Back
Next >
Cancel
Help

Host configuration information for hosts in cluster (172.29.138.8)

Host (Interface)	Status	Dedicated IP address	Dedicated IP subnet mask	Host priority	Initial h
STUBEN(Local Area Connect...	Converged	172.29.138.58	255.255.255.192	1	started

Connect to the host that is to be added to the existing cluster

Host: 172.29.138.59

Connection status
Connected

Interfaces available for configuring the cluster

Interface name	Interface IP
Local Area Connection	172.29.138.59

Log Entry	Date	Time	Clust
0001	12.10.2009	17:45:53	
0002	12.10.2009	18:03:23	172.2
0003	12.10.2009	18:03:26	172.2
0004	12.10.2009	18:03:46	172.2
0005	12.10.2009	18:03:46	172.2

14. For the next as well as for all further node machines, if applicable, proceed in the same way as for the first node machine.

4.3.3 Network Configuration when using Windows NLB

For general configuration please check:
http://www.microsoftnow.com/2007/09/frequently-asked-questions-on-windows.html

This section describes those topics which require special consideration:

4.3.3.1 How to Configure Layer 2 Switches to Work with Windows NLB?

Make sure that the switch does not associate the cluster MAC address with a particular switch port.

4.3.3.2 How to Configure Layer 3 Switches to Work with Windows NLB?

Layer 3 switches need to be configured specially to work with NLB. For the hosts in the cluster, a VLAN must be established; this VLAN must operate in layer 2 mode.

4.3.3.3 How Should IP Packet Fragmentation Be Tackled?

NLB has problems in dealing with fragmented IP packets; thus, fragmentation must be avoided.

Especially in cases where part of the connections between phones and DLS is transmitted through VPN channels, fragmentation may appear easily. This can be avoided by creating room for additional bytes in the VPN channel. For this purpose. the TCP parameter "MSS" (Maximum Segment Size; maximum TCP payload) must be set to a value below the TCP maximum of 1460. Using Cisco® Equipment you should activate the "MSS adjust" feature. Example: **ip tcp adjust-mss 1300**

4.4 Set Up DCMP

To set up the DCMP (DLS Contact-Me Proxy), proceed with the following steps:

- Install DCMP
- Configure DCMP
- Configure DLS for DCMP
- Configure Phone for DCMP
- Test DCMP

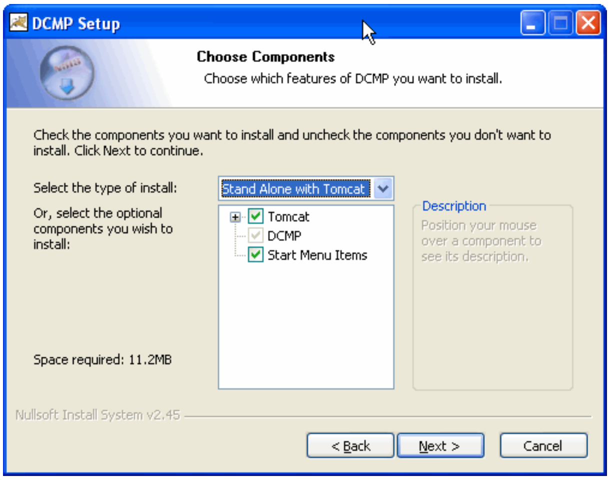
4.4.1 Install DCMP

First, ensure that the DCMP is not installed already. For this purpose, navigate to **http://<IP Address>:18080/dcmp** with a web browser. If you receive an error message, you must install the DCMP. The DCMP can be installed on the DLS machine as well as on a different machine.

In the installation medium, navigate to the directory **dcmp** and start the **dcmp-installer** with a double click.

4.4.1.1 Installation on the DLS Machine

If you wish to install both DCMP and DLS on the same machine, choose the option **DCMP**.



Choose Components

Choose which features of DCMP you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Stand Alone with Tomcat

Or, select the optional components you wish to install:

☑ Tomcat
☑ DCMP
☑ Start Menu Items

Description

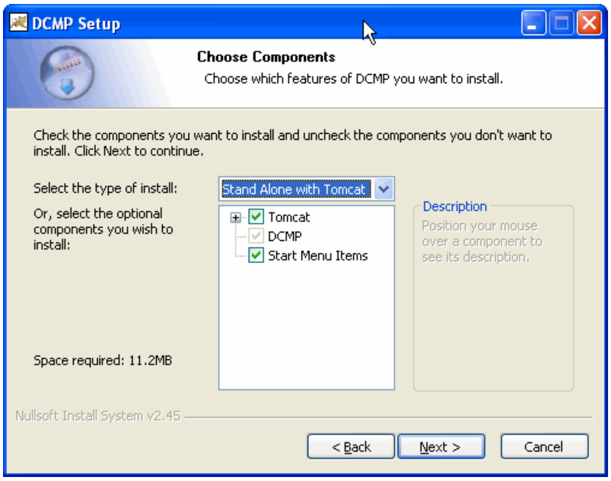
Position your mouse over a component to see its description.

Space required: 11.2MB

Follow the installation instructions.

4.4.1.2 Installation on a Different Machine

For installation on a different machine, select the option **DCMP** and **Service Startup**.



DCMP Setup

Choose Components

Choose which features of DCMP you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Stand Alone with Tomcat

Or, select the optional components you wish to install:

- ☑ Tomcat
- ☑ DCMP
- ☑ Start Menu Items

Description

Position your mouse over a component to see its description.

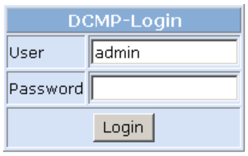
Space required: 11.2MB

Nullsoft Install System v2.45

During the installation, you will be asked for the password for the DCMP.

4.4.2 Configure DCMP

1. With a web browser, navigate to **http://<IP Address>:18080/dcmp** to login at the DCMP server. The user name is **admin**. The password is identical with the admin password for the DLS if the DCMP has been installed along with the DLS. If the DCMP has been installed subsequently, the default password is **Siemens2004**. This should be changed after installation. If the DCMP has been installed on a dedicated server, enter the password you had defined during installation.



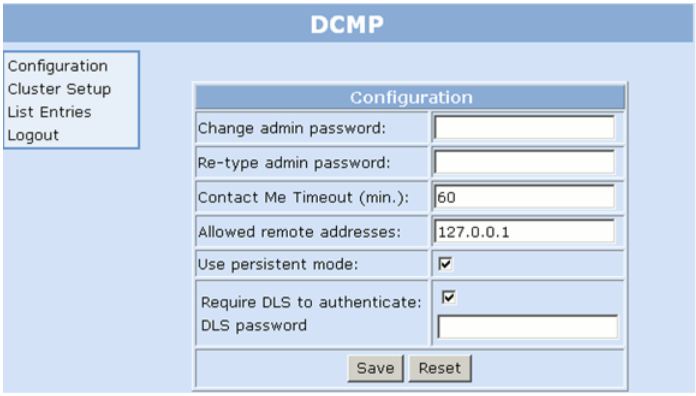
DCMP-Login

User	admin
Password	

2. After login, the initial configuration screen opens up. If desired, you can change the password with **Change admin password** and **Re-type admin password**.

   In the **Allowed remote addresses** field, you enter the addresses of the DLS servers as a comma-separated list, or as a single address, if there is only one DLS server. If the DCMP is installed on the DLS machine, the value is 127.0.0.1.

   If **Require DLS to authenticate** is checked, the DLS must authenticate to communicate with the DCMP. For this option, a **DLS password** must be entered; the DLS must present this password to authenticate with the DCMP.

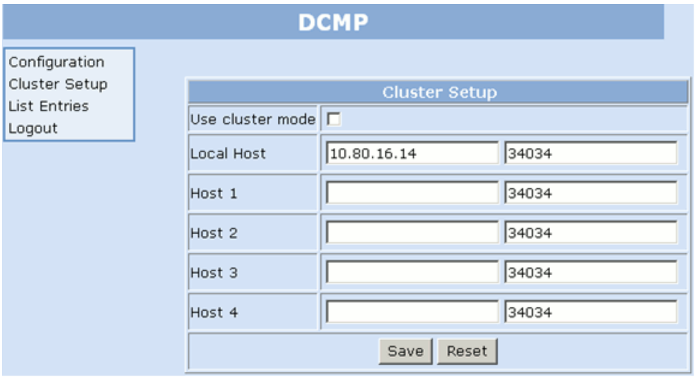


Configuration	
Change admin password:	
Re-type admin password:	
Contact Me Timeout (min.):	60
Allowed remote addresses:	127.0.0.1
Use persistent mode:	☑
Require DLS to authenticate:	☑
DLS password	

3. In the **Cluster Setup** screen, you can check or configure the appropriate addresses and ports for one or more DLS machines. If a DLS cluster is to be used, check **Use cluster mode**.

   The **Local Host** field contains the IP address of the DCMP server.

   When operating the DLS as a cluster, the IP addresses of each machine in the cluster must be entered in **Host 1 ... 4**.



Cluster Setup		
Use cluster mode	☐	
Local Host	10.80.16.14	34034
Host 1		34034
Host 2		34034
Host 3		34034
Host 4		34034

In the **List Entries** screen, you can view all Contact-Me messages from the DLS.

4.4.3 Configure DLS for DCMP

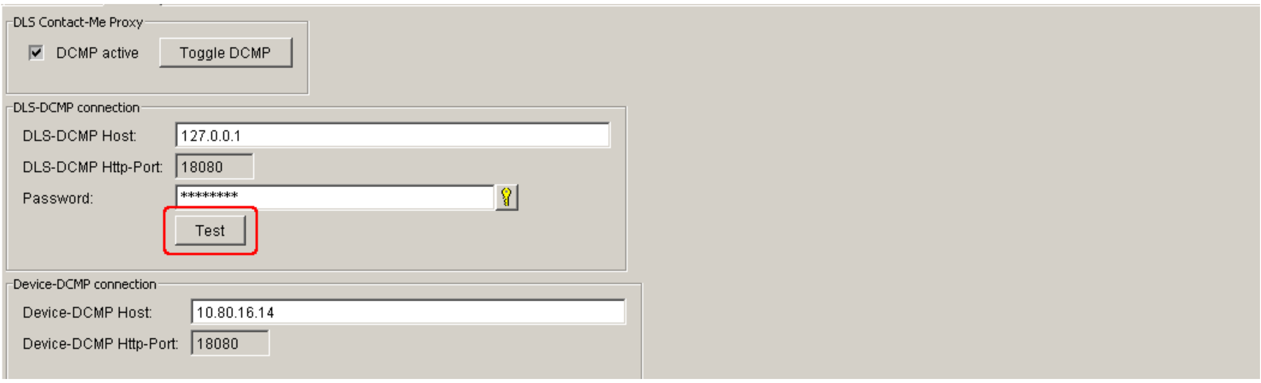
When the DCMP server is ready, the DLS can be configured for DCMP operation.

1. In **Administration** > **Workpoint Interface Configuration** > **"DCMP" Tab**, click the **Toggle DCMP** button to activate the DCMP.

2. If the DCMP is located on the DLS machine, the IP address of the DCMP server will be shown in **DLS-DCMP Host**; otherwise, it must be entered here.

3. If you have activated the **Require DLS to authenticate** option in the DCMP configuration (see Section 4.4.2, "Configure DCMP"), you must enter the **DLS password** previously defined in the DCMP configuration in the **Password** field.

4. To test communications between DLS and DCMP, click on the **Test** button.



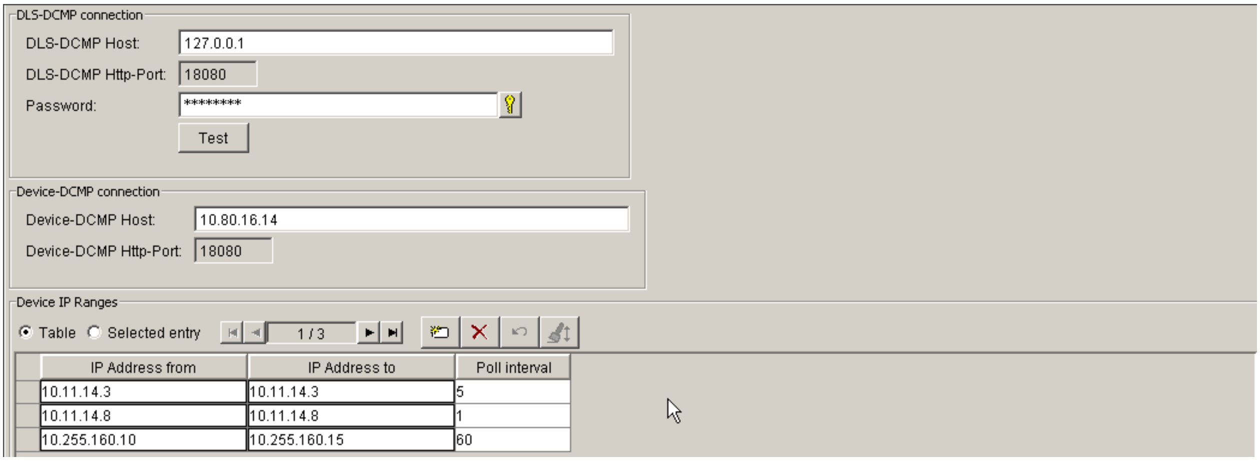
DLS Contact-Me Proxy
☑ DCMP active

DLS-DCMP connection
DLS-DCMP Host: 127.0.0.1
DLS-DCMP Http-Port: 18080
Password: ********

Device-DCMP connection
Device-DCMP Host: 10.80.16.14
Device-DCMP Http-Port: 18080

For testing purposes, a very short **Poll interval** can be chosen; however, in a live environment, longer intervals are recommended.

5. Define one or more **Device IP Ranges**. Any IP Devices within the IP ranges defined by **IP address from** and **IP address to** will be updated via DCMP. Hence, whenever a change is made to an IP device within an IP range listed here, the DLS will send a message to the DCMP to set the Contact-Me entry for that phone.



DLS-DCMP connection
DLS-DCMP Host: 127.0.0.1
DLS-DCMP Http-Port: 18080
Password: ********

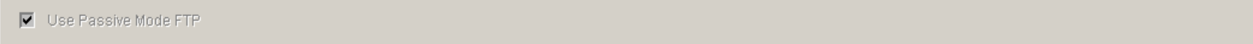
Device-DCMP connection
Device-DCMP Host: 10.80.16.14
Device-DCMP Http-Port: 18080

Device IP Ranges
● Table ○ Selected entry 1 / 3

IP Address from	IP Address to	Poll interval
10.11.14.3	10.11.14.3	5
10.11.14.8	10.11.14.8	1
10.255.160.10	10.255.160.15	60

4.4.4 Configure Phone for DCMP

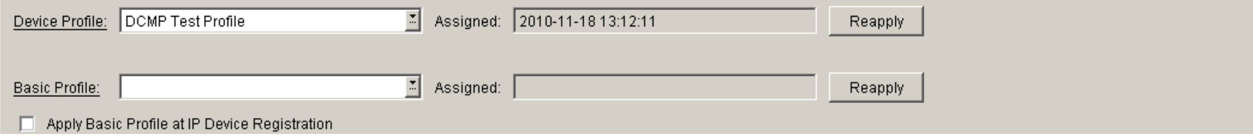
1. The phone should be configured to use passive FTP transfers so it can download software and other data even if it is behind a firewall doing NAT. This is done in **IP Devices** > **IP Phone Configuration** > **Miscellaneous** > **"FTP Server" Tab**. As this flag cannot be changed in an already deployed device, it is recommended to create a "DCMP Miscellaneous" template with this flag set and use that template in the profile for DCMP users.



☑ Use Passive Mode FTP

2. Navigate to **Profile Management** > **Device Profile** and create a device profile using the newly created "DCMP Miscellaneous" template.

3. Navigate to **IP Devices** > **IP Device Management** > **IP Device Configuration**. Use the **Search** function, the "Table" view, and the "Object" view to select the subscriber number for the phone to be configured. In the **"Profile" Tab**, select the profile you just created, and assign it to the phone.



Device Profile: DCMP Test Profile Assigned: 2010-11-18 13:12:11

Basic Profile: Assigned:

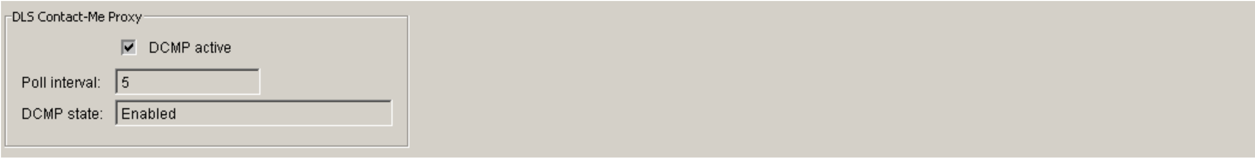
□ Apply Basic Profile at IP Device Registration

4.4.5 Test DCMP

1. First, choose a phone that has an IP address within an IP range configured for DCMP operation (see Section 4.4.3, "Configure DLS for DCMP") and perform a factory default on that phone.

2. When the phone has rebooted, give it the subscriber number you just assigned the DCMP Profile to.

3. Navigate to **IP Devices** > **IP Device Management** > **IP Device Configuration** > **"DCMP" Tab**. The **DCMP active** switch should be checked, and the settings should be as set for this IP address in **Administration** > **Workpoint Interface Configuration** > **"DCMP" Tab**.



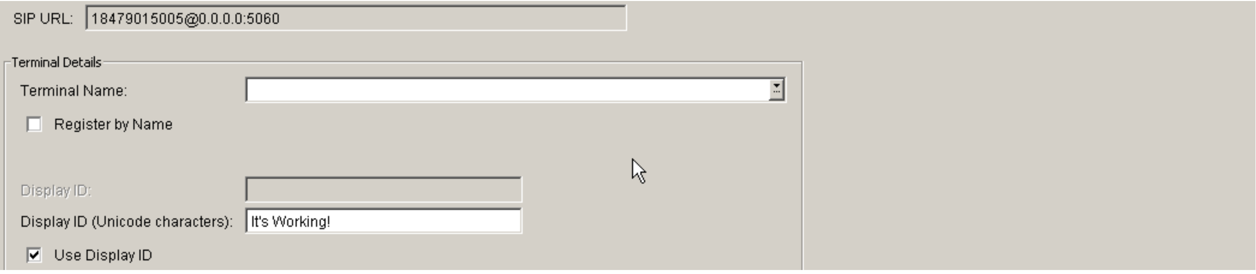
DLS Contact-Me Proxy

☑ DCMP active

Poll interval: 5

DCMP state: Enabled

4. As a test case for a configuration change, modify the display name on the phone. Navigate to **IP Devices** > **IP Phone Configuration** > **Gateway/Server** > **"SIP Terminal Settings" Tab**. Activate **Use Display ID** (or **Use Display ID (Unicode characters)**) and set the **Display ID** to "It’s Working!", for instance. Save the change in DLS.



SIP URL: 18479015005@0.0.0.0:5060

Terminal Details

Terminal Name:

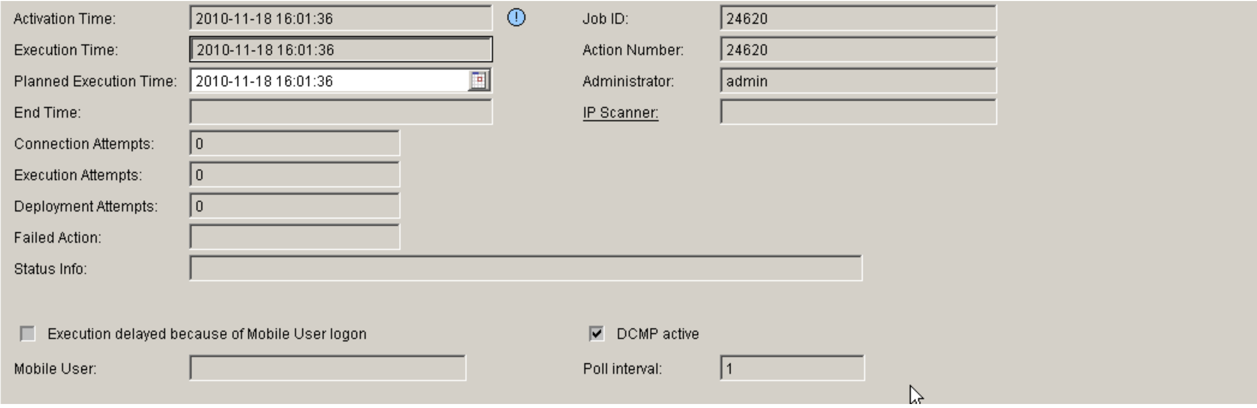
□ Register by Name

Display ID:

Display ID (Unicode characters): It's Working!

☑ Use Display ID

5. To verify that the job is running, look in **Job Coordination** > **Job Control** and click on the **Search** button. Then click on the specific entry and select the "Object" view. In the **"Basic Data" Tab** you can see that the job will be handled via DCMP.



Activation Time:	2010-11-18 16:01:36	Job ID:	24620
Execution Time:	2010-11-18 16:01:36	Action Number:	24620
Planned Execution Time:	2010-11-18 16:01:36	Administrator:	admin
End Time:		IP Scanner:	
Connection Attempts:	0		
Execution Attempts:	0		
Deployment Attempts:	0		
Failed Action:			
Status Info:			

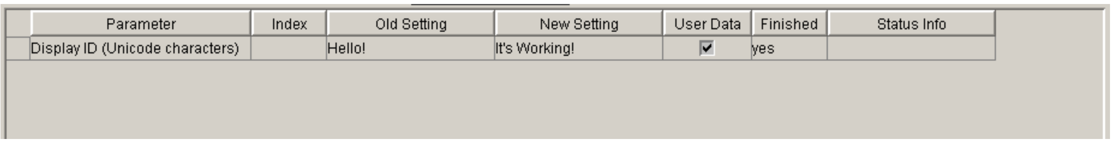
□ Execution delayed because of Mobile User logon

☑ DCMP active

Mobile User:

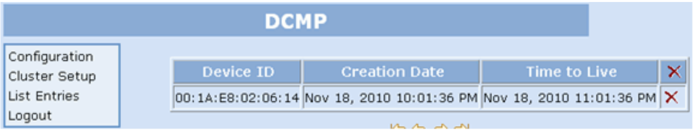
Poll interval: 1

6. In the **"Configuration Data" Tab** you can see the specific change that was requested.



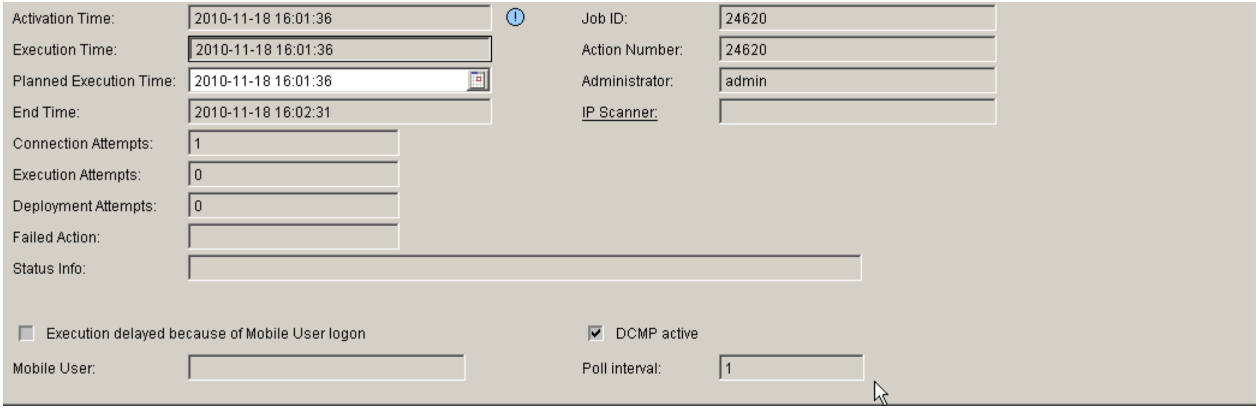
Parameter	Index	Old Setting	New Setting	User Data	Finished	Status Info
Display ID (Unicode characters)		Hello!	It's Working!	☑	yes	

7. In the DCMP GUI, click on the **List Entries** menu. You should see the Contact Me setting in the list. The **Device ID** should be the MAC address of the phone.



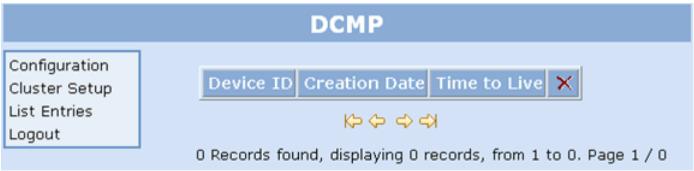
Device ID	Creation Date	Time to Live	✕
00:1A:E8:02:06:14	Nov 18, 2010 10:01:36 PM	Nov 18, 2010 11:01:36 PM	✕

8. In the DLS GUI, in **Job Coordination** > **Job Control** > **"Basic Data" Tab**, you will see an "End Time" once the change is made.



Activation Time:	2010-11-18 16:01:36	Job ID:	24620
Execution Time:	2010-11-18 16:01:36	Action Number:	24620
Planned Execution Time:	2010-11-18 16:01:36	Administrator:	admin
End Time:	2010-11-18 16:02:31	IP Scanner:	
Connection Attempts:	1		
Execution Attempts:	0		
Deployment Attempts:	0		
Failed Action:			
Status Info:			
☐ Execution delayed because of Mobile User logon		☑ DCMP active	
Mobile User:		Poll interval:	1

9. In the DCMP GUI, you will see the Contact Me entry is removed.



Device ID	Creation Date	Time to Live	✕

0 Records found, displaying 0 records, from 1 to 0. Page 1 / 0

The test is finished.

4.5 Installing the DLS

4.5.1 Single Node Operation With Local Database

This is the standard DLS installation. At this, follow the instructions of the installation assistant. On installing DLS V3.0, DB MS SQL2008 is used as default database. For this, the following requirements are necessary:

- MS.Net 3.51
- MSI 4.5

Both programs are available on the DLS installation media. In the subsequent sections, the installation for Windows XP is described as an example.

4.5.1.1 Install MS .Net 3.51

1. In the installation medium, change into the directory `../MS.Net3.51`
2. Start `donetfx35.exe`. Follow the instructions of the assistant and afterwards, execute a restart.
3. Change into the `../MS.Net3.51/MS.Net351_Hotfix` directory and then, depending on the operating system of your PC, into `/XP_2003` or `/Vista_2008`. In the following, the installation for Windows XP is described as an example.
4. Read the instructions in `instructions-x86.txt`
5. Call the updates in the order described underneath, and follow the instructions of the respective assistent.
   Update für .NET Framework 2.0 Service Pack 2: `NDP20SP2-KB958481-x86.exe`
   Update für .NET Framework 3.0 Service Pack 2: `NDP30SP2-KB958483-x86.exe`
   Update für .NET Framework 3.5 Service Pack 1: `NDP35SP1-KB958484-x86.exe`

4.5.1.2 Install MSI4.5

1. Change into the directory `../MSI4.5`
2. Read the instructions in `instructions.txt`
3. Depending on the operating system of your PC, start the update program. In the following, the installation for Windows XP is started as an example:
   Start `WindowsXP-KB942288-v3-x86.exe`

4.5.1.3 Install DLS

Follow the instructions of the OpenScape Deployment Service Setup Wizard contained in the DLS software package.

4.5.2 Single Node Operation With Remote Or Customer Specific Database

Before installing the DLS with a customer specific or external database, Microsoft SQL Server 2005 Enterprise Edition must be installed (see Section 4.2, "Install MS SQL Server for Remote Database") and in operation.

Please proceed as follows:

1. If DLS server and database server reside on different PCs, and a local user account is used on the database server, an identical user account must be created on the DLS server. On the DLS machine, add the account used for the database to the local administrator group.
2. Log on at the DLS server with the account used for the database and start the setup program. Alternatively, you can use the command `runas/user:<used account> <path to setup.exe>` to start the installation.
3. In the **Installation Configuration** screen, in the field **Database Installation Type**, select the option **Use custom or remote Database**.
4. Follow the installation instructions. In the screen **Database Settings**, under **MSSQL specific entries**, enter the database directory you have created for the DLS data before the database installation, e. g. `D:\DATA\DLSDB`. Please notice that the directory path is relative to the database server. In the field **DB Instance**, enter "DLS". Click on **Next**.
5. Under **User Account for Access to SQL Server**, enter the name of the user account previously mentioned, e. g.
   `<local account> ("dlsservice")` or
   `<domain name>\<sql account> ("mydomain\dlsservice")` or
   `<sql account>@<domain url> ("dlsservice@mydomain.com")`, as well as the appropriate password.
6. Finish the installation. You can control the result under **Start** > **Settings** > **Control Panel** > **Adminstration** > **Services: DeploymentService**.

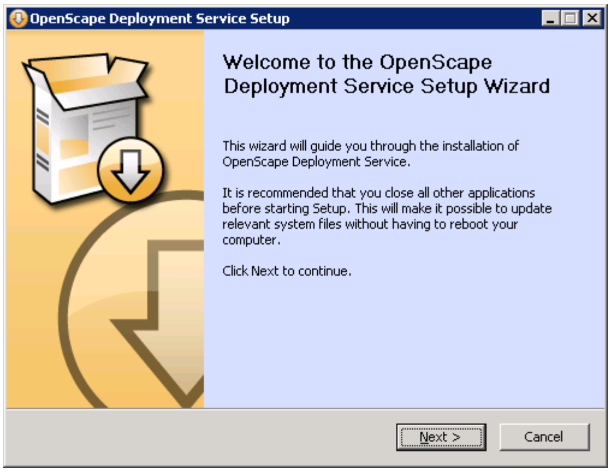
4.5.3 Multi Node Operation

The following example demonstrates the installation of two DLS nodes with mirrored SQL database.

> The first installation as well as the update installation must not be carried out on more than one nodes at a time, as the nodes access common files. Therefore, install the nodes one after another.

4.5.3.1 First Node

1. Start the setup program. After selecting the language, you see a welcome screen.



Welcome to the OpenScape Deployment Service Setup Wizard

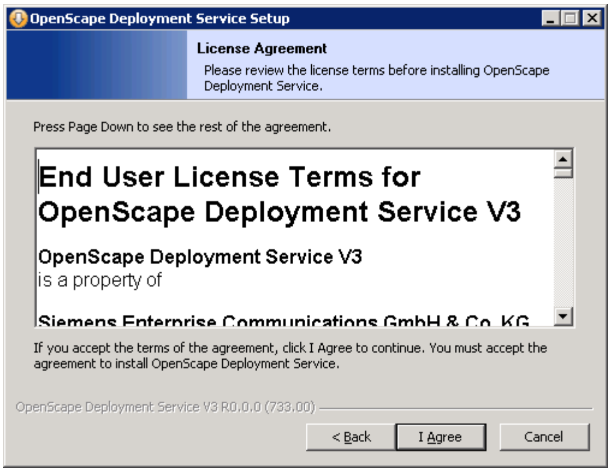
This wizard will guide you through the installation of OpenScape Deployment Service.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Click on **Next**.

2. Click on **I Agree** to accept the license agreement.



License Agreement

Please review the license terms before installing OpenScape Deployment Service.

Press Page Down to see the rest of the agreement.

End User License Terms for OpenScape Deployment Service V3

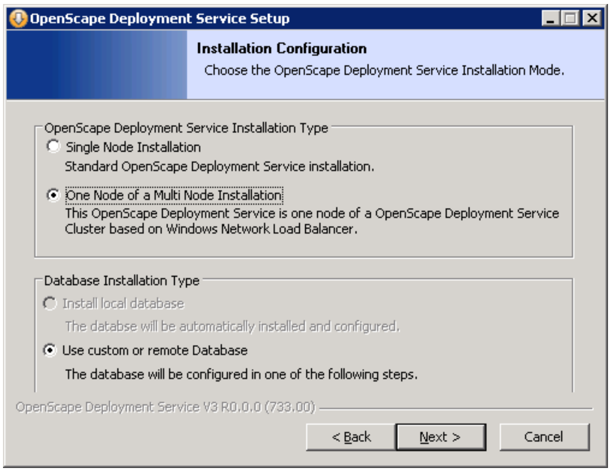
OpenScape Deployment Service V3
is a property of

Siemens Enterprise Communications GmbH & Co. KG

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenScape Deployment Service.

OpenScape Deployment Service V3 R0.0.0 (733.00)

3. In the **Installation Configuration** screen, under **DLS Installation Type**, select the option **One Node of a Multinode Installation**.



OpenScape Deployment Service Setup

Installation Configuration

Choose the OpenScape Deployment Service Installation Mode.

OpenScape Deployment Service Installation Type

○ Single Node Installation
Standard OpenScape Deployment Service installation.

● One Node of a Multi Node Installation
This OpenScape Deployment Service is one node of a OpenScape Deployment Service Cluster based on Windows Network Load Balancer.

Database Installation Type

○ Install local database
The databse will be automatically installed and configured.

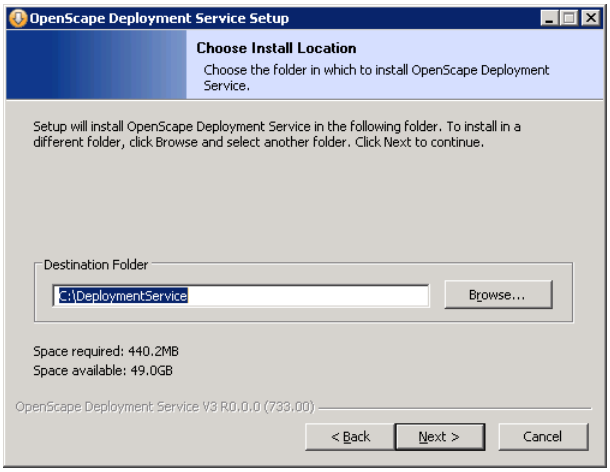
● Use custom or remote Database
The database will be configured in one of the following steps.

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

4. In the **Choose Install Location** screen, choose the target directory in which the DLS shall be installed.

> The directory path must not contain blanks, as in "Program Files", for instance.



OpenScape Deployment Service Setup

Choose Install Location

Choose the folder in which to install OpenScape Deployment Service.

Setup will install OpenScape Deployment Service in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\DeploymentService

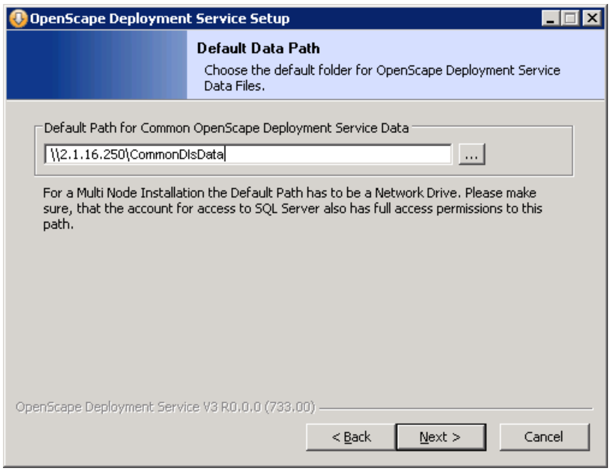
Space required: 440.2MB
Space available: 49.0GB

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

5. In the screen, enter the path of a directory, to which all nodes must have access. Here, configuration data common to all DLS nodes are stored. This directory must exist, and writing access for this directory must be granted to the DLS, also for installation purposes.

> In case a notification window appears here, asking whether another node shall be installed, in addition to existing ones, click on "No". The notification window will appear if the file `common_dls.properties` exists in the specified directory.


OpenScape Deployment Service Setup

Default Data Path

Choose the default folder for OpenScape Deployment Service Data Files.

Default Path for Common OpenScape Deployment Service Data: \\2.1.16.250\CommonDlsData

For a Multi Node Installation the Default Path has to be a Network Drive. Please make sure, that the account for access to SQL Server also has full access permissions to this path.

OpenScape Deployment Service V3 R0.0.0 (733.00)
< Back
Next >
Cancel

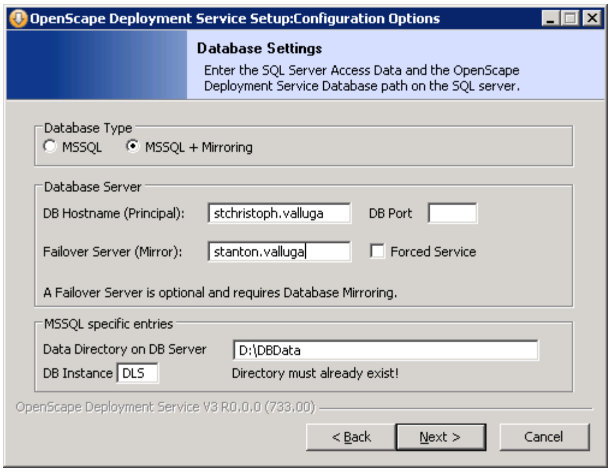
Click on **Next**.

6. In the **Database Settings** screen provide the necessary specifications for the database. If you wish to deploy a mirrored database for maximum reliability, select the option **MSSQL + Mirroring** under **Database Type**. Under **Database Server**, in the field **DB Hostname (Principal)**, specify the "Principal" database server, and in the field **Failover Server (Mirror)**, specify the backup database server, which will fill in in case the Principal fails.

   Under **MSSQL specific entries**, in the field **Data Directory on Server**, enter the directory on the database server in which the DLS database is located. This directory must exist already. It should have been created before theSQL server installation (see Section 4.2, "Install MS SQL Server for Remote Database", step 2).

   > It is recommended to use the same directory path both on the Mirror and on the Principal.

   Under **DB Instance**, enter the instance under which the DLS database is to operate (see Section 4.2, "Install MS SQL Server for Remote Database", step 4 resp. Section 4.2.2, "Microsoft SQL Server 2008", step 9).

   OpenScape Deployment Service Setup:Configuration Options

   Database Settings

   Enter the SQL Server Access Data and the OpenScape Deployment Service Database path on the SQL server.

   Database Type

   ○ MSSQL ● MSSQL + Mirroring

   Database Server

   DB Hostname (Principal): stchristoph.valluga DB Port

   Failover Server (Mirror): stanton.valluga □ Forced Service

   A Failover Server is optional and requires Database Mirroring.

   MSSQL specific entries

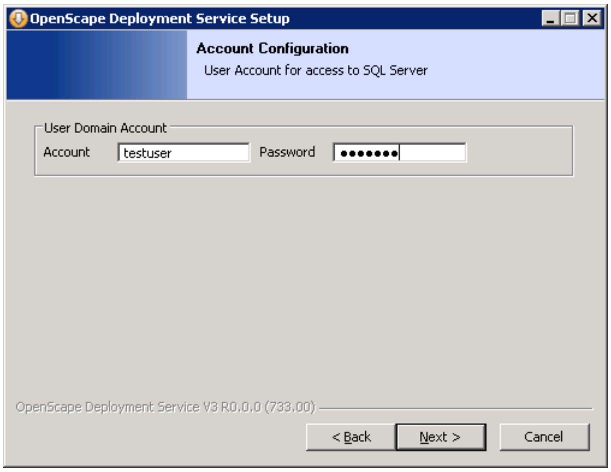
   Data Directory on DB Server: D:\DBData

   DB Instance: DLS Directory must already exist!

   OpenScape Deployment Service V3 R0.0.0 (733.00)

   Click on **Next**.

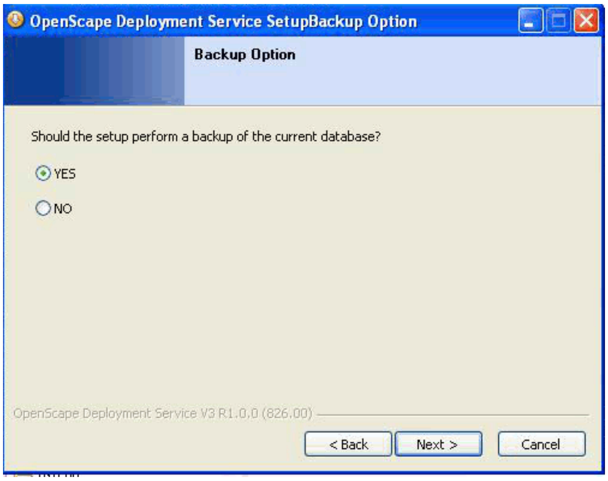
7. In the **Account Configuration** screen, in the fields **Account** and **Password**, enter the access data of the user the DLS shall run under. The user must be a member of the administrator group, and it must exist already.


OpenScape Deployment Service Setup
Account Configuration
User Account for access to SQL Server
User Domain Account
OpenScape Deployment Service V3 R0.0.0 (733.00)
< Back
Next >
Cancel

Account: testuser
Password: •••••••

Click on **Next**.

8. In the **Backup Option** screen, select "Yes" if you wish to save your database while setup/ upgrade.

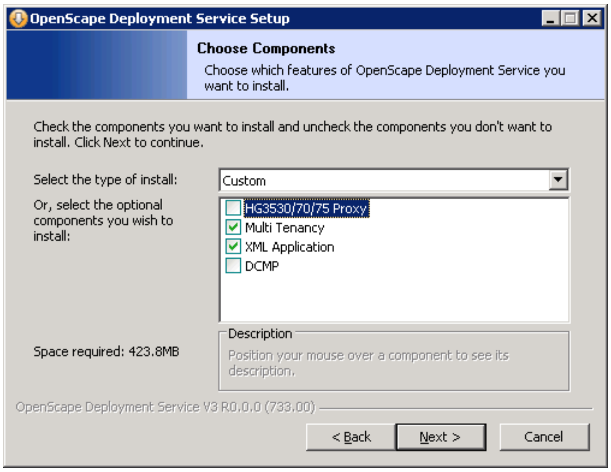

OpenScape Deployment Service SetupBackup Option
Backup Option
OpenScape Deployment Service V3 R1.0.0 (826.00)
< Back
Next >
Cancel

Should the setup perform a backup of the current database?

● YES

○ NO

9. Now, in the **Choose Components** screen, select the desired DLS components.



Choose Components

Choose which features of OpenScape Deployment Service you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Custom

Or, select the optional components you wish to install:

- □ HG3530/70/75 Proxy
- ☑ Multi Tenancy
- ☑ XML Application
- □ DCMP

Space required: 423.8MB

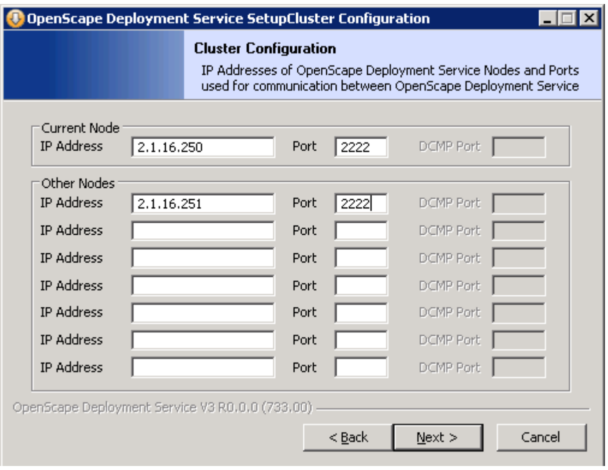
Description

Position your mouse over a component to see its description.

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

10. In the **Cluster Configuration** screen, under **Current Node**, you see the node machine on which you are currently installing the DLS. Under **Other Nodes**, in the **IP address** fields, enter the IP addresses of the corresponding node machines, and in the **Port** fields, enter the port used by the DLS running on the corresponding machine for communication with the other nodes. If you have selected the DCMP in step 8, you must specify the port on which the DLS receives data from the DCMP in the field **DCMP-Port**.



OpenScape Deployment Service SetupCluster Configuration

Cluster Configuration
IP Addresses of OpenScape Deployment Service Nodes and Ports used for communication between OpenScape Deployment Service

Current Node

IP Address	2.1.16.250	Port	2222	DCMP Port	

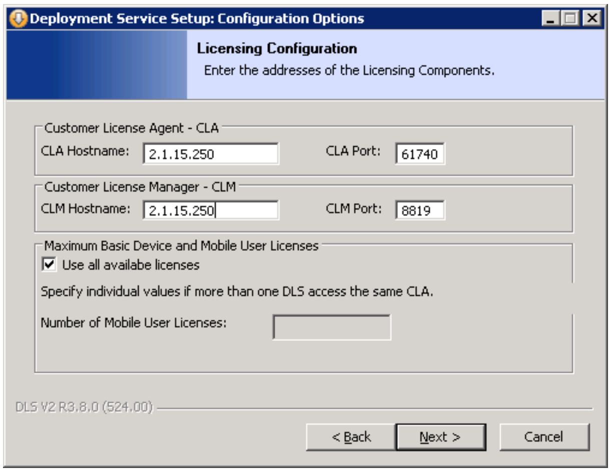
Other Nodes

IP Address	2.1.16.251	Port	2222	DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

11. In the **Licensing Configuration** field, you provide the specifications required for licensing. Under **Customer License Agent - CLA**, in the field **CLA Hostname**, you enter the IP address of the CLA server, and in the field **CLA Port**, you enter the corresponding port. Under **Customer License Manager - CLM**, in the field **CLM Hostname**, enter the IP address of the CLM server, and in the field **CLM Port**, you enter the corresponding port. Under **Maximum Device and Mobile User Licenses**, the appropriate option might well be **Use all available licenses**. If you wish to divide the licenses under diverse DLS instances, enter the number of Mobile User licenses needed for this installation in the field **Number of Mobile User Licenses**.



Deployment Service Setup: Configuration Options

Licensing Configuration
Enter the addresses of the Licensing Components.

Customer License Agent - CLA
CLA Hostname: 2.1.15.250 CLA Port: 61740

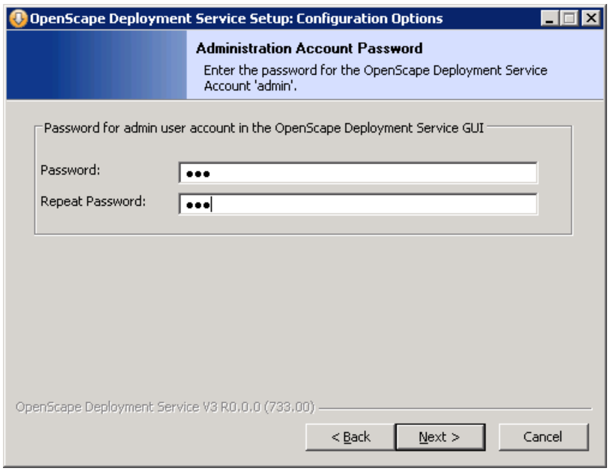
Customer License Manager - CLM
CLM Hostname: 2.1.15.250 CLM Port: 8819

Maximum Basic Device and Mobile User Licenses
☑ Use all availabe licenses
Specify individual values if more than one DLS access the same CLA.
Number of Mobile User Licenses:

DLS V2 R3.8.0 (524.00)

Click on **Next**.

12. In the **Administration Account Password** screen, in the fields **Password**/**Repeat Password**, enter the password for the DLS user "admin".



OpenScape Deployment Service Setup: Configuration Options

Administration Account Password

Enter the password for the OpenScape Deployment Service Account 'admin'.

Password for admin user account in the OpenScape Deployment Service GUI

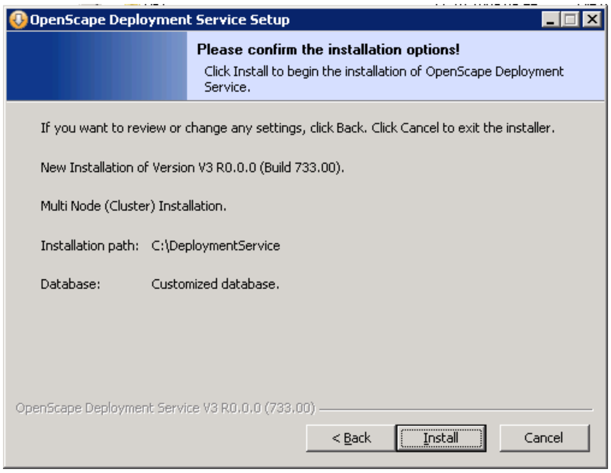
Password: •••

Repeat Password: •••

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

13. In the next screen, you see a brief overview on the installation settings. To start the installation, click on **Install**; to revise settings, click on **Back**.



OpenScape Deployment Service Setup

Please confirm the installation options!

Click Install to begin the installation of OpenScape Deployment Service.

If you want to review or change any settings, click Back. Click Cancel to exit the installer.

New Installation of Version V3 R0.0.0 (Build 733.00).

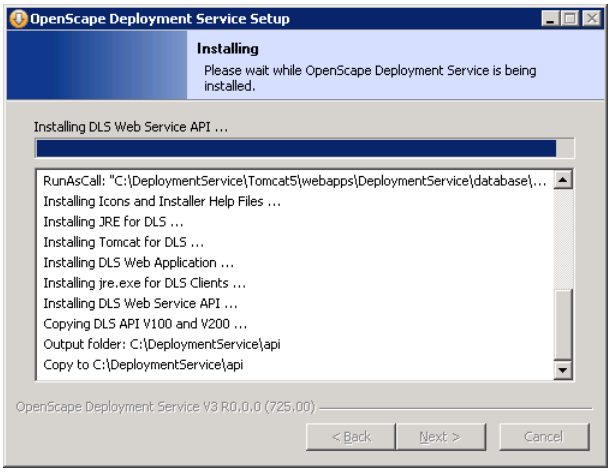
Multi Node (Cluster) Installation.

Installation path: C:\DeploymentService

Database: Customized database.

OpenScape Deployment Service V3 R0.0.0 (733.00)

14. If you have clicked on **Install** previously, you will be presented with messages about the installation process.



Installing

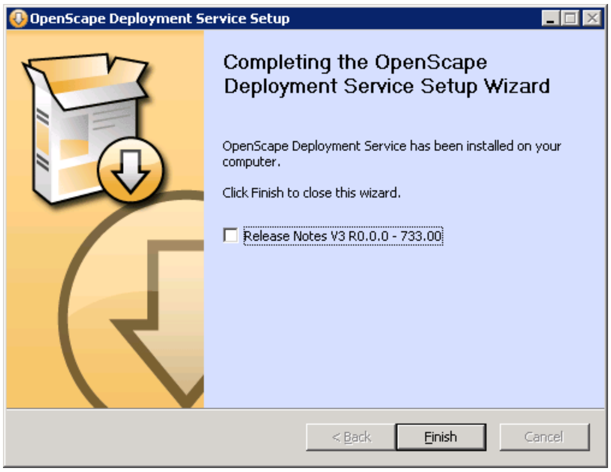
Please wait while OpenScape Deployment Service is being installed.

Installing DLS Web Service API ...

```
RunAsCall: "C:\DeploymentService\Tomcat5\webapps\DeploymentService\database\...
Installing Icons and Installer Help Files ...
Installing JRE for DLS ...
Installing Tomcat for DLS ...
Installing DLS Web Application ...
Installing jre.exe for DLS Clients ...
Installing DLS Web Service API ...
Copying DLS API V100 and V200 ...
Output folder: C:\DeploymentService\api
Copy to C:\DeploymentService\api
```

OpenScape Deployment Service V3 R0.0.0 (725.00)

15. The installation is complete.



Completing the OpenScape Deployment Service Setup Wizard

OpenScape Deployment Service has been installed on your computer.

Click Finish to close this wizard.

□ Release Notes V3 R0.0.0 - 733.00

16. Enter NLB password:

    The password for remote control provided during the NLB administration (see Configure the Network Load Balancer, step 3) must be communicated to the DLS.

    For this purpose, open a DOS box (command shell). The current directory must be set to `<DLS Installationspfad>\DeploymentService\Tomcat5\webapps\DeploymentService\database`

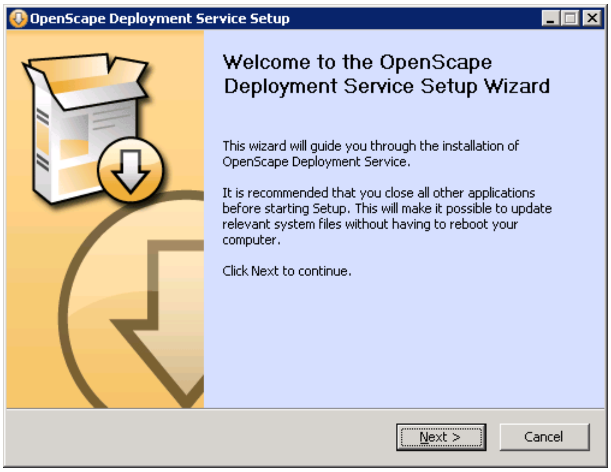
    Enter this DOS command:

    ```
    dlsconfig set nlb_password <the password specified by you>
    ```

    To delete a password, enter an empty string ("") as new password.

4.5.3.2 Second And Further Nodes

1. Start the setup program. After selecting the language, you see a welcome screen.



OpenScape Deployment Service Setup

Welcome to the OpenScape Deployment Service Setup Wizard

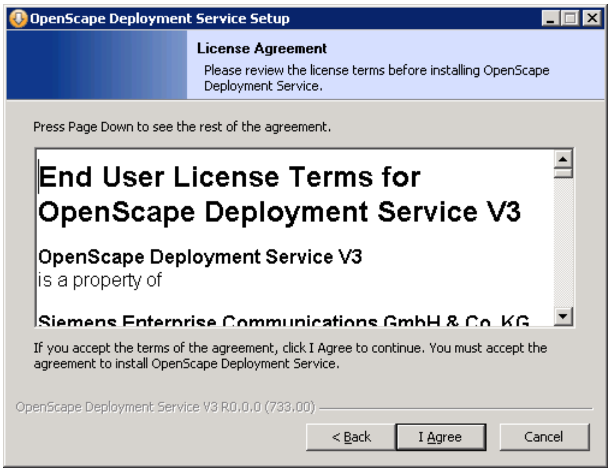
This wizard will guide you through the installation of OpenScape Deployment Service.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Click on **Next**.

2. Click **I Agree** to accept the license agreement.



OpenScape Deployment Service Setup

License Agreement

Please review the license terms before installing OpenScape Deployment Service.

Press Page Down to see the rest of the agreement.

End User License Terms for OpenScape Deployment Service V3

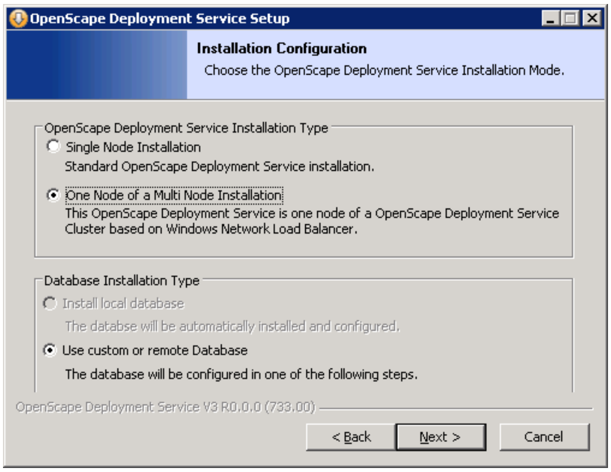
OpenScape Deployment Service V3
is a property of

Siemens Enterprise Communications GmbH & Co. KG

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenScape Deployment Service.

OpenScape Deployment Service V3 R0.0.0 (733.00)

3. In the **Installation Configuration** screen, under **DLS Installation Type**, select the option **One Node of a Multinode Installation**.



OpenScape Deployment Service Setup

Installation Configuration

Choose the OpenScape Deployment Service Installation Mode.

OpenScape Deployment Service Installation Type

○ Single Node Installation
Standard OpenScape Deployment Service installation.

● One Node of a Multi Node Installation
This OpenScape Deployment Service is one node of a OpenScape Deployment Service Cluster based on Windows Network Load Balancer.

Database Installation Type

○ Install local database
The databse will be automatically installed and configured.

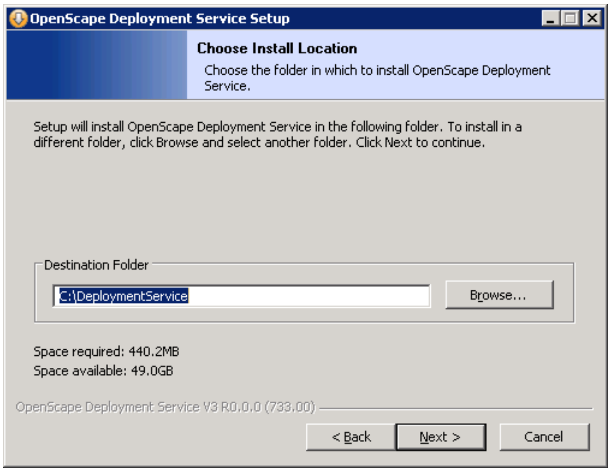
● Use custom or remote Database
The database will be configured in one of the following steps.

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

4. In the **Choose Install Location** screen, choose the target directory, wherein the DLS is to be be installed.

The directory path must not contain blanks, as in "Program Files", for instance.



OpenScape Deployment Service Setup

Choose Install Location

Choose the folder in which to install OpenScape Deployment Service.

Setup will install OpenScape Deployment Service in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

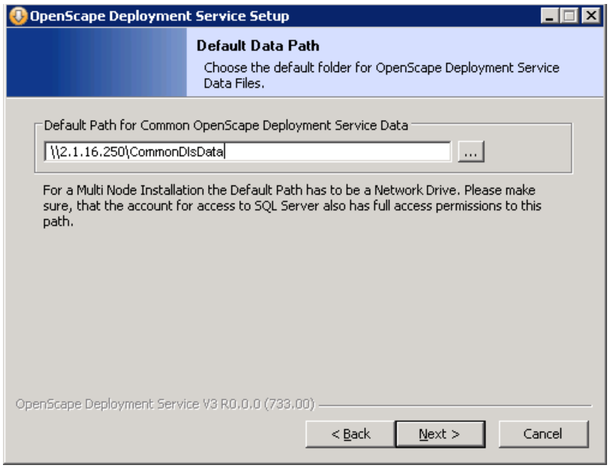
Destination Folder: C:\DeploymentService

Space required: 440.2MB
Space available: 49.0GB

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

5. In the **Default Data Path** screen, specify the path of the directory for common DLS configuration data. This path has been specified in Section 4.5.3.1, "First Node", step 5.



OpenScape Deployment Service Setup

Default Data Path

Choose the default folder for OpenScape Deployment Service Data Files.

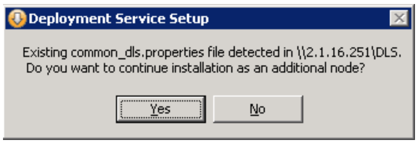
Default Path for Common OpenScape Deployment Service Data: \\2.1.16.250\CommonDlsData

For a Multi Node Installation the Default Path has to be a Network Drive. Please make sure, that the account for access to SQL Server also has full access permissions to this path.

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

6. As the first DLS node is already installed and has stored the file `common_dls.properties` in the appropriate directory, you will be presented with a notification:



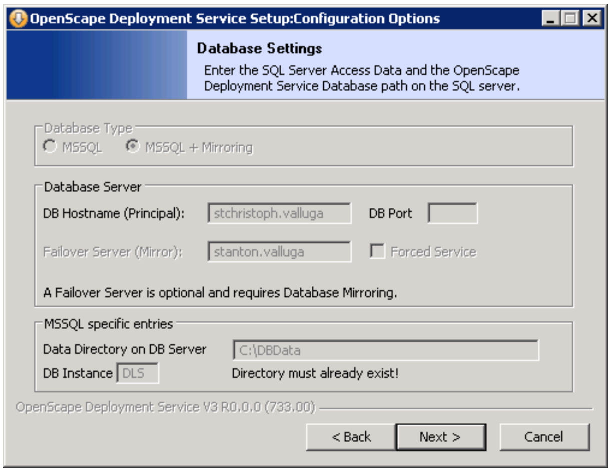
Deployment Service Setup

Existing common_dls.properties file detected in \\2.1.16.251\DLS.
Do you want to continue installation as an additional node?

Click on **Yes**.

7. In the **Database Settings** screen provide the necessary specifications for the database. If you wish to deploy a mirrored database for maximum reliability, select the option **MSSQL + Mirroring** under **Database type**.

   Under **MSSQL specific entries**, in the field **Data Directory on Server**, enter the directory on the database server, in which the DLS database resides. This directory must exist already. Under , you enter the instance the DLS database is to run under (see Section 4.2.1, "Microsoft SQL Server 2005", step 4 resp. Section 4.2.2, "Microsoft SQL Server 2008", step 9).



OpenScape Deployment Service Setup:Configuration Options

Database Settings
Enter the SQL Server Access Data and the OpenScape Deployment Service Database path on the SQL server.

Database Type
○ MSSQL ● MSSQL + Mirroring

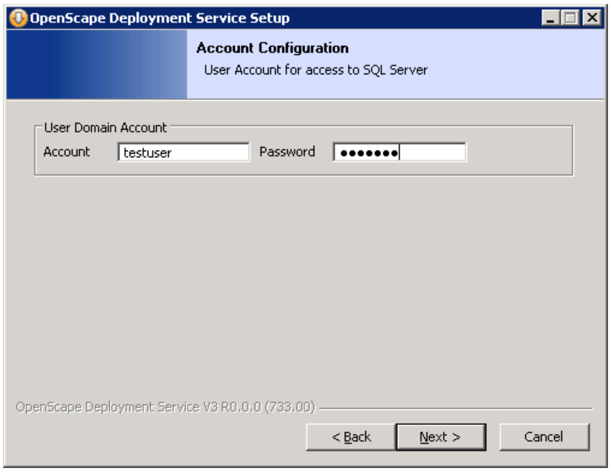
Database Server
DB Hostname (Principal): stchristoph.valluga DB Port
Failover Server (Mirror): stanton.valluga □ Forced Service
A Failover Server is optional and requires Database Mirroring.

MSSQL specific entries
Data Directory on DB Server C:\DBData
DB Instance DLS Directory must already exist!

OpenScape Deployment Service V3 R0.0.0 (733.00)

   Click on **Next**.

8. In the **Account Configuration** screen, in the fields **Account** and **Password**, enter the access data of the user the DLS shall run under. The user must be a member of the administrator group, and it must exist already.



OpenScape Deployment Service Setup

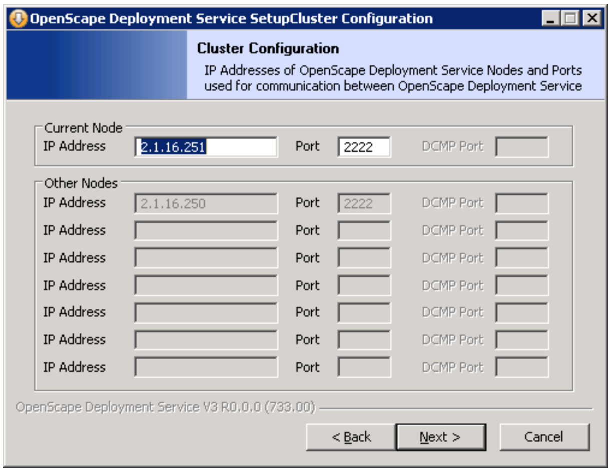
Account Configuration
User Account for access to SQL Server

User Domain Account
Account testuser Password •••••••

OpenScape Deployment Service V3 R0.0.0 (733.00)

   Click on **Next**.

9. In the **Cluster Configuration** screen, under **Current Node**, you see the node machine on which you are currently installing the DLS. Under **Other Nodes**, in the **IP address** fields, enter the IP addresses of the corresponding node machines, and in the **Port** fields, enter the port used by the DLS running on the corresponding machine for communication with the other nodes. If you have selected the DCMP in step 8, you must specify the port on which the DLS receives data from the DCMP in the field **DCMP-Port**. If the data have already been input at the first node, they can be checked, modified, or extended once more.


OpenScape Deployment Service SetupCluster Configuration

Cluster Configuration

IP Addresses of OpenScape Deployment Service Nodes and Ports used for communication between OpenScape Deployment Service

Current Node

IP Address	2.1.16.251	Port	2222	DCMP Port	

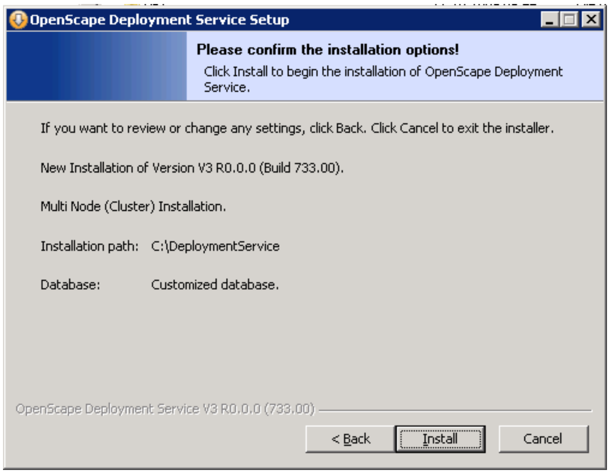
Other Nodes

IP Address	2.1.16.250	Port	2222	DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	
IP Address		Port		DCMP Port	

OpenScape Deployment Service V3 R0.0.0 (733.00)

Click on **Next**.

10. In the next screen, you see a brief overview on the installation settings. To start the installation, click on **Install**; to revise settings, click on **Back**.


OpenScape Deployment Service Setup

Please confirm the installation options!

Click Install to begin the installation of OpenScape Deployment Service.

If you want to review or change any settings, click Back. Click Cancel to exit the installer.

New Installation of Version V3 R0.0.0 (Build 733.00).

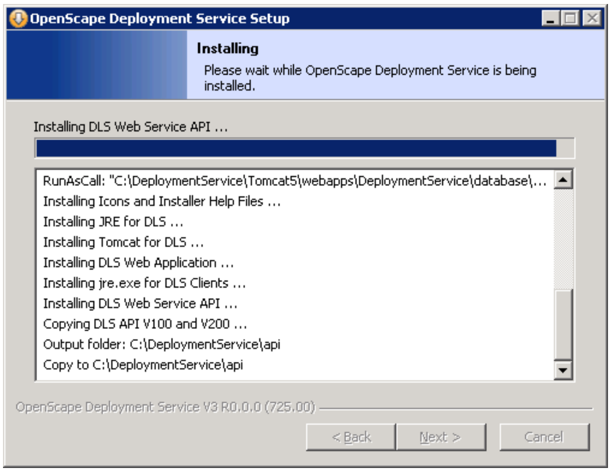
Multi Node (Cluster) Installation.

Installation path: C:\DeploymentService

Database: Customized database.

OpenScape Deployment Service V3 R0.0.0 (733.00)

11. If you have clicked on **Install** previously, you will be presented with messages about the installation process.



Installing

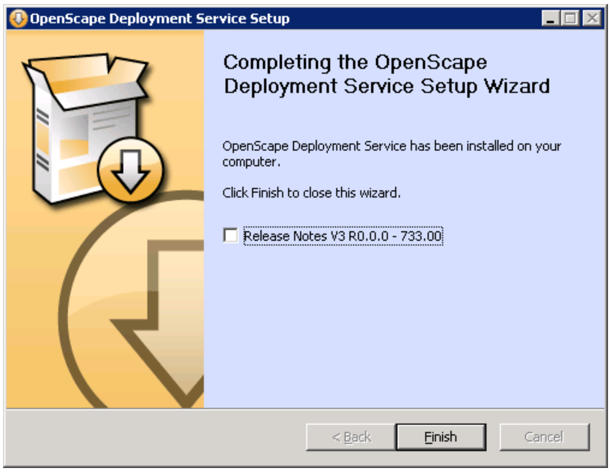
Please wait while OpenScape Deployment Service is being installed.

Installing DLS Web Service API ...

```
RunAsCall: "C:\DeploymentService\Tomcat5\webapps\DeploymentService\database\...
Installing Icons and Installer Help Files ...
Installing JRE for DLS ...
Installing Tomcat for DLS ...
Installing DLS Web Application ...
Installing jre.exe for DLS Clients ...
Installing DLS Web Service API ...
Copying DLS API V100 and V200 ...
Output folder: C:\DeploymentService\api
Copy to C:\DeploymentService\api
```

OpenScape Deployment Service V3 R0.0.0 (725.00)

12. The installation is complete.



Completing the OpenScape Deployment Service Setup Wizard

OpenScape Deployment Service has been installed on your computer.

Click Finish to close this wizard.

□ Release Notes V3 R0.0.0 - 733.00

4.6 SQL Database Mirroring Setup

To guarantee maximum resilience, it is possible to deploy two separate database servers. At this, only one database server is connected to the DLS (single node or cluster), while the data are mirrored on the other server. In case the main server ("Principal") fails, the second server ("Mirror") assumes its function.

For database mirroring, two models are supported:

- **Synchronous Mirroring**: A third server ("Witness") monitors the state of the main server. If the Principal should fail, the Witness will switch over to the Mirror, which will hereby become the Principal. Moreover, the Witness checks whether all transactions have been completed on the Mirror, too. Thus it is ensured that no data loss will occur. However, the performance will be slightly lower than with asynchronous mirroring.

> ⓘ High Availability with guaranteed data loss prevention is possible only with synchronous mirroring.

- **Asynchronous Mirroring**: There is no Witness, and the switchover to the mirror server is done by "Forced Service", i. e., by the DLS.

The following requirements must be fulfilled for database mirroring:

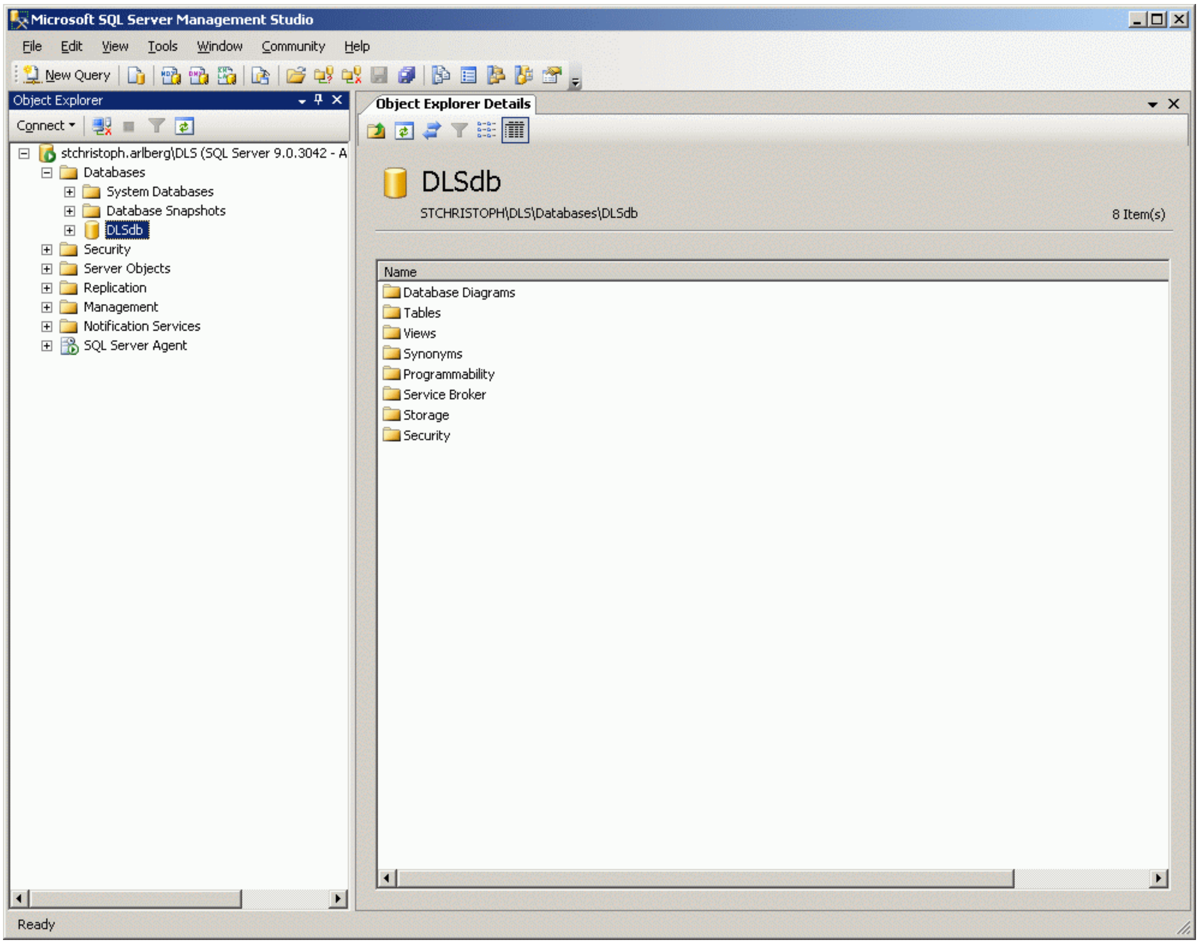
- Microsoft SQL Server 2005/2008 Enterprise Edition with Service Packs 1 und 2 is installed on all servers needed for database mirroring (Prinicpal, Mirror, and Witness, where applicable). If available, SP3 should also be installed (see Section 4.2, "Install MS SQL Server for Remote Database"). The databases can be installed on the DLS nodes as well as on separate server machines.
- Microsoft SQL Server Management Studio has to be installed.
- At least the first DLS node is installed (see Section 4.5, "Installing the DLS") because mirroring can be set up only for a DLS database that has already been set up. This is part of the installation process for the first DLS node.
- The service **DeploymentService** is stopped on all participating DLS nodes.
- For the DLS database (DLSdb), the recovery model "Full" is set.
- The size for the TransactionLog is unlimited.

> As the transaction log can reach any size, it might occur that the hard disk in use gets full, which would lead to SQL server and DLS failure.
> Thus, create a backup plan according to your requirements, and save the transaction log regularly, in addition to the DLS data. This effects a reduction of the currently active transaction log. Moreover, the transaction log should be saved significantly more frequent than the data proper, in order to keep the file as small as possible.
> When a database backup is performed, a complementary .trn file is generated. Those files are the backups of the transaction logs. This process makes sure that the transaction log-File "DLS_Log.LDF" does not grow endlessly.
> The very first creation of a .trn file might take considerably longer when a very large "DLS_Log.LDF" file has to be processed.
> A DLS database restore does not require a correspondant .trn file. However, it is recommended to keep the latest transaction log file for investigation purposes in case a problem should occur.

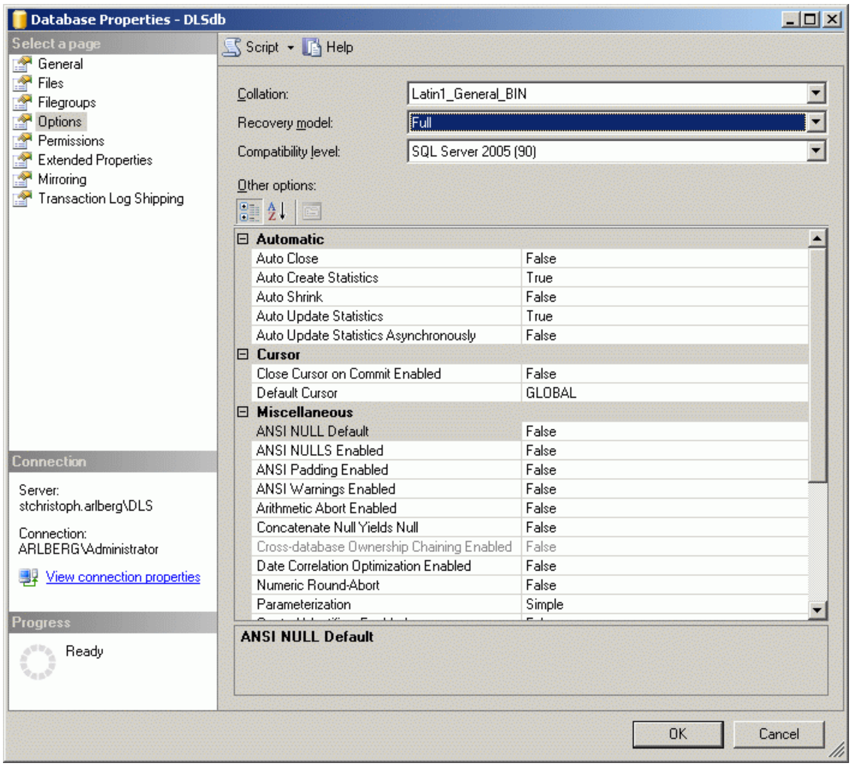
The installation of Microsoft SQL Server 2005/2008 Enterprise Edition is described in Section 4.2, "Install MS SQL Server for Remote Database". We will continue with setting up a synchronously mirrored database.

> When database mirroring is active, no restore of backups is possible.

1. On the machine that is to be used as Principal, go to **Start** > **Microsoft SQL Server 2005/ 2008** > **Microsoft SQL Server Management Studio**. You will be presented with an overview on the existing databases. The Principal should be that database machine that has been specified with the DLS installation.



2. Navigate to the tree on the right hand side of MS SQL Server Management Studio and select the entry **DLSdb**. Now, with the right hand mouse key, click on **DLSdb** and, in the context menu, choose **Properties**. The **Database Properties** screen opens. In the **Options submenu**, under **Recovery model**, select the **Full** option.



Server:
stchristoph.arlberg\DLS

Connection:
ARLBERG\Administrator

Collation: Latin1_General_BIN

Recovery model: Full

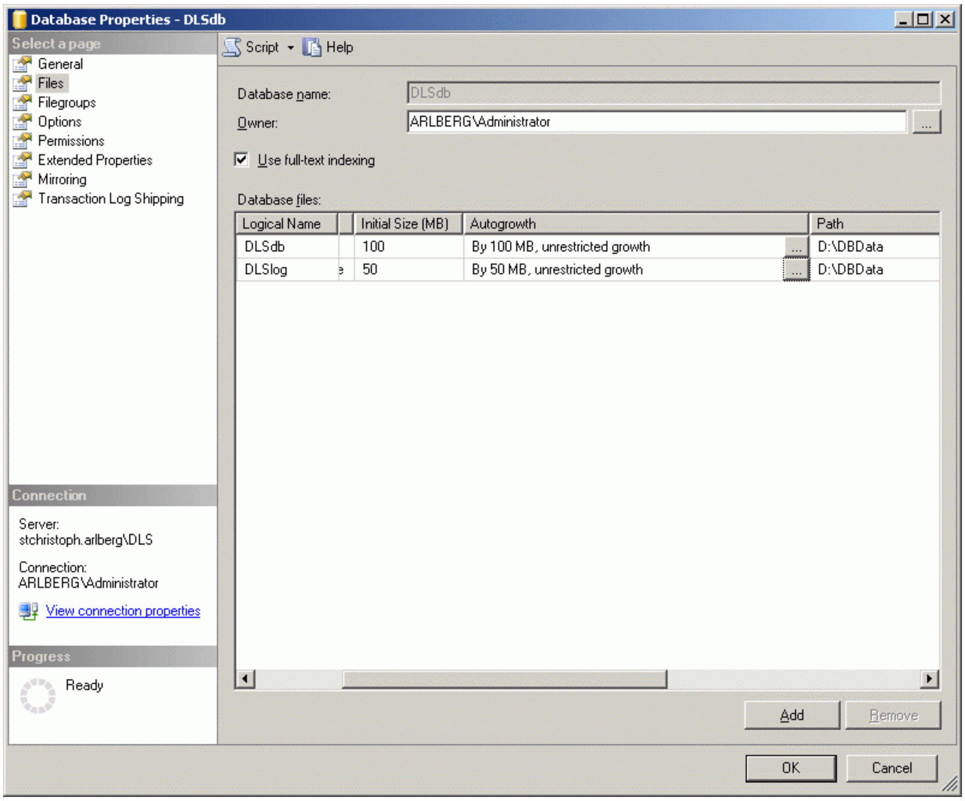
Compatibility level: SQL Server 2005 (90)

Other options:

Automatic	
Auto Close	False
Auto Create Statistics	True
Auto Shrink	False
Auto Update Statistics	True
Auto Update Statistics Asynchronously	False
Cursor	
Close Cursor on Commit Enabled	False
Default Cursor	GLOBAL
Miscellaneous	
ANSI NULL Default	False
ANSI NULLS Enabled	False
ANSI Padding Enabled	False
ANSI Warnings Enabled	False
Arithmetic Abort Enabled	False
Concatenate Null Yields Null	False
Cross-database Ownership Chaining Enabled	False
Date Correlation Optimization Enabled	False
Numeric Round-Abort	False
Parameterization	Simple

ANSI NULL Default

3. It is recommended to set an unlimited file size in the **Files** submenu by selecting **unrestricted growth** for **DLSdb** and **DLSlog**.



Database name: DLSdb

Owner: ARLBERG\Administrator

☑ Use full-text indexing

Database files:

Logical Name		Initial Size (MB)	Autogrowth	Path
DLSdb		100	By 100 MB, unrestricted growth	D:\DBData
DLSlog		50	By 50 MB, unrestricted growth	D:\DBData

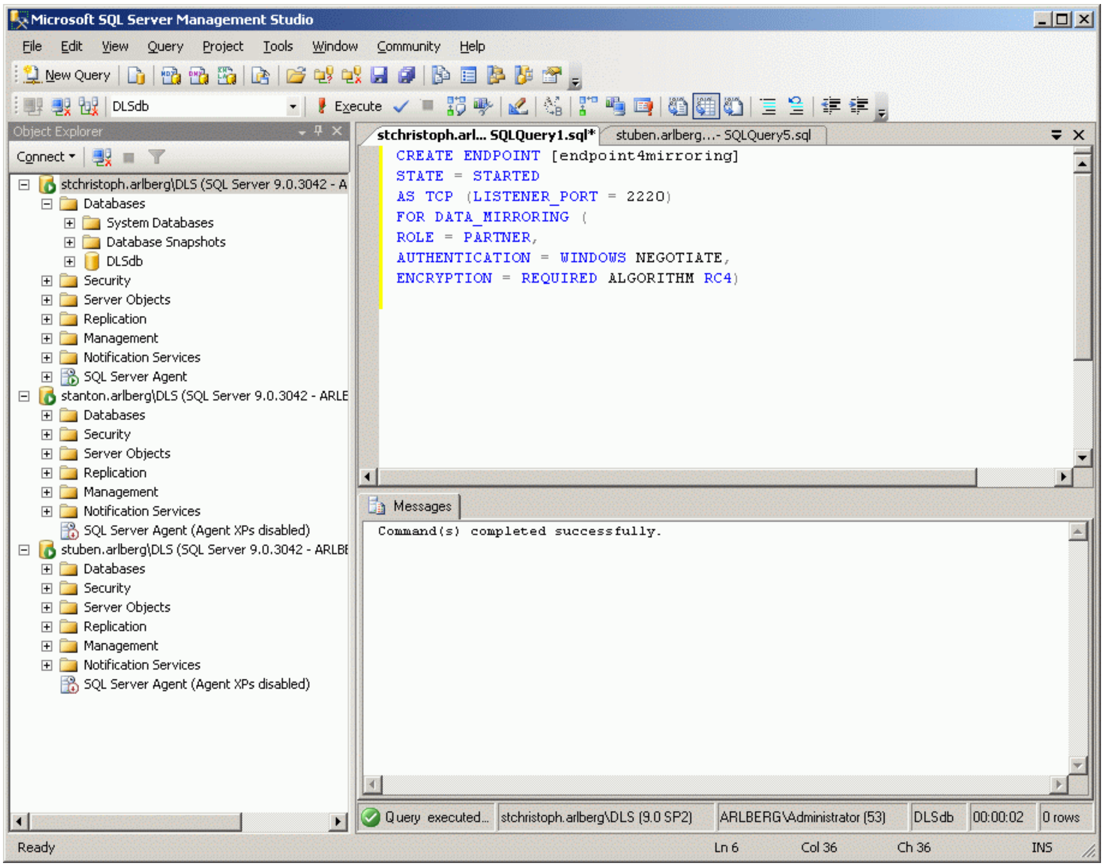
Server:
stchristoph.arlberg\DLS

Connection:
ARLBERG\Administrator

Ready

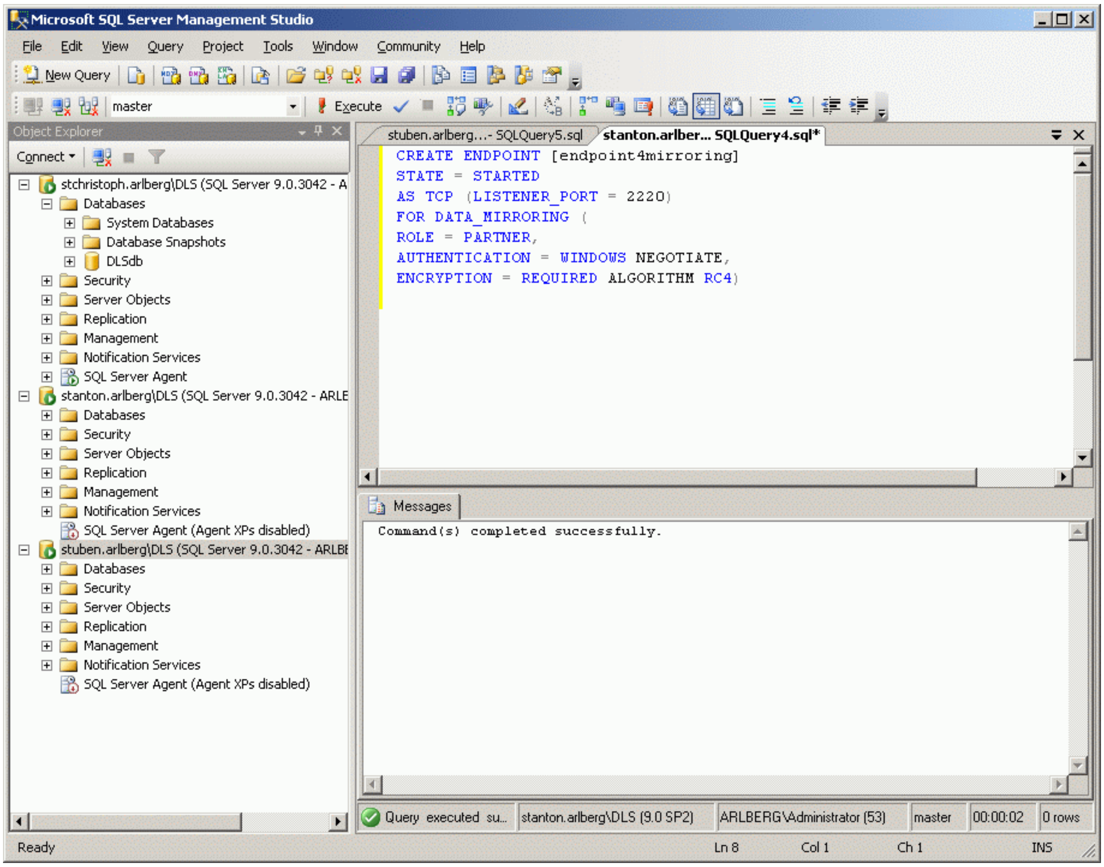
4. Create the "endpoints" for database mirroring by executing the following commands at the Principal server and the Mirror server:

```
CREATE ENDPOINT [endpoint4mirroring]
   STATE = STARTED
   AS TCP (LISTENER_PORT = 2220, LISTENER_IP = ALL)
   FOR DATA_MIRRORING (
      ROLE = PARTNER,
      AUTHENTICATION = WINDOWS NEGOTIATE,
      ENCRYPTION = REQUIRED ALGORITHM RC4)
```


Microsoft SQL Server Management Studio
File Edit View Query Project Tools Window Community Help
New Query
DLSdb
Execute
Object Explorer
Connect ▾
stchristoph.arlberg\DLS (SQL Server 9.0.3042 - A
Databases
System Databases
Database Snapshots
DLSdb
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent
stanton.arlberg\DLS (SQL Server 9.0.3042 - ARLE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stuben.arlberg\DLS (SQL Server 9.0.3042 - ARLBE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stchristoph.arl... SQLQuery1.sql*
stuben.arlberg....- SQLQuery5.sql
Messages
Query executed...
stchristoph.arlberg\DLS (9.0 SP2)
ARLBERG\Administrator (53)
DLSdb
00:00:02
0 rows
Ready
Ln 6
Col 36
Ch 36
INS

```
CREATE ENDPOINT [endpoint4mirroring]
STATE = STARTED
AS TCP (LISTENER_PORT = 2220)
FOR DATA_MIRRORING (
ROLE = PARTNER,
AUTHENTICATION = WINDOWS NEGOTIATE,
ENCRYPTION = REQUIRED ALGORITHM RC4)
```

```
Command(s) completed successfully.
```

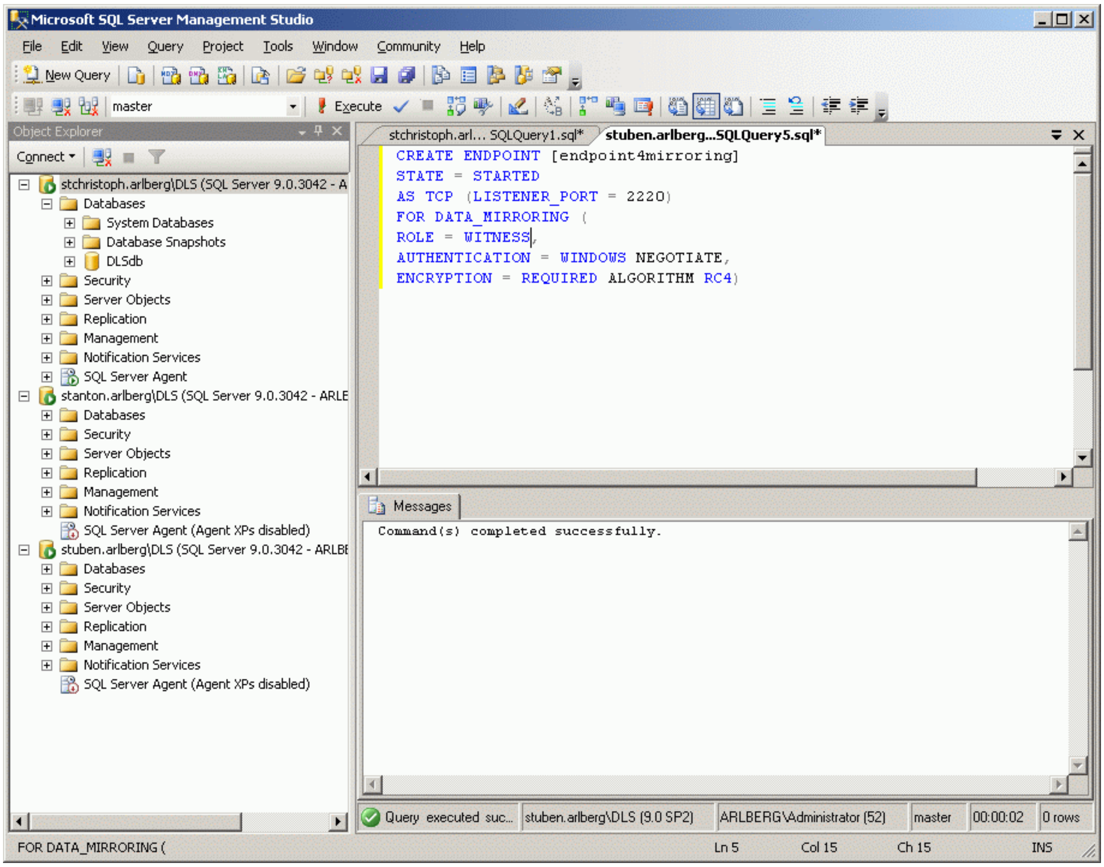

Microsoft SQL Server Management Studio
File Edit View Query Project Tools Window Community Help
New Query
master
Execute
Object Explorer
Connect
stchristoph.arlberg\DLS (SQL Server 9.0.3042 - A
Databases
System Databases
Database Snapshots
DLSdb
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent
stanton.arlberg\DLS (SQL Server 9.0.3042 - ARLE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stuben.arlberg\DLS (SQL Server 9.0.3042 - ARLBE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stuben.arlberg...- SQLQuery5.sql
stanton.arlber... SQLQuery4.sql*
Messages
Query executed su...
stanton.arlberg\DLS (9.0 SP2)
ARLBERG\Administrator (53)
master
00:00:02
0 rows
Ready
Ln 8
Col 1
Ch 1
INS

```
CREATE ENDPOINT [endpoint4mirroring]
STATE = STARTED
AS TCP (LISTENER_PORT = 2220)
FOR DATA_MIRRORING (
ROLE = PARTNER,
AUTHENTICATION = WINDOWS NEGOTIATE,
ENCRYPTION = REQUIRED ALGORITHM RC4)
```

```
Command(s) completed successfully.
```

5. Create the Witness by executing the following commands on the designated machine:

```
CREATE ENDPOINT [endpoint4mirroring]
   STATE = STARTED
   AS TCP (LISTENER_PORT = 2220, LISTENER_IP = ALL)
   FOR DATA_MIRRORING (
      ROLE = WITNESS,
      AUTHENTICATION = WINDOWS NEGOTIATE,
      ENCRYPTION = REQUIRED ALGORITHM RC4)
```


Microsoft SQL Server Management Studio
File Edit View Query Project Tools Window Community Help
New Query
master
Execute
Object Explorer
Connect
stchristoph.arlberg\DLS (SQL Server 9.0.3042 - A
Databases
System Databases
Database Snapshots
DLSdb
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent
stanton.arlberg\DLS (SQL Server 9.0.3042 - ARLE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stuben.arlberg\DLS (SQL Server 9.0.3042 - ARLBE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stchristoph.arl... SQLQuery1.sql*
stuben.arlberg...SQLQuery5.sql*
Messages
Query executed suc...
stuben.arlberg\DLS (9.0 SP2)
ARLBERG\Administrator (52)
master
00:00:02
0 rows
FOR DATA_MIRRORING (
Ln 5
Col 15
Ch 15
INS

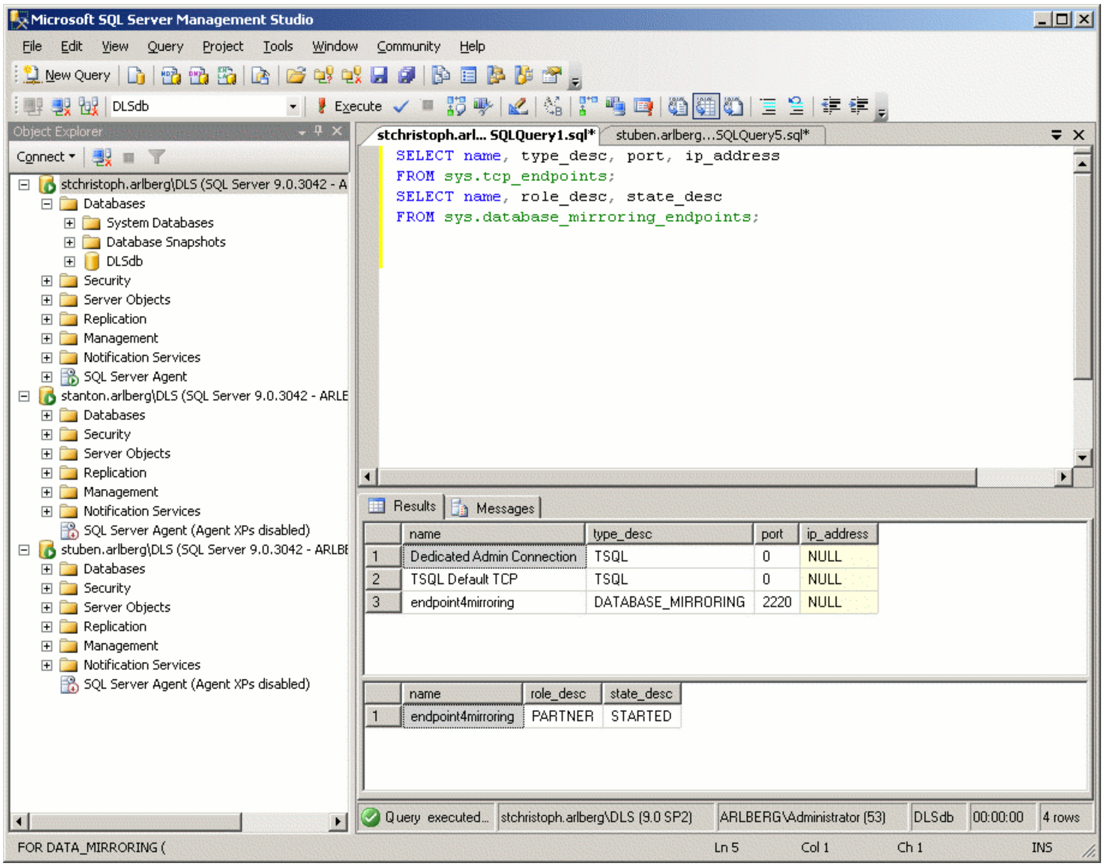
```
CREATE ENDPOINT [endpoint4mirroring]
STATE = STARTED
AS TCP (LISTENER_PORT = 2220)
FOR DATA_MIRRORING (
ROLE = WITNESS,
AUTHENTICATION = WINDOWS NEGOTIATE,
ENCRYPTION = REQUIRED ALGORITHM RC4)
```

```
Command(s) completed successfully.
```

6. You can view the result by executing the code on all three database servers:

```
SELECT name, type_desc, port, ip_address
   FROM sys.tcp_endpoints;
SELECT name, role_desc, state_desc
   FROM sys.database_mirroring_endpoints;
```

This exemplifies the output for the Principal.



Microsoft SQL Server Management Studio
File Edit View Query Project Tools Window Community Help
New Query
DLSdb
Execute
Object Explorer
Connect
stchristoph.arlberg\DLS (SQL Server 9.0.3042 - A
Databases
System Databases
Database Snapshots
DLSdb
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent
stanton.arlberg\DLS (SQL Server 9.0.3042 - ARLE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stuben.arlberg\DLS (SQL Server 9.0.3042 - ARLBE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stchristoph.arl... SQLQuery1.sql*
stuben.arlberg...SQLQuery5.sql*
Results
Messages

```
SELECT name, type_desc, port, ip_address
FROM sys.tcp_endpoints;
SELECT name, role_desc, state_desc
FROM sys.database_mirroring_endpoints;
```

	name	type_desc	port	ip_address
1	Dedicated Admin Connection	TSQL	0	NULL
2	TSQL Default TCP	TSQL	0	NULL
3	endpoint4mirroring	DATABASE_MIRRORING	2220	NULL

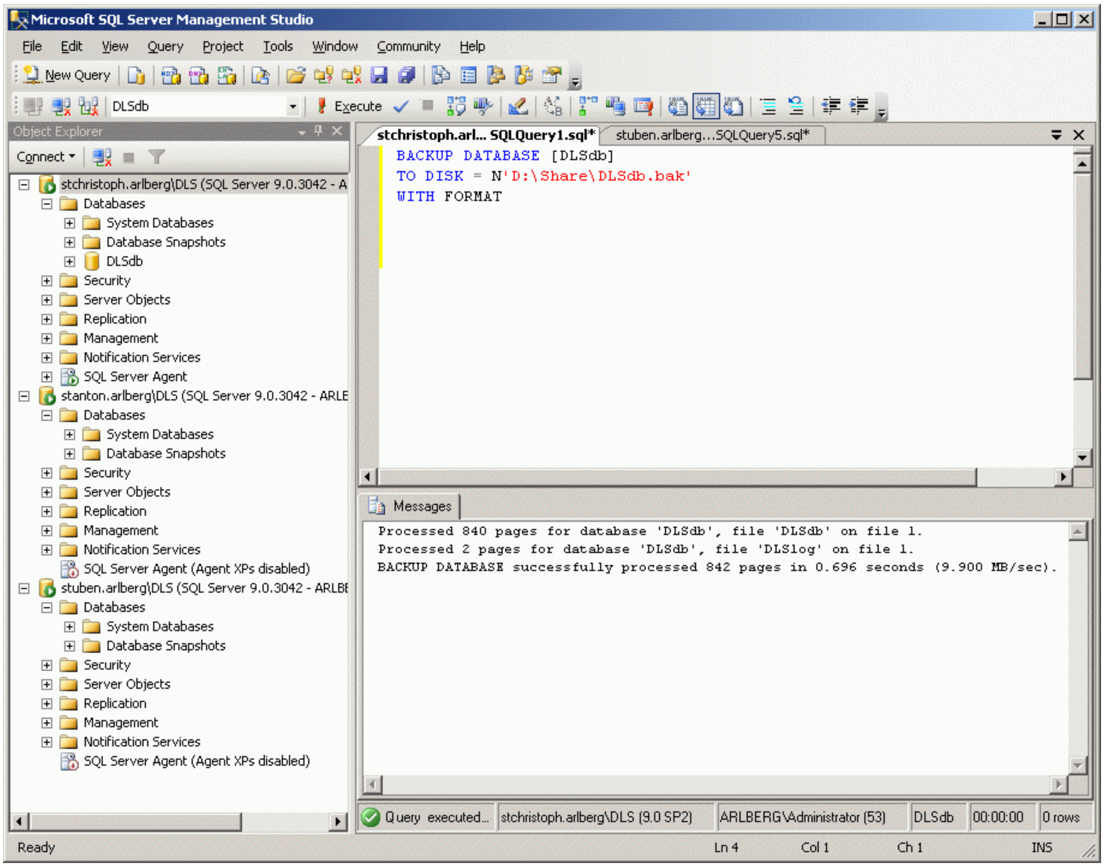
	name	role_desc	state_desc
1	endpoint4mirroring	PARTNER	STARTED

Query executed... | stchristoph.arlberg\DLS (9.0 SP2) | ARLBERG\Administrator (53) | DLSdb | 00:00:00 | 4 rows

FOR DATA_MIRRORING (Ln 5 Col 1 Ch 1 INS

7. Now, generate a backup of the DLS database on the Principal server:

```
BACKUP DATABASE [DLSdb]
   TO DISK = N'D:\Share\DLSdb.bak'
   WITH FORMAT
```

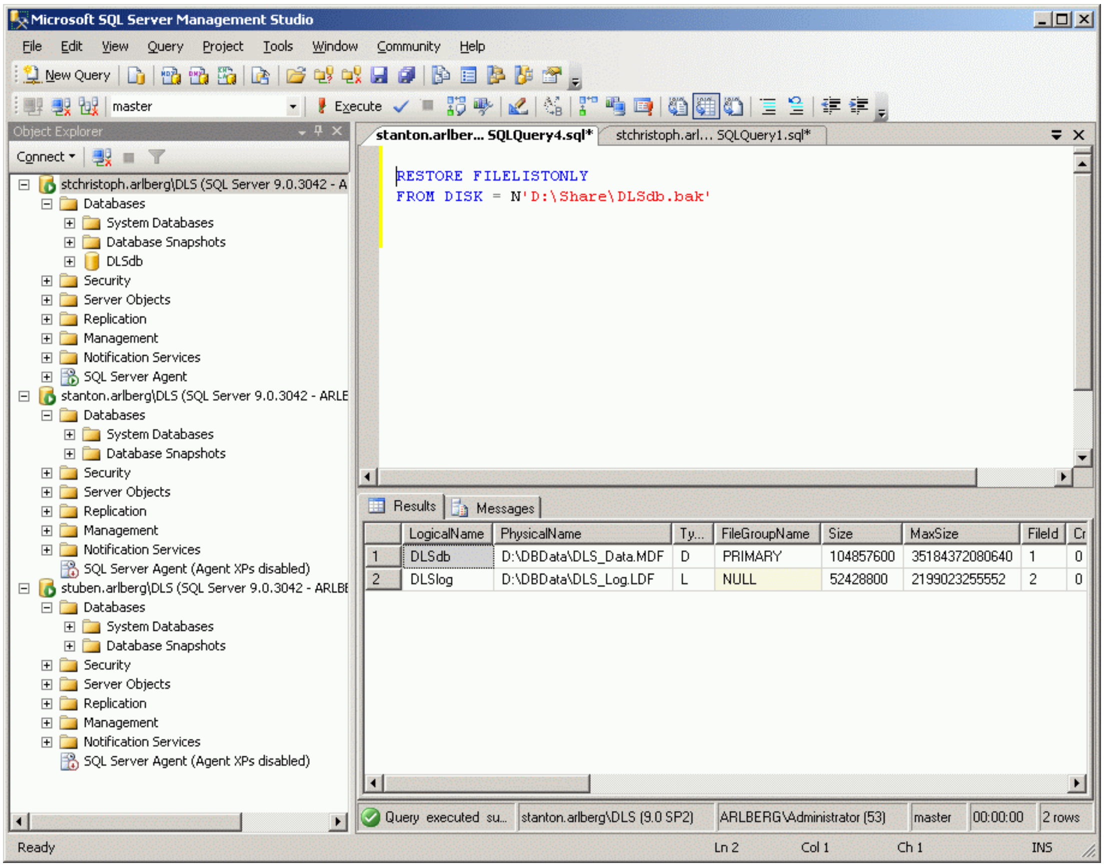


```
BACKUP DATABASE [DLSdb]
TO DISK = N'D:\Share\DLSdb.bak'
WITH FORMAT
```

```
Processed 840 pages for database 'DLSdb', file 'DLSdb' on file 1.
Processed 2 pages for database 'DLSdb', file 'DLSlog' on file 1.
BACKUP DATABASE successfully processed 842 pages in 0.696 seconds (9.900 MB/sec).
```

8. To prepare for database recovery at the Mirror server, you must know the logical and physical names of the backup files. For this purpose, enter the following code:

```
RESTORE FILELISTONLY
   FROM DISK = N'D:\Share\DLSdb.bak'
```



```
RESTORE FILELISTONLY
FROM DISK = N'D:\Share\DLSdb.bak'
```

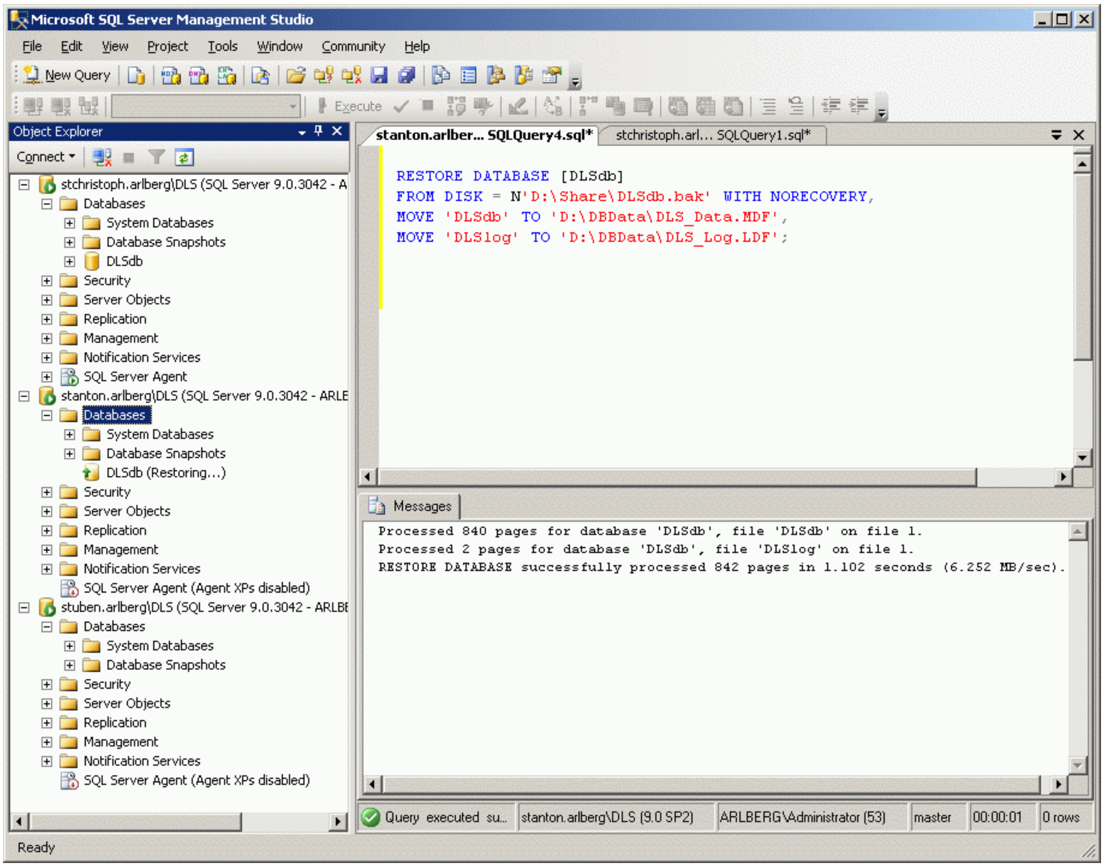
	LogicalName	PhysicalName	Ty...	FileGroupName	Size	MaxSize	FileId	Cr
1	DLSdb	D:\DBData\DLS_Data.MDF	D	PRIMARY	104857600	35184372080640	1	0
2	DLSlog	D:\DBData\DLS_Log.LDF	L	NULL	52428800	2199023255552	2	0

Query executed su... | stanton.arlberg\DLS (9.0 SP2) | ARLBERG\Administrator (53) | master | 00:00:00 | 2 rows

Ln 2 Col 1 Ch 1 INS

9. By means of these names, start the database recovery now.

```
RESTORE DATABASE [DLSdb]
FROM DISK = N'D:\Share\DLSdb.bak' WITH NORECOVERY,
MOVE 'DLSdb' TO 'D:\DBData\DLS_Data.MDF',
MOVE 'DLSlog' TO 'D:\DBData\DLS_Log.LDF';
```

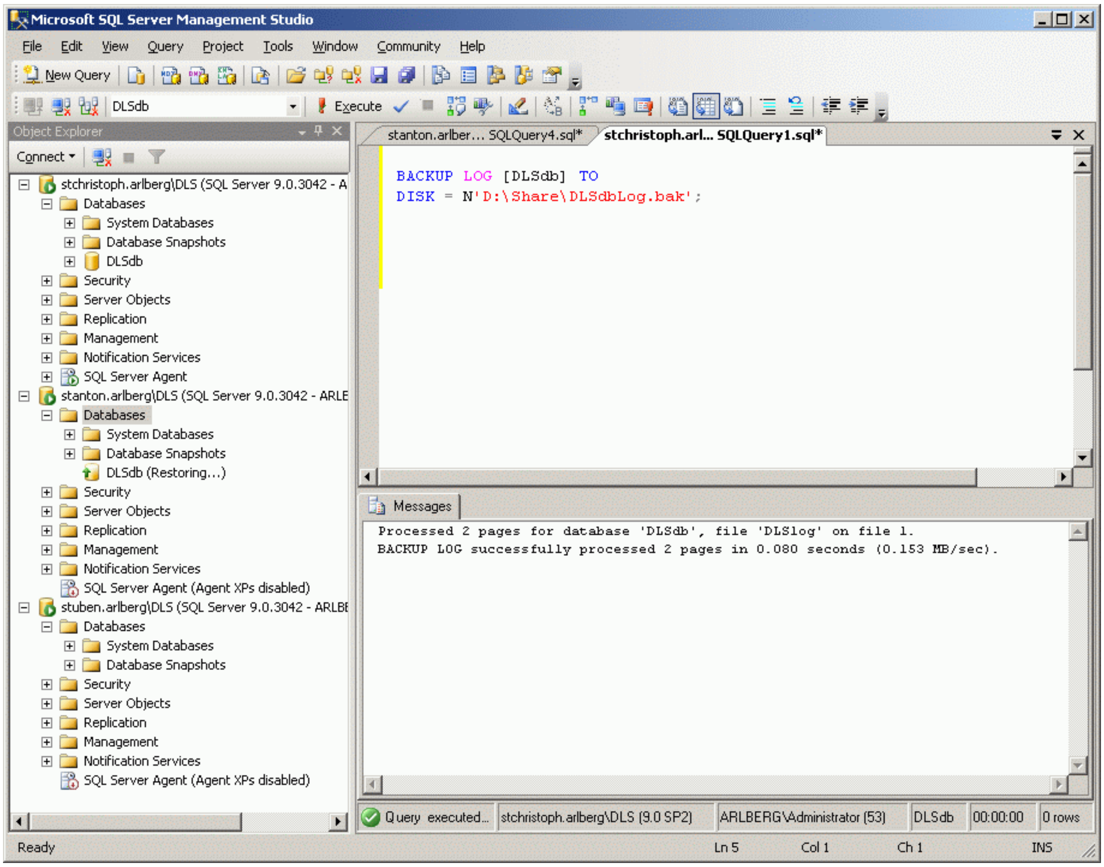


```
RESTORE DATABASE [DLSdb]
FROM DISK = N'D:\Share\DLSdb.bak' WITH NORECOVERY,
MOVE 'DLSdb' TO 'D:\DBData\DLS_Data.MDF',
MOVE 'DLSlog' TO 'D:\DBData\DLS_Log.LDF';
```

```
Processed 840 pages for database 'DLSdb', file 'DLSdb' on file 1.
Processed 2 pages for database 'DLSdb', file 'DLSlog' on file 1.
RESTORE DATABASE successfully processed 842 pages in 1.102 seconds (6.252 MB/sec).
```

10. On the Principal, generate a backup of the initial transaction protocol.

```
BACKUP LOG [DLSdb] TO
   DISK = N'D:\Share\DLSdbLog.bak';
```



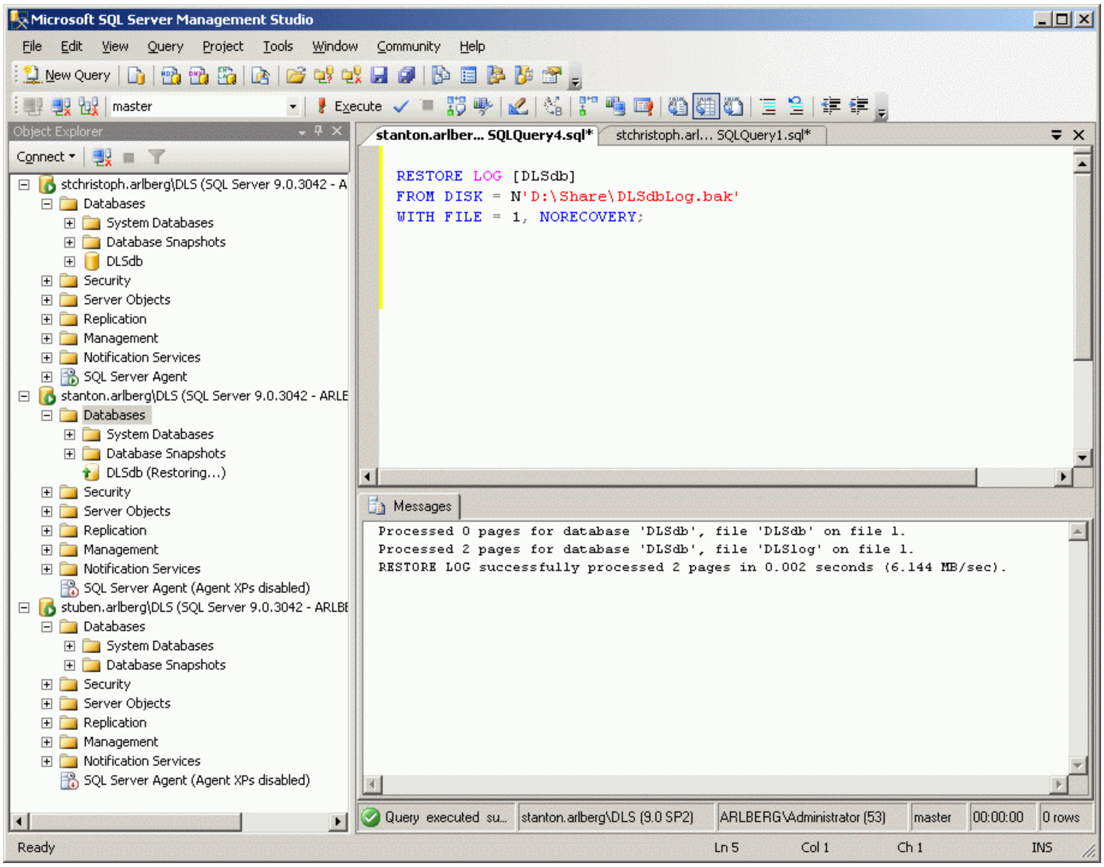
```
BACKUP LOG [DLSdb] TO
DISK = N'D:\Share\DLSdbLog.bak';
```

```
Processed 2 pages for database 'DLSdb', file 'DLSlog' on file 1.
BACKUP LOG successfully processed 2 pages in 0.080 seconds (0.153 MB/sec).
```

Note down the file ID in the message window (in the example: 1)

11. Subsequently, carry out the recovery of the transaction protocol. Take the file ID from the message window of the previous backup process (see step 10).

```
RESTORE LOG [DLSdb]
FROM DISK = N'D:\Share\DLSdbLOG.bak'
WITH FILE = 1, NORECOVERY;
```

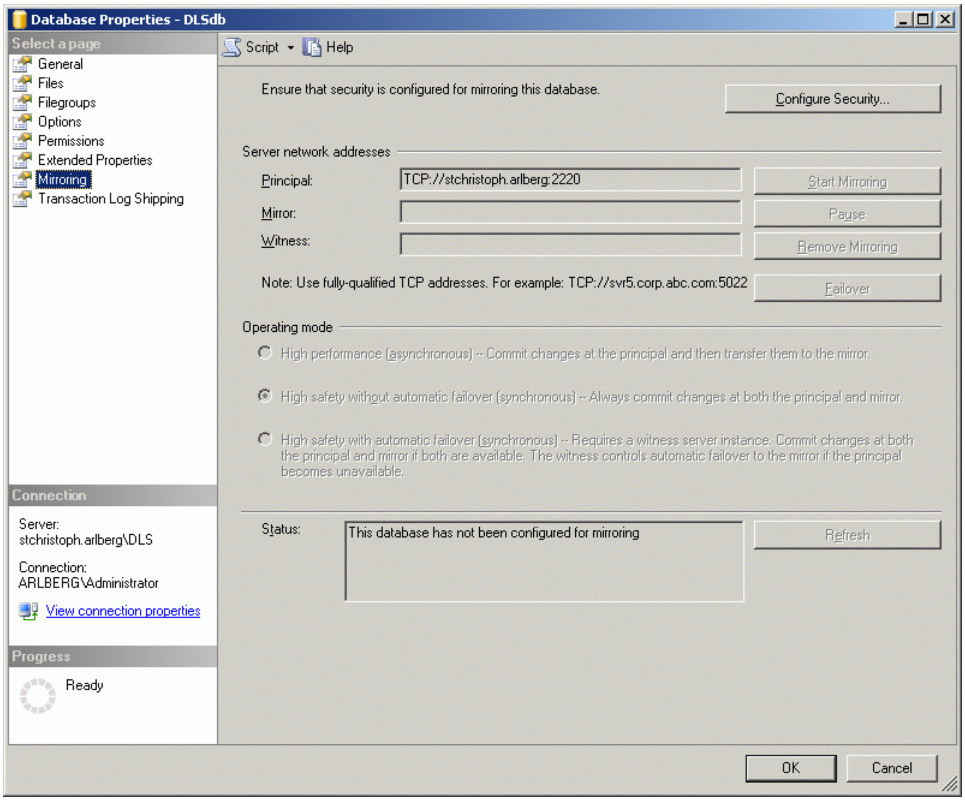


```
RESTORE LOG [DLSdb]
FROM DISK = N'D:\Share\DLSdbLog.bak'
WITH FILE = 1, NORECOVERY;
```

```
Processed 0 pages for database 'DLSdb', file 'DLSdb' on file 1.
Processed 2 pages for database 'DLSdb', file 'DLSlog' on file 1.
RESTORE LOG successfully processed 2 pages in 0.002 seconds (6.144 MB/sec).
```

12. The DLS uses its own stored procedures in the master database, which are not comprised by the DLSdb backup and restore. Hence, the script `create_master_usp.sql` must be executed at the Mirror. You can find this script in
`<DLS installation directory>\Tomcat5\webapps\`
`DeploymentService\database\dbinstaller\mssql\DlsDb`

13. To start the mirroring, click on the database **DLSdb** with the right hand mouse key, navigate to the **Tasks** submenu, and select **Mirror**.



Ensure that security is configured for mirroring this database.

Server network addresses

Principal: TCP://stchristoph.arlberg:2220

Mirror:

Witness:

Note: Use fully-qualified TCP addresses. For example: TCP://svr5.corp.abc.com:5022

Operating mode

○ High performance (asynchronous) -- Commit changes at the principal and then transfer them to the mirror.

● High safety without automatic failover (synchronous) -- Always commit changes at both the principal and mirror.

○ High safety with automatic failover (synchronous) -- Requires a witness server instance. Commit changes at both the principal and mirror if both are available. The witness controls automatic failover to the mirror if the principal becomes unavailable.

Status: This database has not been configured for mirroring

Connection

Server:
stchristoph.arlberg\DLS

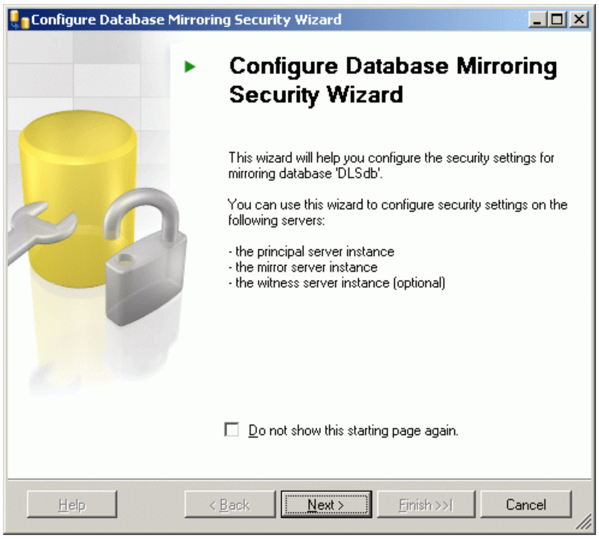
Connection:
ARLBERG\Administrator

Progress

Ready

Click on **Configure Security...**.

14. A wizard for configuring the mirroring security settings appears.



Configure Database Mirroring Security Wizard

This wizard will help you configure the security settings for mirroring database 'DLSdb'.

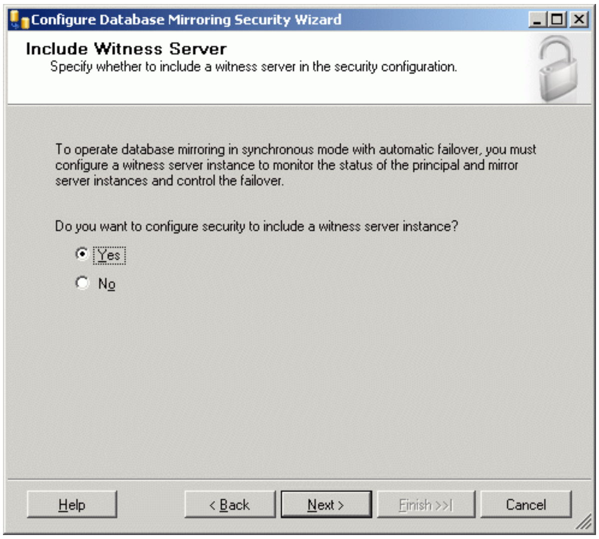
You can use this wizard to configure security settings on the following servers:

- the principal server instance
- the mirror server instance
- the witness server instance (optional)

☐ Do not show this starting page again.

Click on **Next**.

15. In the **Include Witness Server** screen, chose **Yes**.



Include Witness Server

Specify whether to include a witness server in the security configuration.

To operate database mirroring in synchronous mode with automatic failover, you must configure a witness server instance to monitor the status of the principal and mirror server instances and control the failover.

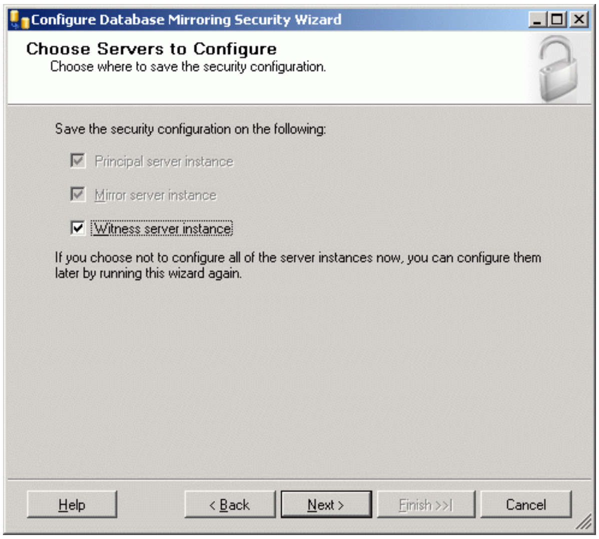
Do you want to configure security to include a witness server instance?

● Yes

○ No

Click on **Next**.

16. Please ensure that in the **Choose Servers to Configure** screen, the option **Witness server instance** is selected.



Choose Servers to Configure

Choose where to save the security configuration.

Save the security configuration on the following:

☑ Principal server instance

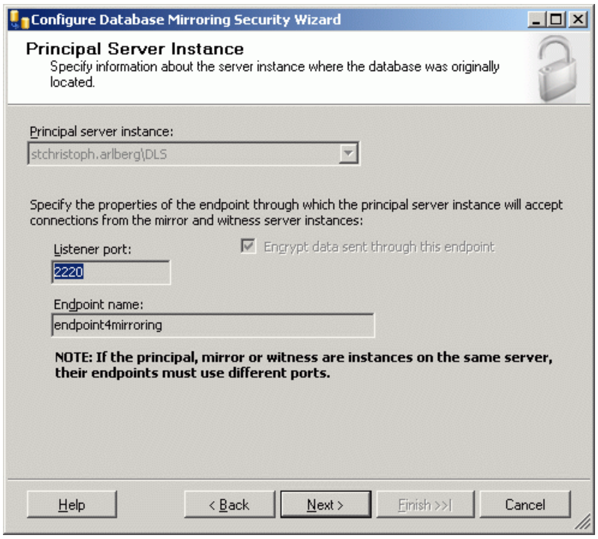
☑ Mirror server instance

☑ Witness server instance

If you choose not to configure all of the server instances now, you can configure them later by running this wizard again.

Click on **Next**.

17. In the **Principal Server Instance** screen, check the settings for the Principal server, and modify them, if necessary. It is especially important that the port specified in the **Listener port** field, which has been determined with the role allocation (steps 4,5), has not been allocated elsewhere.



Principal Server Instance

Specify information about the server instance where the database was originally located.

Principal server instance: stchristoph.arlberg\DLS

Specify the properties of the endpoint through which the principal server instance will accept connections from the mirror and witness server instances:

Listener port: 2220

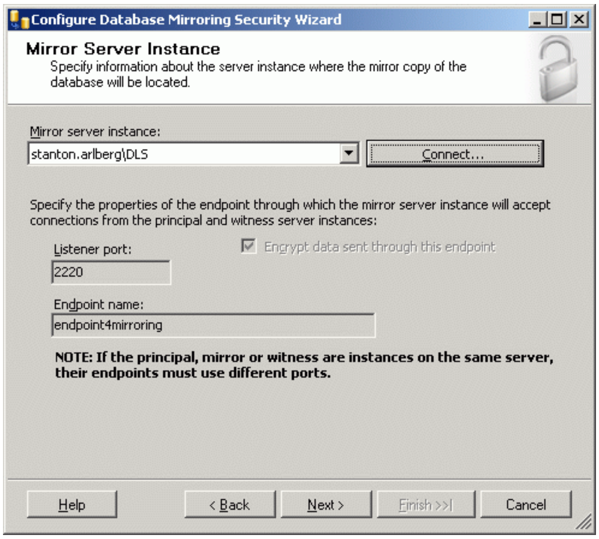
☑ Encrypt data sent through this endpoint

Endpoint name: endpoint4mirroring

NOTE: If the principal, mirror or witness are instances on the same server, their endpoints must use different ports.

Click on **Next**.

18. Analogous to the Principal server, check the settings for the Mirror server in the **Mirror Server Instance** screen, and modify them, if necessary.



Configure Database Mirroring Security Wizard

Mirror Server Instance

Specify information about the server instance where the mirror copy of the database will be located.

Mirror server instance: stanton.arlberg\DLS

Specify the properties of the endpoint through which the mirror server instance will accept connections from the principal and witness server instances:

Listener port: 2220

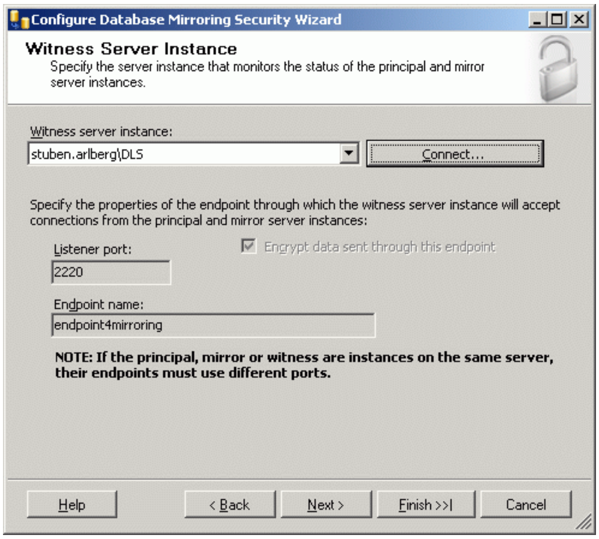
☑ Encrypt data sent through this endpoint

Endpoint name: endpoint4mirroring

NOTE: If the principal, mirror or witness are instances on the same server, their endpoints must use different ports.

Click on **Next**.

19. Analogous to the Mirror server, check the settings for the Mirror server in the **Witness Server Instance** screen, and modify them, if necessary.



Configure Database Mirroring Security Wizard

Witness Server Instance

Specify the server instance that monitors the status of the principal and mirror server instances.

Witness server instance: stuben.arlberg\DLS

Specify the properties of the endpoint through which the witness server instance will accept connections from the principal and mirror server instances:

Listener port: 2220

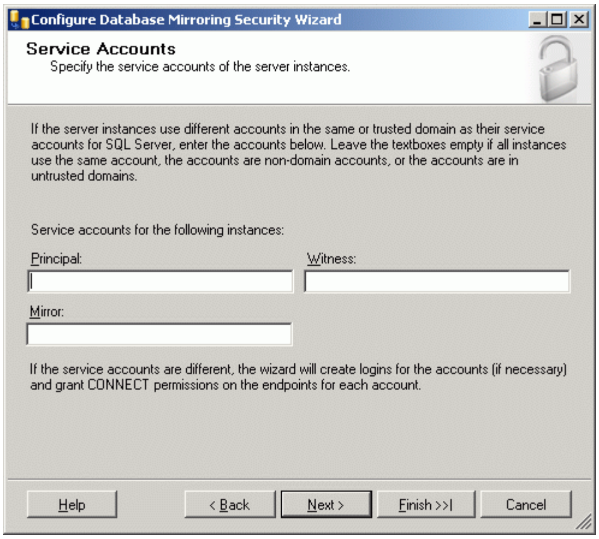
☑ Encrypt data sent through this endpoint

Endpoint name: endpoint4mirroring

NOTE: If the principal, mirror or witness are instances on the same server, their endpoints must use different ports.

Click on **Next**.

20. In the **Service Accounts** screen, you do not have to make any entries, as all three server instances run under the same account.



Configure Database Mirroring Security Wizard

Service Accounts

Specify the service accounts of the server instances.

If the server instances use different accounts in the same or trusted domain as their service accounts for SQL Server, enter the accounts below. Leave the textboxes empty if all instances use the same account, the accounts are non-domain accounts, or the accounts are in untrusted domains.

Service accounts for the following instances:

Principal:

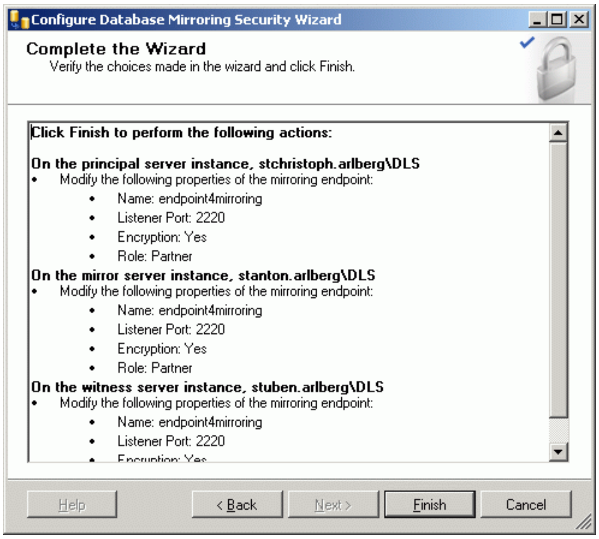
Witness:

Mirror:

If the service accounts are different, the wizard will create logins for the accounts (if necessary) and grant CONNECT permissions on the endpoints for each account.

Click on **Next**.

21. In the **Complete the Wizard** screen, you can conclude with checking the settings for the three server instances.



Configure Database Mirroring Security Wizard

Complete the Wizard

Verify the choices made in the wizard and click Finish.

Click Finish to perform the following actions:

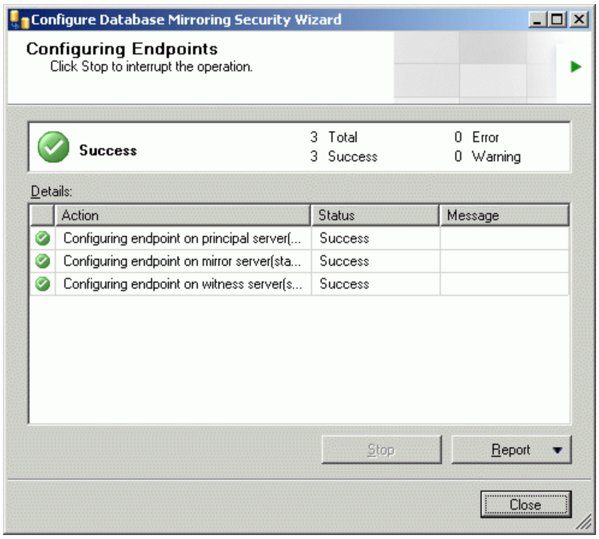
On the principal server instance, stchristoph.arlberg\DLS
- Modify the following properties of the mirroring endpoint:
  - Name: endpoint4mirroring
  - Listener Port: 2220
  - Encryption: Yes
  - Role: Partner

On the mirror server instance, stanton.arlberg\DLS
- Modify the following properties of the mirroring endpoint:
  - Name: endpoint4mirroring
  - Listener Port: 2220
  - Encryption: Yes
  - Role: Partner

On the witness server instance, stuben.arlberg\DLS
- Modify the following properties of the mirroring endpoint:
  - Name: endpoint4mirroring
  - Listener Port: 2220
  - Encryption: Yes

Click on **Finish**.

22. The screen **Configuring Endpoints** informs on the process of the configuration.



Configuring Endpoints
Click Stop to interrupt the operation.

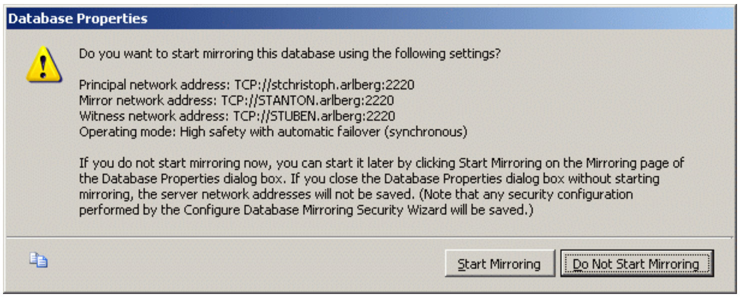
Success — 3 Total, 3 Success, 0 Error, 0 Warning

Details:

Action	Status	Message
✓ Configuring endpoint on principal server(...	Success	
✓ Configuring endpoint on mirror server(sta...	Success	
✓ Configuring endpoint on witness server(s...	Success	

When the procedure is completed, click on **Close**.

23. Start mirroring with **Start Mirroring**. The mirrored DLS database is ready for operation.



Do you want to start mirroring this database using the following settings?

Principal network address: TCP://stchristoph.arlberg:2220
Mirror network address: TCP://STANTON.arlberg:2220
Witness network address: TCP://STUBEN.arlberg:2220
Operating mode: High safety with automatic failover (synchronous)

If you do not start mirroring now, you can start it later by clicking Start Mirroring on the Mirroring page of the Database Properties dialog box. If you close the Database Properties dialog box without starting mirroring, the server network addresses will not be saved. (Note that any security configuration performed by the Configure Database Mirroring Security Wizard will be saved.)

24. In the main screen of Microsoft SQL Server Management Studio, you can monitor the database mirroring by clicking on **DLSdb** with the right hand mouse key, and selecting **Launch Database Mirroring Monitor...** in the **Tasks** submenu.

    Furthermore, it is possible to switch off the mirroring during operation. In the main screen of Microsoft SQL Server Management Studio, click **DLSdb** with the right hand mouse key. In the **Tasks** submenu, select the option **Mirroring**, and click the button **Remove Mirroring**.

    For more information about this and other possibilities, please refer to the relevant documentation for Microsoft SQL Server 2005 Enterprise Edition.

4.7 Start DLS

Before you start the DLS, please ensure that the system time is synchronous on all machines. This will be the case if the DNS server included in Windows 2003 Server is used, as the time is provided here. In case you use a workgroup instead of this DNS server, you must guarantee synchronizity by other means.

1. Start the DLS on each node.
2. Start the cluster by means of the Network Load Balancer Manager.

> ⓘ If you wish to shut down a DLS node, perhaps for maintenance purposes, first remove the machine using the Network Load Balancer Manager. Thus, it is granted that this DLS instance will not receive requests any more.

4.8 Initial Configuration

For initial DLS configuration, we recommend configuring the following areas one after the other:

1. **Change Password/Configure Account**
   Call: Main Menu > Administration > Account Management > Account Configuration
   If necessary, change the admin password that has been set during installation and configure new accounts, if necessary.

   You can find a description of the fields in Section 6.1, "Account Management".

2. **Configure FTP Server**
   Call: Main Menu > Administration > Server Configuration > FTP Server Configuration
   Enter the data for the connection to one or more FTP servers.
   You must connect to an FTP server in order to download IP phone software.
   You can find a description of the fields and additional information in Section 6.2.4, "FTP Server Configuration".

3. **Configure HTTP Server**
   Call: Main Menu > Administration > Server Configuration > HTTPS Server Configuration
   Enter the data for the connection to one or more HTTPS servers.
   OpenStage terminals can use an HTTPS server instead of an FTP server for downloading IP phone software.
   You can find a description of the fields and additional information in Section 6.2.5, "HTTPS Server Configuration".

4. **Windows Network Drive Configuration**
   Call: Main Menu > Administration > Server Configuration > Network Drive Configuration
   Enter the data for the Windows network drive.
   The specifications for the Windows network drive are needed for downloading IP client software.
   You can find a description of the fields and additional information in Section 6.2.6, "Network Drive Configuration".

5. **Settings (Logging)**
   Call: Main Menu > Administration > Display Logging Data > Activity and Error Log OR > P&P Import Protocols
   If necessary, change the information on which events should be logged and how long log data should be saved.
   You can find a description of the fields and additional information in Section 6.4, "Display Logging Data".

6. **Import Templates**
   Call: Main Menu > Profile Management > Template Overview > "Template data" Tab
   You have the option to load existing DLS templates stored in ZIP files.
   Please refer to Section 15.4, "Editing Templates" for more information on templates.

7. **Element Manager**
   Call: Main Menu > Element Manager > Element Manager Configuration
   Select the element manager type you want to configure under **Element Manager type**. For configuration options, see Section , "Element Manager".

4.9 Starting the DLS Client

4.9.1 Starting the Client

Before you start the DLS, you should have completed initial configuration (see Section 4.8, "Initial Configuration").

Start the DLS client as follows:

- On the server computer:
  - Using the Windows Start menu **Start** > **Programs** > **Deployment Service** > **DeploymentService**.
  - Using the **DeploymentService** program shortcut on the desktop.
- On the client computer:
  - By entering one of the following URLs in the Web browser:
    http://[IP address]:18080/DeploymentService/
    or
    https://[IP address]:10443/DeploymentService/ (for an encrypted connection)

You can find information on operating the DLS client from Chapter 5 onwards.

4.10 Installing Network Components

Normally, the network components that are described here are already in place. However, if any of the components have to be retrofitted, this chapter provides you with the description that you will need.

It describes the following components:

- FTP Server
- HTTPS Server
- General Information on DHCP
- DHCP Server in a Windows Environment
- DHCP Server in a Linux/Unix Environment
- Configuring the DNS Server for DLS

4.10.1 FTP Server

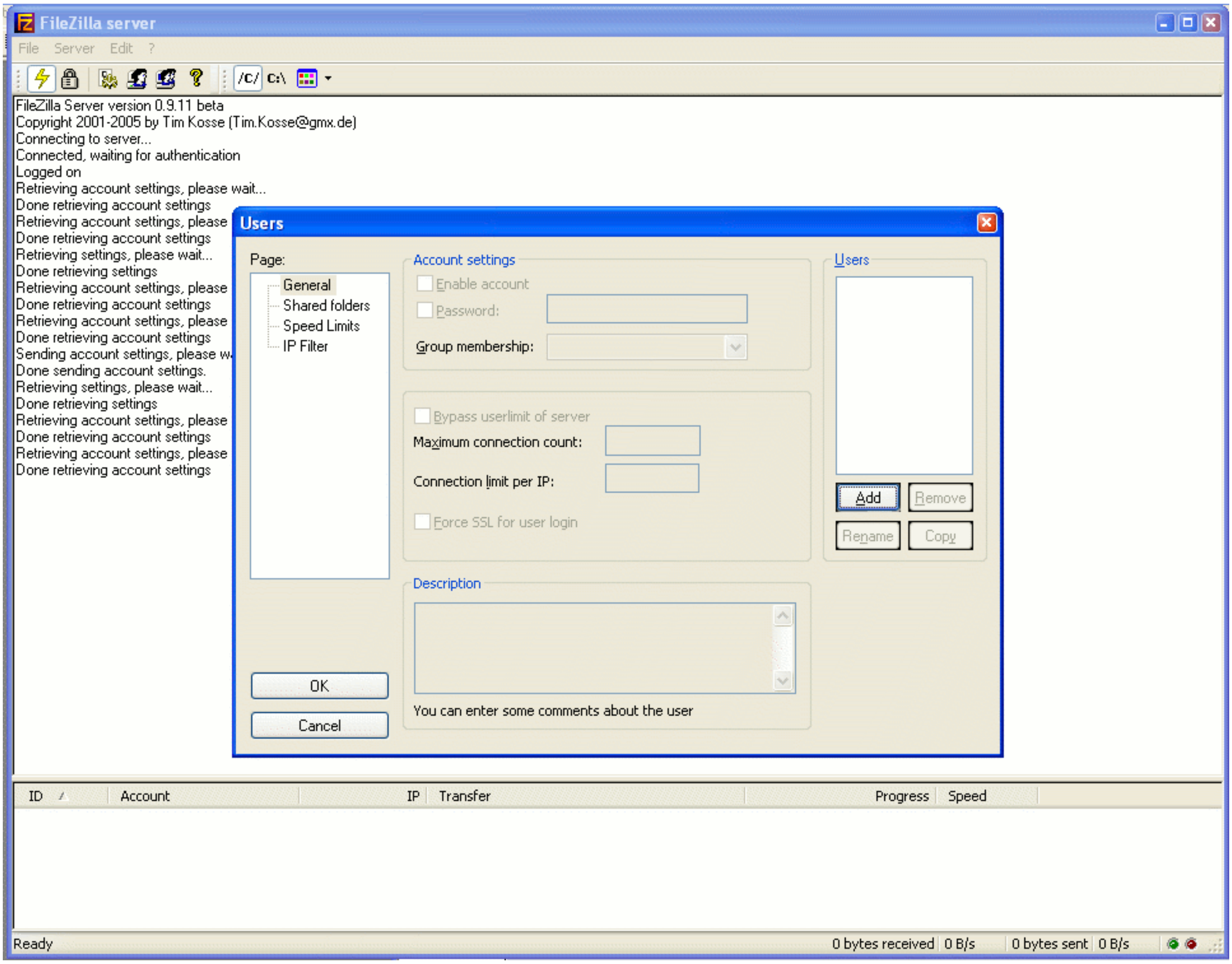
The following example shows how to configure the *FileZilla* server program.

4.10.1.1 Installation and Configuration

Install the software (*FileZilla Server* in this example, available at http://sourceforge.net/projects/filezilla/).

Start the server program.

Configure a user. To do this, select **Edit** > **Users** from the menu. Select **General** from the **Page** area. Click the **Add** button under the left section of the dialog window. An input window is displayed. Enter the user name in this window. Activate the **Enable account** option in the **Account Settings** area. If you want to assign the user a password, activate the **Password** option in the same area and enter a password.

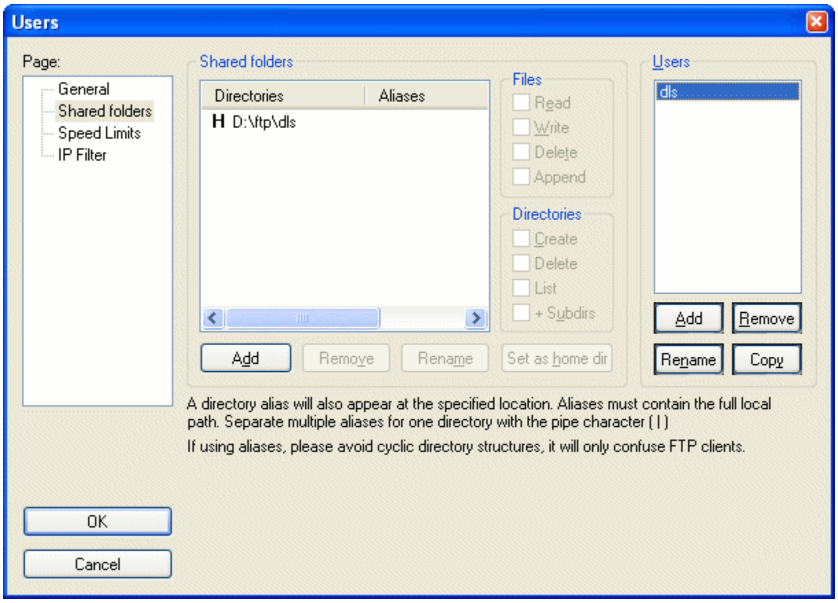


```
FileZilla Server version 0.9.11 beta
Copyright 2001-2005 by Tim Kosse (Tim.Kosse@gmx.de)
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please
Done retrieving account settings
Retrieving settings, please wait...
Done retrieving settings
Retrieving account settings, please
Done retrieving account settings
Retrieving account settings, please
Done retrieving account settings
Sending account settings, please w
Done sending account settings.
Retrieving settings, please wait...
Done retrieving settings
Retrieving account settings, please
Done retrieving account settings
Retrieving account settings, please
Done retrieving account settings
```

You can enter some comments about the user

Ready   0 bytes received 0 B/s   0 bytes sent 0 B/s

To assign the new user a directory, select **Shared Folders** in the **Page** area and click **Add**. In the subsequent window, select the directory where you want to store the software subdirectories. To assign read access to the DLS, activate the **Read** option in the **Files** area.



Directories	Aliases
H D:\ftp\dls	

Users: dls

A directory alias will also appear at the specified location. Aliases must contain the full local path. Separate multiple aliases for one directory with the pipe character (|)

If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.

Click **OK**. The FTP server is now available. Current connections are displayed in the server’s status window.

4.10.2 HTTPS Server

Terminals in the OpenStage series can download files over HTTPS. To use this option, you must install an HTTPS server. For installation help, consult the instructions supplied with the relevant software.

4.10.3 General Information on DHCP

IP phones feature a DHCP client so that the parameters required for full plug&play can be transferred via DHCP.

In addition to the standard parameters (IP address, network mask, and default router), you can configure the following options via DHCP:

- IP routing/route 1 & 2 (option 33)
- IP address of the SNTP server (option 42)
- Time zone adjustment (option 2)
- IP addresses for the primary and secondary DNS servers (option 6)
- DNS domain name for the phone (option 15)
- IP addresses for the SIP server and SIP registrar (option 120)
- Vendor-specific parameters (option 43)

In Siemens IP phones, the DLS IP address and the VLAN ID can be communicated via vendor-specific parameters.

VLAN ID assignment via DHCP works as follows on optiPoint 410/420 phones:

If the "DHCP" VLAN method is set on the phone and QoS is active on layer 2, the VLAN ID is assigned by a DHCP server. This procedure is made up of two steps. The phone starts by issuing a *discovery* message with the "OptiPoint" *vendor class* to try to obtain an IP address for a DHCP server. If the "offer" from the DHCP server contains option 43 (*vendor-specific options*) and the corresponding data, the phone saves the VLAN ID received and returns the *lease* after the DHCP server ACK. In the second step, the phone sends a tagged *discovery* message in the VLAN whose ID it received in the first step. This time, the "OptiIpPhone" vendor class is used. The subsequent *offer* may also contain option 43 with the DLS address.

If the VLAN method is set to "manual", only a lease with the "OptiIpPhone" vendor class is obtained from the phone.

4.10.4 DHCP Server in a Windows Environment

The Windows 2000 Server or Windows 2003 Server operating system contains the DHCP Server components.

This section describes how to set up and configure a new Windows 2000 DHCP server in a Windows 2000 Active Directory domain. The Windows 2000 DHCP service provides clients with IP addresses and information on the location of the particular standard gatekeeper, the DNS server, and the WINS server.

> We recommend that you use a DHCP server in the DLS environment to
> - support full plug&play and
> - ensure the authenticity of the DLS server.

4.10.4.1 Installation

You can install DHCP either during or after the original installation of Windows 2000 Server or Advanced Server. However, there must be a functioning DNS server configured in the environment. This allows active DNS forwarding via DHCP.

To check the DNS server, click **Start**, then click **Run**, enter `cmd`, press the <ENTER> key, enter ping [name displayed for the DNS server in your environment] and then press the <ENTER> key. If the query is unsuccessful, the message "Unknown host [DNS server name]" will be displayed.

To install the DHCP service on an existing Windows 2000 Server, proceed as follows:

1. In the Windows Start menu, select **Start** > **Settings** > **Control Panel**.
2. Double-click **Add/Remove Programs** and then select the option **Add/Remove Windows Components**.
3. In the **Windows Component Wizard**, click **Networking Services** under **Components** and then click **Details**.
4. Activate the **DHCP (Dynamic Host Configuration Protocol)** check box if it is not already activated, and then click **OK**.
5. In the **Windows Component Wizard**, click **Next** to start the Windows 2000 setup program.
6. Insert the Windows 2000 Advanced Server CD-ROM into the CD-ROM drive when you are prompted to do so. The setup program copies the data for the DHCP server and the DHCP tool on to your computer.
7. When setup is complete, click **Finish**.

4.10.4.2 General Configuration

After you install and start the DHCP service, you must create a scope (a range of valid IP addresses that are available for leasing to DHCP clients). Each DHCP server in your environment should have at least one scope which does not overlap with another DHCP server scope in your environment. In Windows 2000, DHCP servers must be authorized within an Active Directory domain environment in order to prevent DHCP rogue servers (outside servers set up with malicious intent) from setting up a network connection and authorizing a DHCP server.

Normally, the server is authorized when the server is first added to the DHCP console during installation and configuration of the DHCP service. If you install and configure the DHCP service on a member server or stand-alone server, however, you must configure the DHCP server.

To authorize a DHCP server, proceed as follows:

1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.

   > ℹ You must be logged on to the server with an account that is a member of the "Organization administrators" group.

2. In the DHCP console menu, select the new DHCP server. If there is a red arrow in the lower right corner of the server object, the server has not been authorized yet.
3. Right-click the server, and then click **Authorize**.
4. After a few moments, right-click the server again, and then click **Refresh**. The server should now be shown with a green arrow in the lower right corner, which indicates that the server has been authorized.

To create a new scope, proceed as follows:

1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.

   > ℹ In the console structure, select the DHCP server on which you want to create a new DHCP scope.

2. Right-click the server and then left-click **New Scope**.
3. In the scope creation wizard, click **Next** and then enter a name and description for the scope. You can choose any name but it should provide a good description of the purpose of the new scope in the network. For example, you could enter "Client addresses in the administration building".
4. Enter the address range that can be used as a lease in this scope, for example, from the starting IP address 192.168.100.1 to the end address 192.168.100.100. Because these addresses will be issued to clients, they should all be valid addresses in the network that are not currently in use. If you want to use another subnet mask, enter the new subnet mask. Click **Next**.

5. Enter all IP addresses that should be eliminated from the scope that you entered. This includes all addresses that may have already been statically assigned to different computers in your organization. Click **Next**.
6. Enter the number of days, hours, and minutes after which an IP address lease from this scope expires. This specifies the time period for which a client can hold a leased address without having to renew it. Click **Next**.
7. Select **Yes, I want to configure these options now** and then extend the wizard to add settings for the most common DHCP options. Click **Next**.
8. Enter the IP address of the standard gatekeeper that should be used by clients that have received an IP address from this scope.
9. Click **Add** to include the standard gatekeeper address in the list, and then click **Next**.

> ⓘ If there are already DNS servers in the network, enter your organization's domain name in the **Parent Domains** field. Enter the name of the DNS server and then click **Resolve** to ensure that the DHCP server can set up a connection to the DNS server and determine its address. Then click **Add** to include this server in the list of DNS servers that are assigned to the DHCP clients. Click **Next**.

10. Click **Yes, I want to activate this scope now** to activate the scope and allow clients to take leases from the scope.
11. Click **Next** and **Finish**.

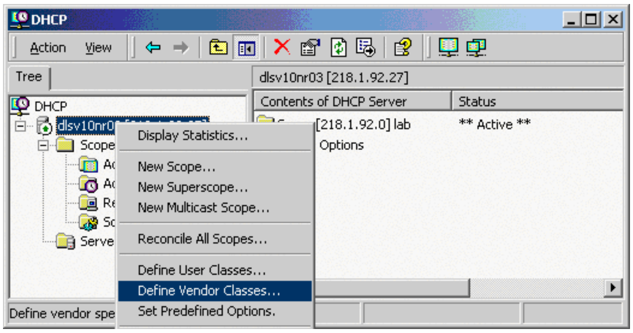
4.10.4.3 Configuring the DHCP Server for DLS

You should configure the DHCP server in such a way that when a IP Device issues an IP address query, the server automatically transmits the IP address and port number of the DLS along with the IP address and address of the DNS and default router to the IP Device. After this process, the IP Device can contact the DLS. This additional information may be provided by the DHCP server in the form of *vendor-specific information elements* (DHCP option 43) or based on *vendor classes*.

Both methods are illustrated, using examples, below.

Alternative 1: Vendor-specific information element (DHCP option 43)

1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. In the DHCP console menu, double-click the new DHCP server. Right-click **Server Options** and select **Configure Options...** in the context menu.
3. Activate the check box next to **043 Vendor Specific Info**.



4. In the **Data entry** field, enter the required vendor information.

   In our example, the vendor name and IP address are entered. The input is in hex with the following syntax.

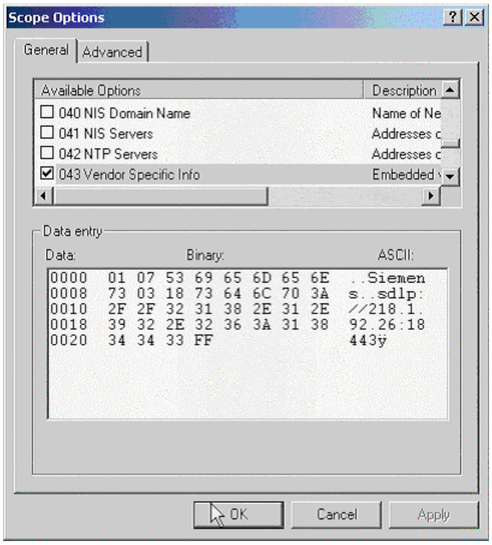
   First the vendor name:

Code	Length	Vendor name						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

Table 4-1 Vendor name as an ASCII and hex value

> For information on converting ASCII characters to hexadecimal values, see "Section 17.1, "ASCII Table (Standard)"" and "Section 17.1, "ASCII Table (Enhanced)"".

Because the vendor name is always **Siemens**, you can always enter the value **01 07 53 69 65 6D 65 6E 73**, as shown in the following dialog window.



Available Options	Description
□ 040 NIS Domain Name	Name of Ne
□ 041 NIS Servers	Addresses c
□ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded \

Data entry

Data: Binary: ASCII:

```
0000  01 07 53 69 65 6D 65 6E   ..Siemen
0008  73 03 18 73 64 6C 70 3A   s..sdlp:
0010  2F 2F 32 31 38 2E 31 2E   //218.1.
0018  39 32 2E 32 36 3A 31 38   92.26:18
0020  34 34 33 FF               443ÿ
```

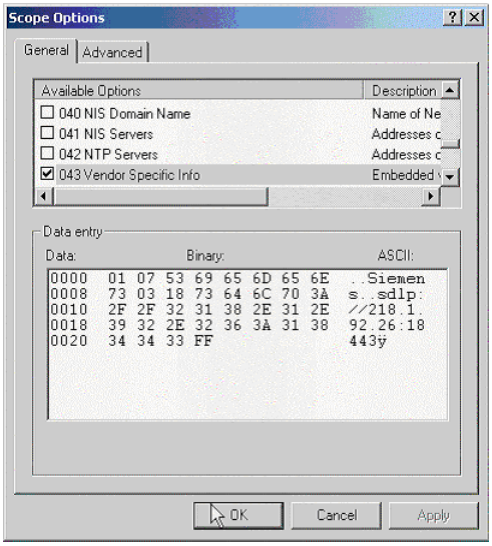
The code **01** stands for a vendor name. It is then followed by the length specification, that is, seven places (as a hex value: **07**) and finally the vendor name as a hex value.

5. In the **Data entry** field, enter the DLS IP address. As this is dependant on your configuration, the syntax given here is only an example.

Code	**Length**	**DLS IP address**																							
3	24	s	d	l	p	:	/	/	2	1	8	.	1	.	9	2	.	2	6	:	1	8	4	4	3
03	18	73	64	6C	70	3A	2F	2F	32	31	38	2E	31	2E	39	32	2E	32	36	3A	31	38	34	34	33

Table 4-2 DLS IP address as an ASCII and hex value

After the code **03** for the IP address comes the length of the IP address, which in our example is 24 characters long (in hex, this is the value **18**). This is followed by the IP address as a hex value (in the example, the address sdlp://192.168.2.19:18443).



Available Options	Description
☐ 040 NIS Domain Name	Name of Ne
☐ 041 NIS Servers	Addresses c
☐ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded

```
Data:           Binary:                   ASCII:
0000   01 07 53 69 65 6D 65 6E   ..Siemen
0008   73 03 18 73 64 6C 70 3A   s..sdlp:
0010   2F 2F 32 31 38 2E 31 2E   //218.1.
0018   39 32 2E 32 36 3A 31 38   92.26:18
0020   34 34 33 FF               443ÿ
```

Confirm the information with **OK**.

Up to three values (tags) can be stored as information.

1. Tag "001": Vendor name **Siemens** (required).
2. Tag "002": Allotted VLAN ID (only if necessary).
3. Either tag "003": When entering the DLS IP address.
   Or tag "004": When entering the DLS hostname (a DNS server must be present).

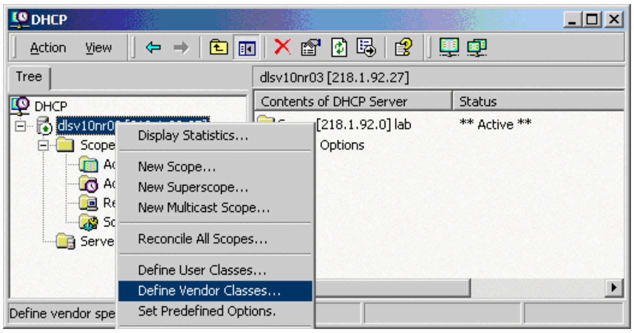
Alternative 2: Vendor class

The following example explains how to set up a new vendor class, assign options to the class, and define the scope of the new class.

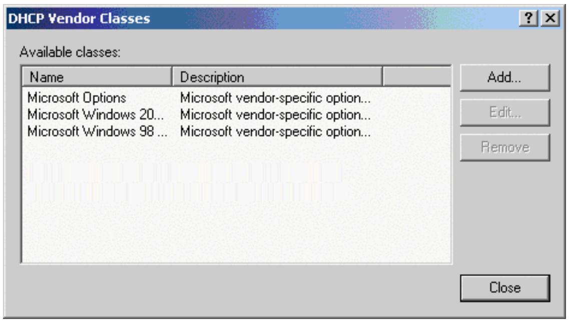
1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.

Setting up a new vendor class

2. In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.



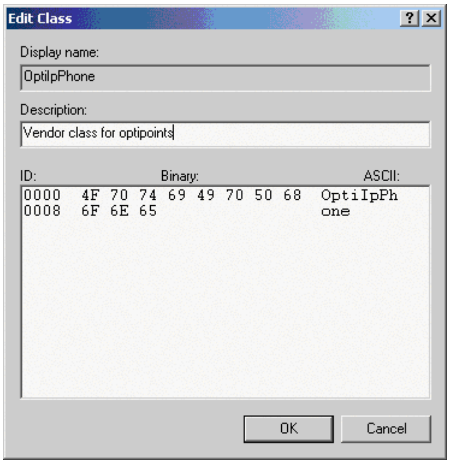
3. A dialog window opens with a list of the classes that are already available.



Name	Description
Microsoft Options	Microsoft vendor-specific option...
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...

Click **Add...** to add a new class.

4. Define a new *vendor class* with the name **OptiIpPhone** for IP phones (or **opticlient** for optiClients) and enter a description of this class.



Edit Class

Display name: OptiIpPhone

Description: Vendor class for optipoints

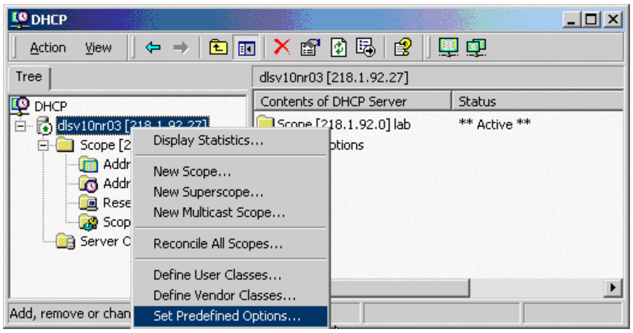
```
ID:         Binary:                   ASCII:
0000    4F 70 74 69 49 70 50 68   OptiIpPh
0008    6F 6E 65                  one
```

Click **OK** to apply the changes. The new vendor class now appears in the list.

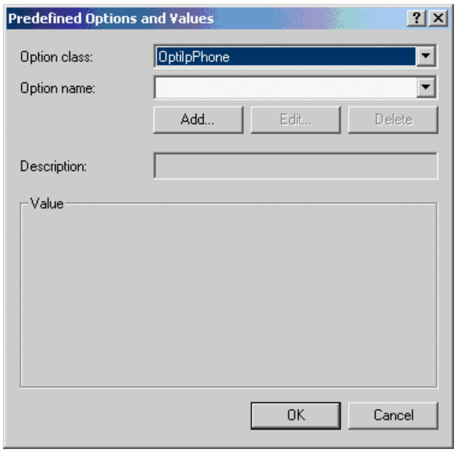
5. Exit the window with **Close**.

Adding options to the new vendor class

6. In the DHCP console, right-click the DHCP server in question and select **Set Predefined Options...** in the context menu.



7. In the dialog window, select the class that you just defined (**OptiIpPhone**) and click **Add...** to add a new option.



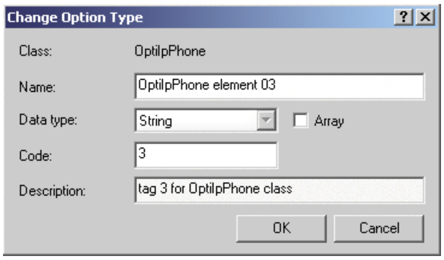
Predefined Options and Values

Option class: OptiIpPhone

Option name:

Description:

8. Enter the data for the new option.



Change Option Type

Class: OptiIpPhone

Name: OptiIpPhone element 03

Data type: String ☐ Array

Code: 3

Description: tag 3 for OptiIpPhone class

Give this option a name and select the data type in the **Data type** field according to the option to be configured:

- 01: **String**
- 02: **Long**
- 03: **String**
- 04: **String**

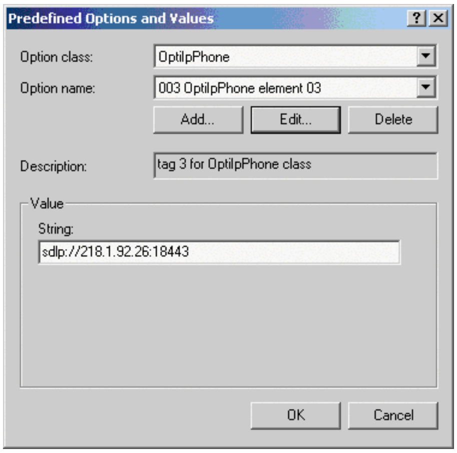
Enter the tag number corresponding to the current option in the field **Code**:

- 01: **1**
- 02: **2**
- 03: **3**
- 04: **4**

Additionally, a description description for this option should be entered in the field Description.

Click **OK** to apply the changes.

9. Enter the value for this option.



Option class: OptiIpPhone

Option name: 003 OptiIpPhone element 03

Description: tag 3 for OptiIpPhone class

String: sdlp://218.1.92.26:18443

The two options required are:

Option name	Vendor	Value
001 optiPoint Element 1	OptiIpPhone	Siemens
003 optiPoint Element 3	OptiIpPhone	sdlp://[DLS IP address]:18443

Table 4-3 DHCP options and values

If a DNS server is available, the host name of the DLS can also be entered as **004 optiPoint Element 4** instead of the DLS IP address (the DLS IP address is entered throughout the rest of the description of the example).

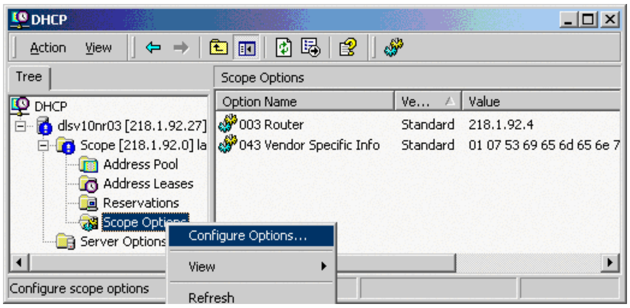
> If a VLAN is used, it is also necessary to specify a VLAN ID as tag 2.

10. Click **OK** and repeat steps 7 to 9 for each additional option.

> For DHCP servers on a Windows 2003 Server:
>
> Windows 2003 Server contains a bug that prevents you from using the DHCP console to create an option with the ID 1 for a user-defined vendor class. Instead, this entry must be created with the `netsh` tool in the command line (DOS shell).
>
> You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:
>
> ```
> netsh dhcp server add optiondef 1 "Optipoint element 001"
> STRING 0 vendor=OptiIpPhone comment="Tag 001 for Optipoint"
> ```
>
> The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.
>
> This error was corrected in Windows 2003 Server SP2.

Defining the scope for the new vendor class

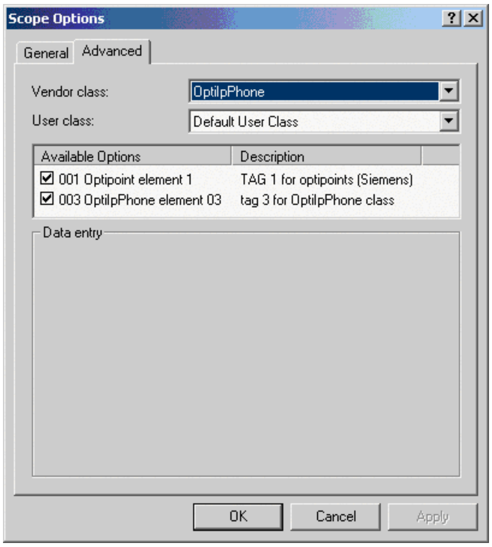
11. Select the DHCP server in question and the **Scope** and right-click **Scope Options**. Select **Configure Options...** in the context menu.



Scope Options

Option Name	Ve...	Value
003 Router	Standard	218.1.92.4
043 Vendor Specific Info	Standard	01 07 53 69 65 6d 65 6e 7

12. Select the **Advanced** tab. Under **Vendor class**, select the class that you previously defined (**OptiIpPhone**) and, under **User class**, select **Default User Class**.



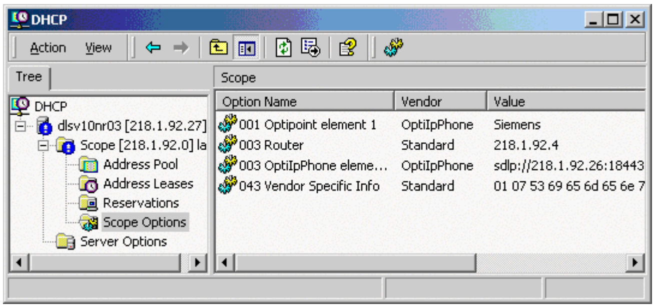
Vendor class: OptiIpPhone

User class: Default User Class

Available Options	Description
☑ 001 Optipoint element 1	TAG 1 for optipoints (Siemens)
☑ 003 OptiIpPhone element 03	tag 3 for OptiIpPhone class

Activate the check boxes for the options that you want to assign to the scope (in the example, **001** and **003**).

13. The DHCP console now shows the information that will be transmitted for the corresponding IP Devices.



Scope

Option Name	Vendor	Value
001 Optipoint element 1	OptiIpPhone	Siemens
003 Router	Standard	218.1.92.4
003 OptiIpPhone eleme...	OptiIpPhone	sdlp://218.1.92.26:18443
043 Vendor Specific Info	Standard	01 07 53 69 65 6d 65 6e 7

Information from the **Standard** vendor is transmitted to all clients while information from the **OptiIpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.

4.10.4.4 Troubleshooting

Clients cannot receive any IP address

If a DHCP client does not have a configured IP address, this normally means that the client cannot set up a connection to a DHCP server. This is due either to a network problem or to the fact that the DHCP server is not available.

If the DHCP server has been started and other clients can retrieve valid addresses, check whether the client has a valid network connection and all hardware devices associated with the client (including cables and network cards) are working properly.

The DHCP server is not available.

Frequently, the reason why a DHCP server does not provide the clients with address leases is because the DHCP service has not started correctly. If this is the case, the server may not have been authorized for operation in the network.

If you were previously able to start the DHCP server but it has stopped in the meanwhile, use the event display to examine the system log for entries that may explain the cause.

> ⓘ To restart the DHCP service, click **Start**, click **Run**, enter *cmd*, and then press the <ENTER> key. Enter *net start dhcpserver* and then press the <ENTER> key.

4.10.5 DHCP Server in a Linux/Unix Environment

This section describes how to configure vendor-specific options under Linux and Unix to enable plug&play functionality.

> We recommend that you use a DHCP server in the DLS environment to
> - support full plug&play and
> - ensure the authenticity of the DLS server.

The configuration of vendor-specific options may differ from the example shown here depending on the DHCP server used. Refer to the Linux and Unix help pages (man-pages) for more information (for example, dhcp-options and dhcpd.conf).

The options are configured in the /etc/dhcpd.conf file. You can use a text editor to modify this file. Normally, this file contains a sample configuration which you can edit to meet your individual requirements.
Please make a backup of the configuration file before making any changes.

The following configuration contains all necessary parameters:

```
Line   Contents
1      option domain-name-servers 192.168.3.2;
2      option broadcast-address 192.168.3.255;
3      option routers 192.168.3.2;
4      option subnet-mask 255.255.255.0;
5      option domain-name "DSLSUB3";
6      default-lease-time 864000;
7      max-lease-time 8640000;
8      ddns-update-style ad-hoc;
9
10     class "OptiIpPhone" {
11      option vendor-encapsulated-options
12      01:07:53:69:65:6D:65:6E:73:
13      03:19:73:64:6C:70:3A:2F:2F:31:39:32:2E:31:36:38:2E:33:2E:33:30:3A:31:38:34:34:33;
14      match if substring (option vendor-class-identifier, 0, 11) = "OptiIpPhone";
15     }
16
17     class "VLAN-discovery-OptiPoint" {
18      option vendor-encapsulated-options
19      01:07:53:69:65:6D:65:6E:73:
20      02:04:00:00:00:0A;
Line  Contents
21      match if substring (option vendor-class-identifier, 0, 9) = "OptiPoint";
22     }
23     subnet 192.168.3.0 netmask 255.255.255.0 {
24      range 192.168.3.100 192.168.3.254;
25     }
```

The instructions in lines 10 to 15 transfers DLS addresses to workpoints. Lines 12 and 13 contain two hexadecimal values consisting of:
Option - Length - Value.

The first of the two lines contains the value "Siemens". The second line contains "sdlp://192.168.3.6:18443" (DLS address).

Line 10 contains a freely selectable name and line 14 determines the vendor class to which the configuration applies.

Lines 17 to 21 contains the allocation of the VLAN ID. The VLAN ID is handed over in line 20 with the option 2, the length 4 and the value as a hexadecimal number (here 0A = 10). In contrast to the other options, the decimal VLAN ID is converted into a hexadecimal number.

> For information on converting ASCII characters to hexadecimal values, see "ASCII Table (Standard)" and "ASCII Table (Enhanced)" on page 17-2 and on page 17-3.

Restart the DHCP service once you have modified the configuration. Use the `rcdhcpd restart` or alternatively the `etc/init.d/dhcp stop` command and then `/etc/init.d/dhcp start` to do this. To check syntax, enter `rcdhcp check-syntax` via the console.

If the configuration is correct, terminals should register independently on the DLS after a restart. If the configuration is not correct, you can use a "network sniffer", for example, *Ethereal* (V 0.10.11 or higher), to locate any errors.

4.10.6 Configuring the DNS Server for DLS

> The following only describes the settings that are necessary for configuring the DNS server for DLS. For general installation and configuration, please read the documentation on the DNS server.

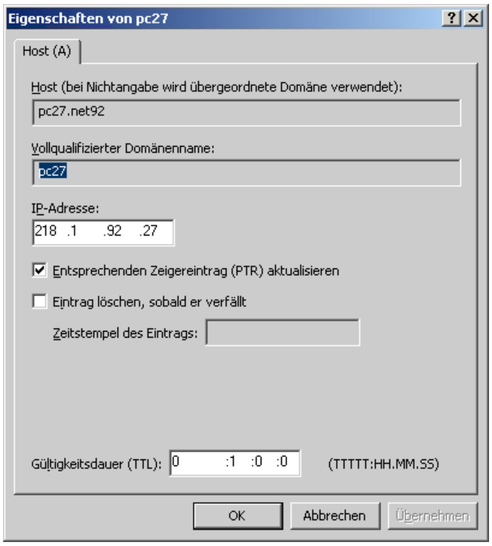
To be able to enter the DLS as a host name, there must be a DNS server with the appropriate configuration.

Example:

DLS IP address: 218.1.92.27

Requested host name: sdlp://pc27.net92:18443

For this example, you must make the following entry in the DNS server:



Eigenschaften von pc27

Host (A)

Host (bei Nichtangabe wird übergeordnete Domäne verwendet): pc27.net92

Vollqualifizierter Domänenname: pc27

IP-Adresse: 218 .1 .92 .27

☑ Entsprechenden Zeigereintrag (PTR) aktualisieren

□ Eintrag löschen, sobald er verfällt

Zeitstempel des Eintrags:

Gültigkeitsdauer (TTL): 0 :1 :0 :0 (TTTTT:HH.MM.SS)

4.11 Using pcAnywhere for Remote DLS Access

> Remote access from the Siemens Service Centers (RCC) to the DLS in the customer facility is described in the DLS Service Guideline.

The following must be observed to use pcAnywhere as a remote connection.

4.11.1 General Information

- Install an operating system with 128-bit encryption on the host computer (the computer that accepts the pcAnywhere calls).
- Make the settings described in the Siemens CERT current action plan for the host computer. Install the latest service pack (at least) on the host computer.
- Install the latest pcAnywhere patches on the host computer.
- Enable host computer access for pcAnywhere users over RLA or ReLaX only.
- Restrict access rights to host computer accounts that are permitted to use pcAnywhere.
- Set restrictive NTFS rights on all directories on the host computer.
- Change the status and the data port of pcAnywhere in the registry both on the host computer and on the remote computers:
  Change the values for **TCPIPDataPort** or **TCPIPStatusPort** in the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System** from **5631** or **5632**, for example, to **6631** or **6632**.

4.11.2 Settings on the Host Computer

Make the following settings under **Main Menu** > **File** > **Program Options** on pcANYWHERE:

- Activate logging in the Windows NT event logfile with **Use NT Event Logbook**.
- To prevent unauthorized access to the host user's network rights, activate the option **Security** in both fields and the item **Logoff user**.
- If you want the host computer to wait for another call after the restart, activate the option **Start with Windows**.
- Activate the option **NT User Rights**.
  To add remote users and use Windows NT security rights: Select the individual users or groups in the Windows NT user list. The users or groups on this list are generated and updated by the Windows NT system administrator. If you have administrator rights for Windows NT, you can add or delete users by clicking the **NT User Manager** button.
- Activate the option **Record failed connections in logbook**. Failed attempts are then entered in the pcAnywhere logbook.
- Activate the option **Case-sensitivity for password**.
- Activate the options **Restrict login attempts per call** and **Restrict login time**.

- Use **Data Encryption** during the sessions. Select symmetrical encryption (at least).
- Activate the option **Interrupt in case of Inactivity**.
- Object protection: Enter a password to protect this connection object against unauthorized use. You must re-enter the password in the **Confirm Password** field. Passwords used to protect objects are always case-sensitive.
- Activate the option **Required to display the properties**. The user is then prompted to enter a password before he can view the properties of this object.

4.11.3 Settings on the Remote Computer

> Enter the IP address of the host computer you want pcAnywhere to reach in the field **Host PC or IP address to be accessed**. If you do not make any entry here, a search is initiated on the network segment connected for a pcAnywhere host computer. This causes unnecessary network load and can lead to problems.

- Do not activate the option **Automatic login at host on connection**. Saving this information in pcAnywhere is not sufficiently secure.
- Use **Data Encryption** during the sessions. Select symmetrical encryption (at least).

4.11.4 Encryption Levels

Public key

This option offers the highest level of security and is used if a certification authority offers the CSP[1] a public key both on the host and on the remote side.

Symmetrical

This option represents the next-highest security level and is used if there is no certification authority, just a CSP available.

pcANYWHERE

This option offers minimum encryption and is used if CSP is not available. This is the only encryption level that is compatible with pcAnywhere 2.0, 5.0, and 7.x.

[1] Cryptographic Service Provider: Operating system software that provides cryptographic services compatible with Microsoft CryptoAPI. Simple CSPs are included in the scope of supply of Windows NT 4.0 and Microsoft Internet Explorer Version 3.0 and higher.

4.12 Uninstalling the Deployment Service

To completely remove a DLS installation from a computer, you must uninstall two components one after the other.

> ⚠ An uninstallation also deletes all data in the DLS database. To avoid data loss, create a backup of the database before you carry out the uninstallation (see Section 15.8, "Backup/Restore").

4.12.1 Uninstalling the DLS

1. In the Windows Start menu, select **Settings** > **Control Panel** > **Add/Remove Programs** and then click the **Deployment Service** entry in the list of installed software.
2. Click **Remove** and follow the rest of the procedure.

When the uninstallation is complete, both the DLS application and the Web server that was installed (*Tomcat*) are removed from the server PC.

> ⓘ The root directory created during DLS installation, "DeploymentService", is emptied during uninstallation, but must be deleted manually.

4.12.2 Uninstalling the SQL Server

If you want to reinstall the DLS, the installation routine will give you an option for uninstalling the existing Microsoft SQL Server 2005/2008. Otherwise you can remove it manually:

1. In the Windows Start menu, select **Settings** > **Control Panel** > **Add/Remove Programs** and click the **Microsoft SQL Server 2005/2008** entry in the list of installed software.
2. Click **Remove** and follow the rest of the procedure.

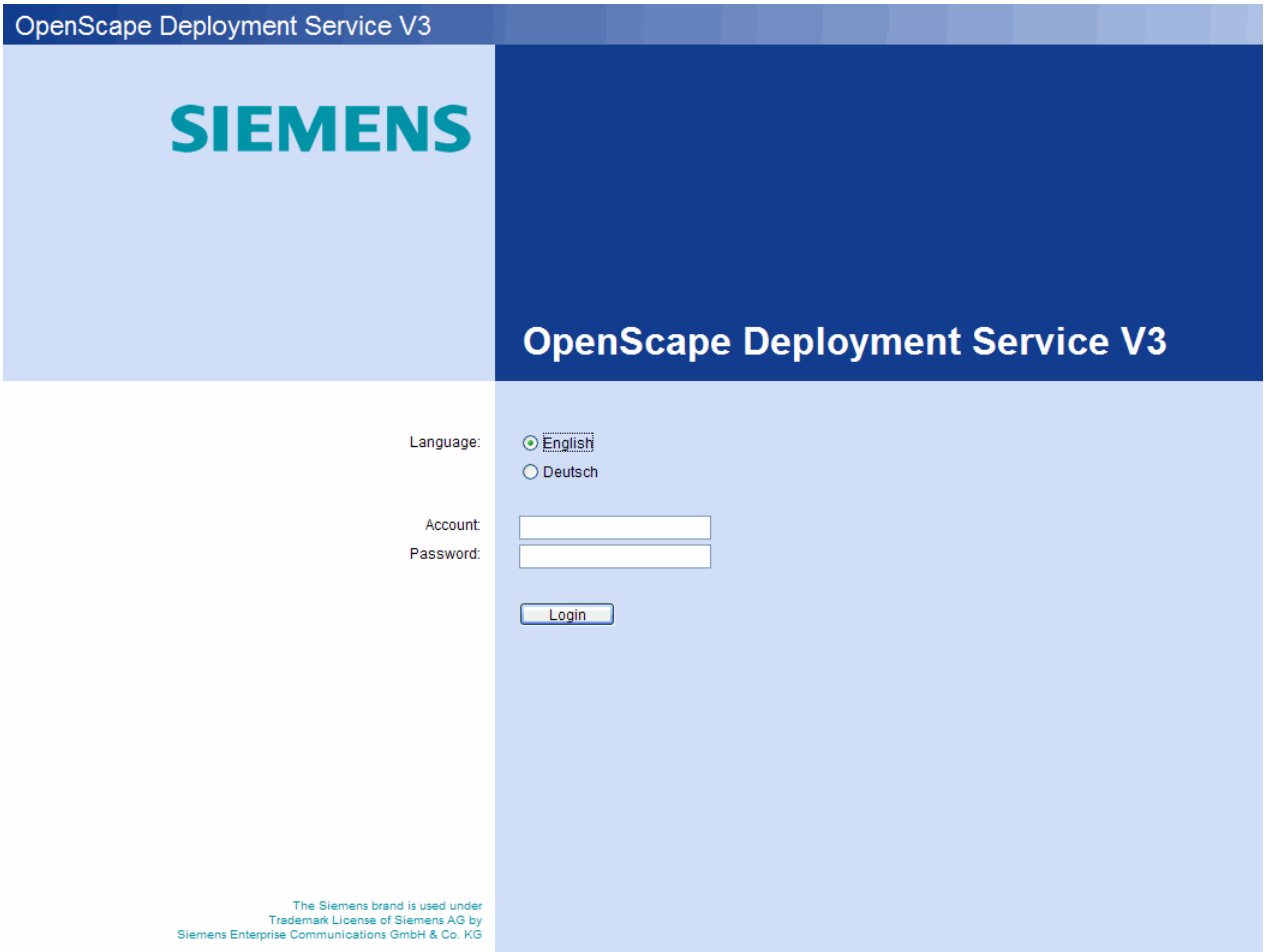
When the uninstallation is complete, the SQL database application is removed from the server PC.

5 The DLS User Interface

5.1 Starting and Logging On

1. Enter one of the following URLs in the Web browser:
   http://[IP address]:18080/DeploymentService/
   or
   https://[IP address]:10443/DeploymentService/ (for an encrypted connection)
   For [IP address], enter the IP address of the computer on which the Deployment Service is running (DLS server).

2. The Login window appears:

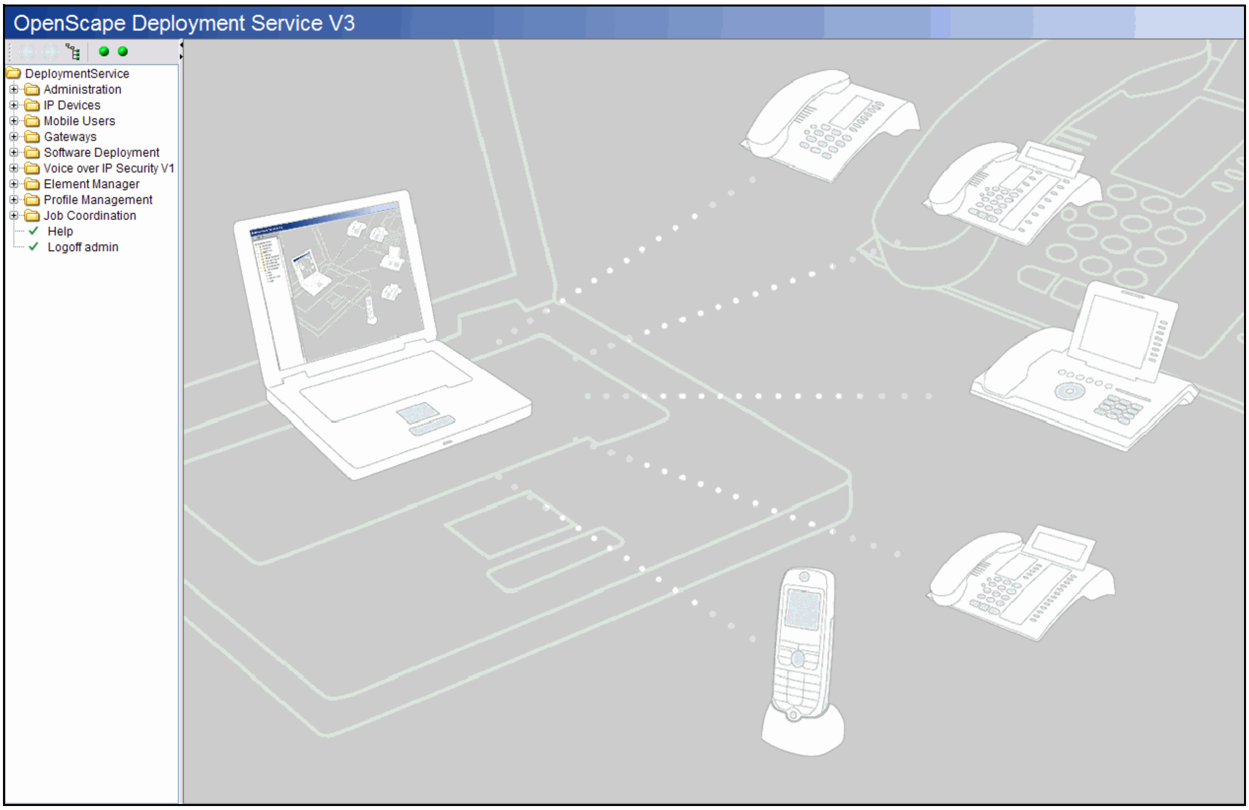

OpenScape Deployment Service V3
SIEMENS
OpenScape Deployment Service V3
Account:
Password:
Login

Language: ● English ○ Deutsch

The Siemens brand is used under Trademark License of Siemens AG by Siemens Enterprise Communications GmbH & Co. KG

Enter "admin" for **Account** and the password set during installation for **Password**. If applicable, select your language and confirm with **Login**.

3. The startup screen is displayed:



> Communication between the DLS server and **DLS client** is set up using the port number **18080** or **10443** (secured connection).
>
> Note that communication between the DLS server and **IP device** takes place over port **18443** (default mode) or **18444** (secure mode).
> For more information, refer to Section 7.6.4.4, ""DLS Connectivity" Tab".

5.2 Ending

1. In the main menu (see Section 5.4.1), select **Logoff <account>**.
2. Confirm the security prompt with **Yes**.
   The login window reappears in readiness for a new account to log on.
3. Close the browser window.

5.3 Opening the Context-Sensitive Help Function

This manual can be viewed in online help format for each DLS client interface topic (page in content area, see Section 5.4.2). For help, select the entry **Help Topics** under **Help** in the menu bar.

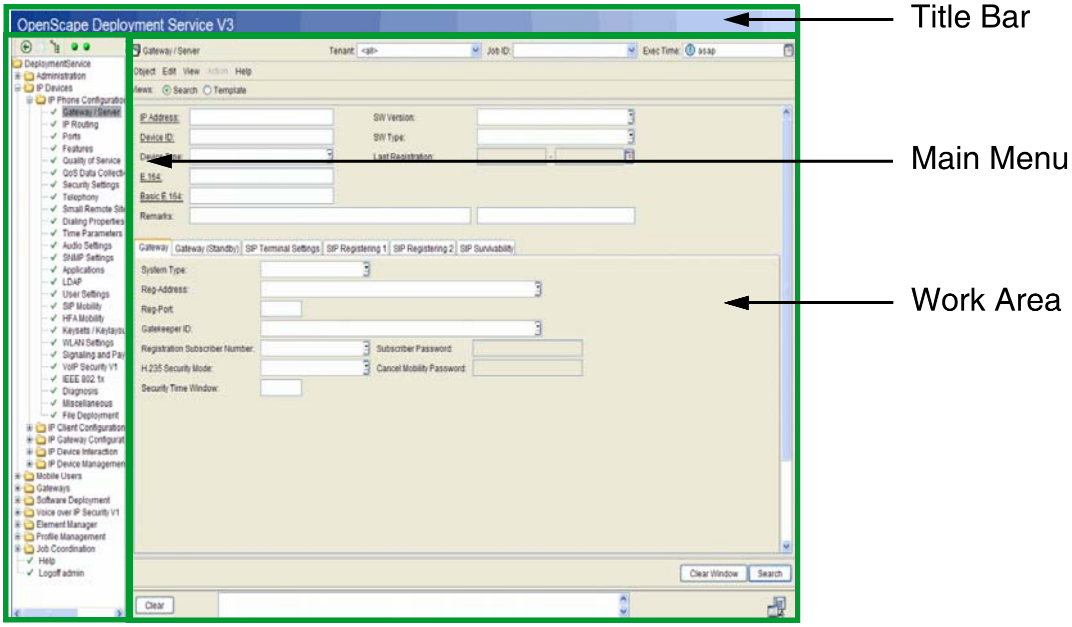
The local version of the DLS (OpenScape Deployment Service local) does not support the context sensitive help function. The general help will be opened.

You can call up help without a special topic by clicking **Help** in the main menu (see Section 5.4.1).

Help is displayed in a new browser window.

5.4 Application Interface

The application interface has three parts:

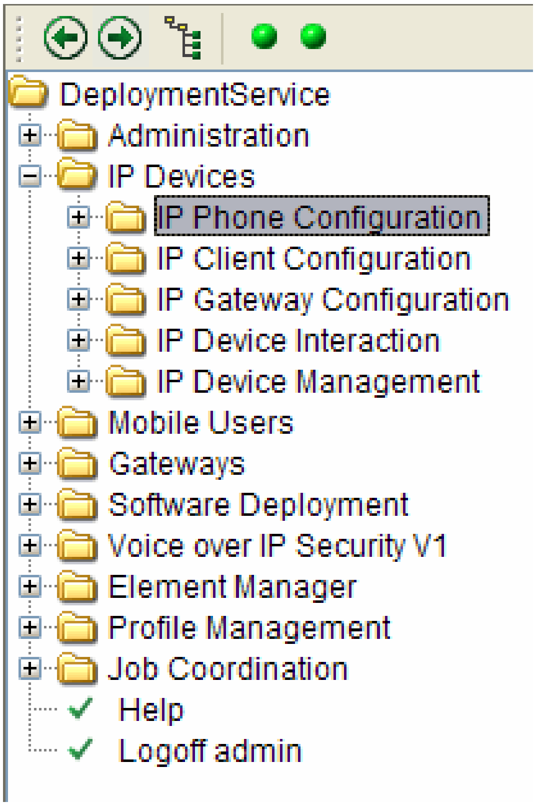


You can change the position of the division between the main menu and the working area by clicking and dragging the separator. Clicking one of the arrow icons in the upper area of the separator moves the division all the way to the right or left, so that the working area or main menu is removed from the display.

> You can also use the operating sequence in Section 15.1, "First Steps: Changing IP Device Parameters" to get to know the interface better.

5.4.1 Main Menu

The structure of this manual from Chapter 6, "Administration" onwards largely reflects the structure of this main menu.



The main menu contains the following buttons:

← → With the aid of these buttons, you can navigate between menus that have been opened before. The back button will get active as soon as a menu has been opened. The forward button will get active as soon as the back button has been clicked.

By clicking on this button, you can open and close all submenus.

🟢 🟢 The status display for current jobs is updated with every server access, but it can also be triggered via a popup menu. For this purpose, click on the status display and, in the popup menu, select **Update Status**. If a specific job shall be observed, it is recommended to reset the display by selecting **Reset Status**. Via **Show Jobs**, you can navigate to the **Job Control** menu; there, you can see details on each job. Timer controlled jobs appear in the display not till then when they are started.
The display on the left informs about running jobs. The following states are possible:
🟢 There are no running jobs.
🟡 Job running.
The display on the right informs about finished and failed jobs. The following states are possible:

🟢 Jobs have been executed without errors.
🔴 A job has failed. If the job is cancelled (see Section 14.1, "Job Control"), the display is set to green again.

You can use the structured main menu to reach all DLS components. Simply click the "+" or "-" in front of a directory symbol (or double-click the directory name) to open or close the directory. Click a contents icon to display the contents in the work area.

The contents icons may look like this:

📁 Directory with further subdirectories or pages.

✓ Page in normal mode (action completed without encountering error or not yet completed).

❗ Page where an action is currently running, for example, when scanning IP Devices.

🛑 Page with an action that ended incorrectly.

● Page not accessible due to missing account rights.

In addition, the main menu features these special functions:

✓ Help

Opens the online help.

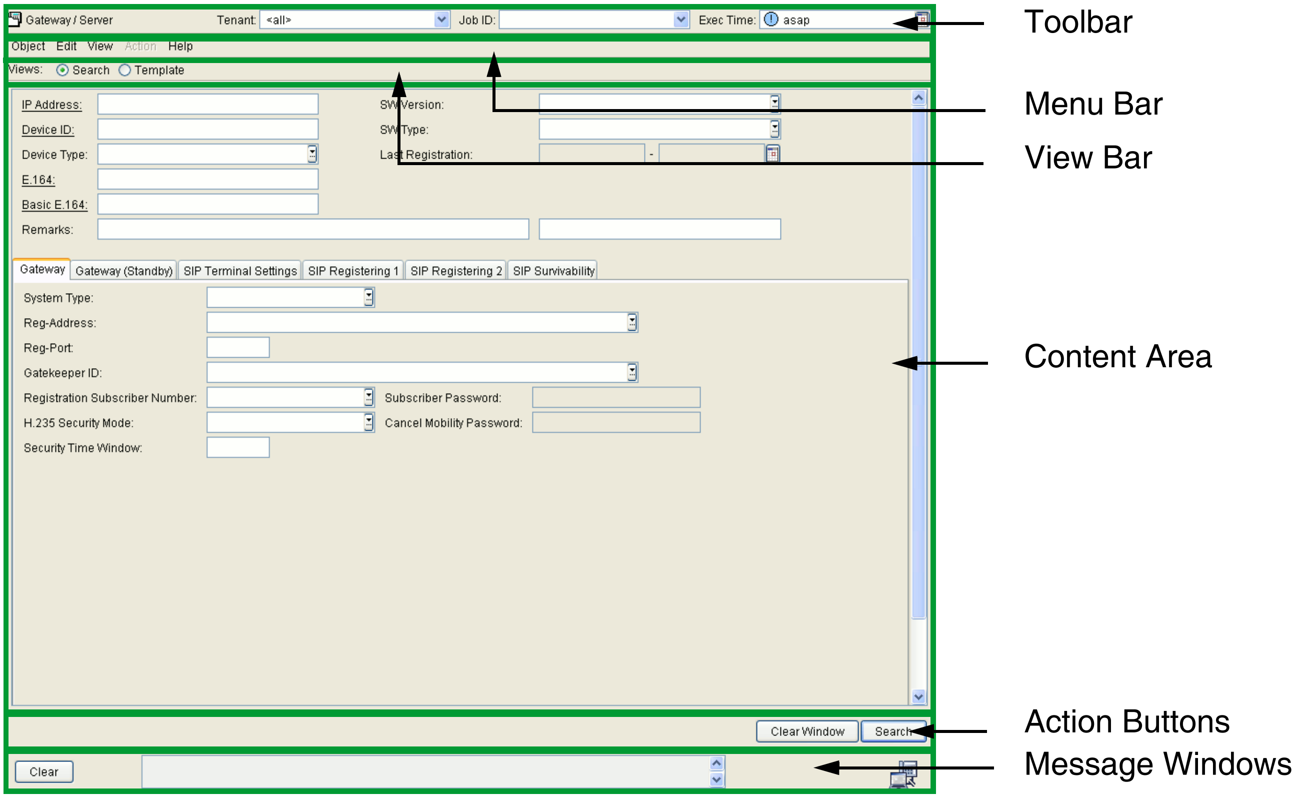
✓ Logoff <account>

Logs off the user indicated in <account>.

For information on other icons, see Section 5.4.2.4, "Icons beside entry fields".

5.4.2 Work Area

To the right of the main menu is the work area which is split up as follows:



Toolbar

Menu Bar

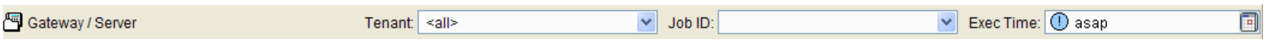
View Bar

Content Area

Action Buttons

Message Windows

5.4.2.1 Toolbar



The component currently open in the main menu is displayed on the left.

On the right hand side, elements for

- Tenants
- Job ID
- Exec Time

are displayed.

Tenant

All tenants associated with the current account are shown. Additionally, for the ’admin’ account,

- <all> = all tenants, and
- <not assigned> = tenants which are not assigned to any account,

are shown.

Job ID

A job is a combination of deployment actions that should be executed at a fixed time.

> Switching from daylight saving time to regular time (one hour back) will not lead to a second execution of a job that has been started in the time interval hereby doubled. When switching from regular time to daylight saving time (one hour advance), a job which is scheduled for this skipped time will not be executed.

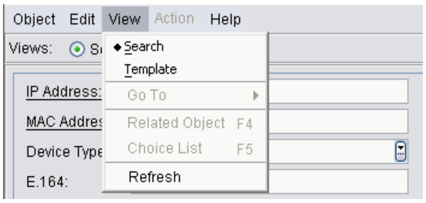
For more information, see the interface description in Chapter 14, "Job Coordination" and sequence descriptions in Section 15.7, "Using Job Coordination".

Exec Time

Specify the execution time for the job. The defaut is „asap“, that is, the job is executed immediately. By clicking on the calendar symbol ▦, you can define a point in time and conditions for job execution with the aid of a separate calendar dialog.

5.4.2.2 Menu Bar

The number of entries shown by the menu bar varies depending on the content area.



In many cases, different options are available for executing a function. Sample function: **Search**: this can be performed using the **Object** entry in the menu bar, the button of the same name, or the `<F3>` function key.

The following lists all entries that can be found in the menu bar:

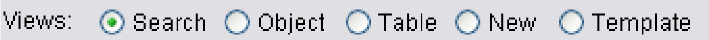
- **Object**
  - **New** (create new data record)
  - **Save** (save data record, `<F3>`)
  - **Discard** (discard changes to a data record)
  - **Delete** (delete data record)
  - **Search** (search for data record, `<F3>`)
  - **Copy** (copy data record)
  - **Paste** (insert copied data record)
- **Edit**
  - **Undo Window** (undo last change in a page of the content area)
  - **Clear Window** (delete all entries in a content area page)
  - **Undo Field** (undo last change in a field)
  - **Cut** (cut out the marked content)
  - **Copy** (copy the marked content)
  - **Paste** (insert marked content)
  - **Clear Selection** (remove marking)
  - **Select All** (mark all objects)

- **View**
  - **Search** (Search view)
  - **Object** (Object view)
  - **Table** (Table view)
  - **New** (view for creating a new object)
  - **Template** (Template view)
  - **Go To**
    - **First Object** (jump to first data record)
    - **Previous Object** (jump to previous data record)
    - **Next Object** (jump to next data record)
    - **Last Object** (jump to last data record)
  - **Related Object** (related objects, `<F4>`)
  - **Choice List** (show the selection list field,`<F5>`)
  - **Refresh** (refresh the view)
- **Action**
  - **Discard Job** (cancel the job currently running)
  - **Import File** (import job file)
  - **Export File** (export job file)
  - **Get Template** (load template data)
  - **Save As Template** (save template data)
  - **Rename Template** (change name of saved template)
  - **Delete Template** (delete saved template)
  - **Copy To Template** (copy data to template)
  - **Apply Template** (transfer template data to current view)
  - **Generate All Templates** (templates are generated for all objects or masks associated with the selected IP Device type)
  - **Save Selected Mobile User to Archive** (save mobile user data in a ZIP archive; see Section 16.13.10.2, "Saving Mobile User Data")
  - **Load Mobile User from Archive** (retrieve mobile user data from a ZIP archive; see Section 16.13.10.3, "Loading Mobile User Data")
- **Help**
  - **Help Topics** (open context-sensitive help for DLS)
  - **About...** (information on DLS)

5.4.2.3 View Bar

There are several views available for some contents.
You can select a view under the menu bar.

> You can also call up all view bar options using the **View** menu (see Section 5.4.2.2, "Menu Bar").



Views: ● Search ○ Object ○ Table ○ New ○ Template

The following lists all options available for the views:

- **Search**
  Shows a search mask in the content area for filtering individual IP Devices from the total set of registered IP Devices.
- **Object**
  Shows an individual data record for an IP Device in the content area.
- **Table**
  Shows a list of all available data records in the content area.
- **New**
  Creates a new data record.
- **Template**
  Shows a template in the content area that you can save and then use later for searches.

> If you are in the **Search** view, you can change all elements (for example, by entering values in fields or activating check boxes) in order to define the search criteria or enter data.
> In the **Template** and **New** views, only data that can be edited and saved in the DLS database is visible. All other fields are dimmed. General data from the content area cannot be saved as a template.
> Frequently, when the search result contains data from existing IP Devices (**Object** or **Table** view), some elements are uneditable and therefore also dimmed.

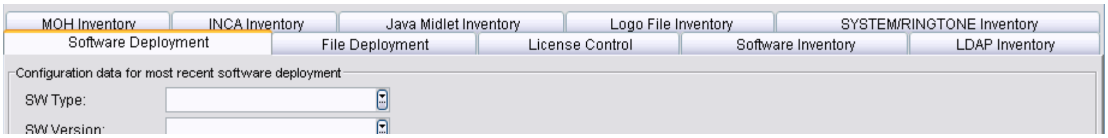
5.4.2.4 Content Area

This is where information is shown and where you can enter or select data.

> If necessary, a distinction can be made between the views available (see Section 6, "Administration") when setting element parameters in the content area (starting in Section 5.4.2.3, "View Bar").
> These settings dictate whether you can change elements or only view them.

Tabs

In the case of large content volumes, it is advisable to split the contents into individual groups. The content groups can then be selected and displayed via tabs in the content area.



Configuration data for most recent software deployment

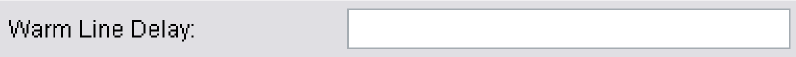
SW Type:

SW Version:

Click the tab containing the contents you want to view or edit. Information on the various tab interfaces can be found in Chapter 6, "Administration" to Chapter 14, "Job Coordination".

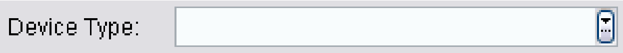
The most important control elements

- **Text field**

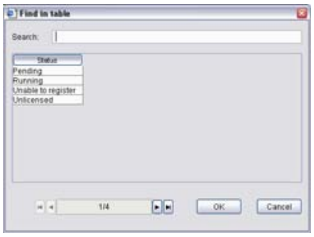
  Warm Line Delay:

  For displaying and entering freely selected alphanumerical characters.
- **Selection list field**

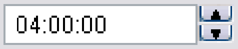
  Device Type:

  For selecting an item from a list and for entering freely selected text.
  If available, the **Find in Table** dialog opens with several entries when you click the list button at the right of the field.

Status
Pending
Running
Unable to register
Unlicensed

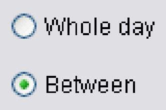
- **Choice field**

  04:00:00

  Click a value (for example, `17`) and increase or decrease the value by clicking the appropriate arrow.

- **Options**

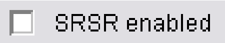
  

  ○ Whole day

  ● Between

  For selecting one of several possible options.

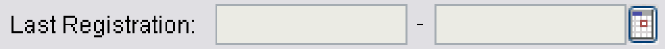
- **Check box**

  □ SRSR enabled

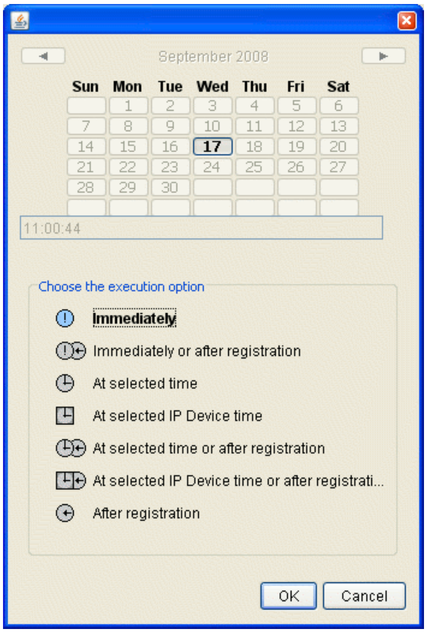
  For activating or deactivating a property. There is also a third status for a check box in the **Search** view, which is known as "undefined" (half-tone display).

- **Time field with calendar button**

  Last Registration: -

  This button provides you with a separate calendar dialog for selecting a point in time and conditions for job execution.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	**17**	18	19	20
21	22	23	24	25	26	27
28	29	30				

  11:00:44

  Choose the execution option

  - **Immediately**
  - Immediately or after registration
  - At selected time
  - At selected IP Device time
  - At selected time or after registration
  - At selected IP Device time or after registrati...
  - After registration

  The following options are available:

  - **Immediately**: The job is executed immediately. If the IP Device should be unreachable, the job will be cancelled.
  - **Immediately or after registration**: The job is executed immediately. If the IP Device should be unreachable, the job will be started anew when the IP Device is registered.
  - **At selected time**: The job is started at the point in time selected in the calender field.

  - **At selected IP Device time**: The job is started at the point in time selected in the calender field. However, here, not the system time on the DLS server is valid, but the local time in the IP Device. This option is expedient when the DLS server and the IP Devices are in separate time zones.
  - **At selected time or after registration**: The job is started at the point in time selected in the calender field. If the IP Device should be unreachable, the job will be started anew when the IP Device is registered.
  - **At selected IP Device time or after registration**: The job is started at the point in time selected in the calender field. However, here, not the system time on the DLS server is valid, but the local time in the IP Device. This option is expedient when the DLS server and the IP Devices are in separate time zones. If the IP Device should be unreachable, the job will be started anew when the IP Device is registered.
  - **After registration**: The job is executed when the IP Device is registered.

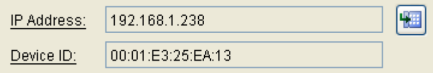
  OK accepts the value in the time field, **Cancel** closes the calendar without accepting the data.

- **Time field with calendar button and Exec Time**

> Please note that no new execution time will be calculated when the IP Device is moved to another timezone meanwhile.

- **Open WBM with a current IP address**

  If you click the browser button beside the **IP Address** field, Web-Based Management (WBM) opens for the workpoint in a new browser window with this IP address.



IP Address: 192.168.1.238

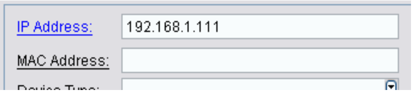
Device ID: 00:01:E3:25:EA:13

  The button is only active if the field contains an IP address. For information on how to operate the WBM, refer to the Workpoint Administration Manual.

- **More icon buttons**

  Icon buttons (for example,) appear within an object (for example, for an IP phone) when more than one entry is available or can be inserted for each object (see Section 5.4.2.4, "Multiple objects").

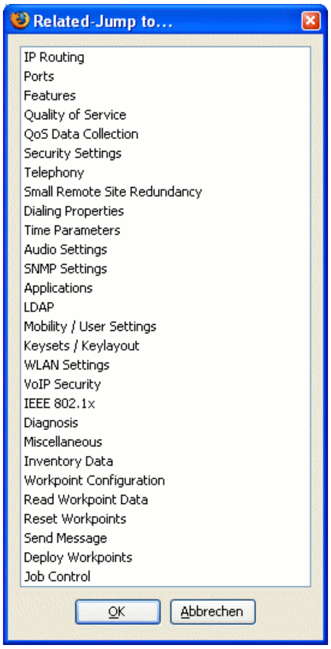
- **Search with parameter acceptance (Related Jump)**
  User-friendly interface links help you to search for the value entered for different fields, such as, **IP address** and **device ID**) in other interfaces under **IP Devices** .



IP Address: 192.168.1.111

MAC Address:

Click the underlined link (shown in blue when the mouse hovers over it).



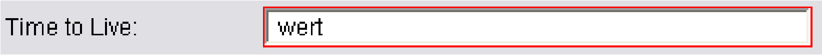
A dialog window opens with a list of all additional topics involving **IP Devices.**
Select an entry from the list and click **OK**. The display then shows the interface that you selected with the value that was transferred, and a search is performed automatically.

Entry field display

Elements that do not allow direct input are dimmed on the screen). Fields that are not relevant to the current configuration are also dimmed, for example, an SIP parameter in a HFA workpoint.

Mandatory fields are shown with a black frame.

Elements that contain an invalid value are shown with a red frame after you leave the field or when an action is executed.



Time to Live: wert

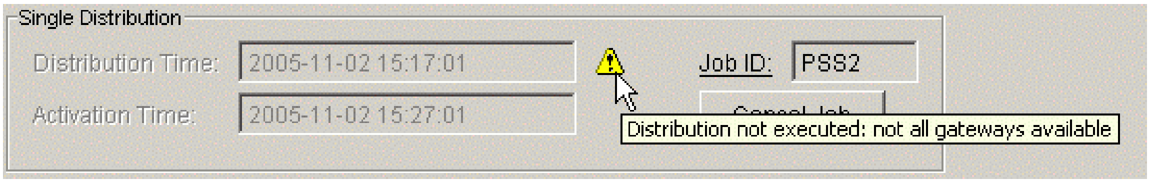
If this is the case, correct the value and perform the action again.

Often when you hover the mouse over elements, information known as "ToolTips" appears at the mouse pointer (example).

Limit of Jobs per Minute: Numeric

Icons beside entry fields

In certain instances, information or warning icons may appear next to some input fields. An explanation (or ToolTip) appears if you place the cursor over the icon. Example:



Single Distribution

Distribution Time: 2005-11-02 15:17:01

Activation Time: 2005-11-02 15:27:01

Job ID: PSS2

Distribution not executed: not all gateways available

Icon	Area	Field	Meaning
ⓘ	IP Phone Configuration IP Client Configuration	Device Type	Workpoint authentication at the DLS has failed. This may be due to an invalid authentication mode, for example. See Section 7.6.4.4, ""DLS Connectivity" Tab".
✖	IP Phone Configuration IP Client Configuration	Device ID	The IP address is assigned to another device (IP address conflict). In many cases, the DHCP server has assigned the same address twice.
⚠	IP Phone Configuration IP Client Configuration	Device Type	The device type specified is not supported.
	Key Distribution	Distribution Time	Not all gateways could be reached during key distribution. For more information on key distribution, see Section 16.11.
	Title Bar	Pending Alarms	Alarm notification for selected DLS users. For further information, see Section 6.5, "Alarm Configuration".
👥	IP Phone Configuration	E.164	The telephone is set up as a Mobility Phone, but no Mobile User is logged on. For more information on mobility, see Section 3.7, "DLS Mobility - General Information".
👥	IP Phone Configuration	E.164	A Mobile User is logged on to the IP phone. For more information on mobility, see Section 3.7, "DLS Mobility - General Information".
🔧	IP Phone Configuration	Device Type	The current configured device is not yet attached, that is, it is a virtual device.

Table 5-1 Information and warning icons in the content area

Icon	Area	Meaning
	Field	
🗑	**IP Phone Configuration** **IP Client Configuration** **IP Gateway Configuration**	The device has been deleted via API interface. If it is to be used again, it can be recovered by initiating **Read IP Device Data**.
	Device Type	
➘	**IP Phone Configuration** **IP Client Configuration**	After a restore, all devices are marked with this symbol until they have registered with the DLS again.
	Device Type	

Table 5-1 Information and warning icons in the content area

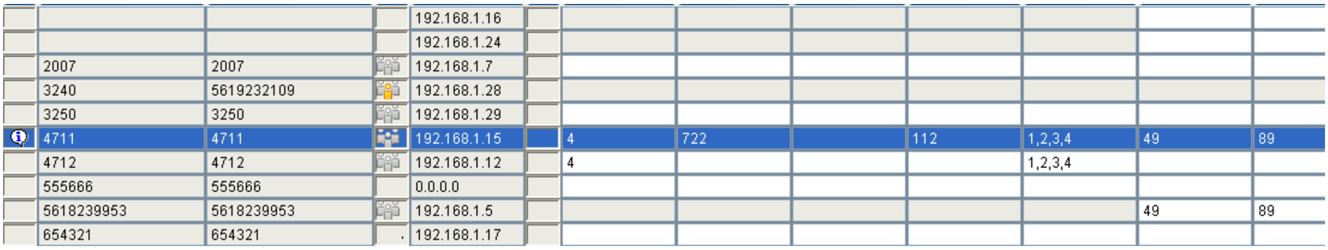
Some icons are also displayed in a separate column in Table view. This means that workpoints with particular properties (error messages) can be easily sorted and filtered out. Icons are also displayed in the main menu (Section 5.4.1, "Main Menu") and in the message window (Section 5.4.2.6, "Message Windows").

Multiple selection and data transfer in Table view

If changes were made in the **IP Devices** area, you can transfer these changes to additional devices in the search selection.

> If running a DLS client on Windows XP, check that your color scheme is set to "Default (blue)". The list display may not work properly if your color scheme is set to "Olive Green" or "Silver".
>
> Call: "Display Properties" > "Appearance" > "Color scheme".

Change to **Table** view **before** saving. The entry with the changed parameters is shown in dark blue.

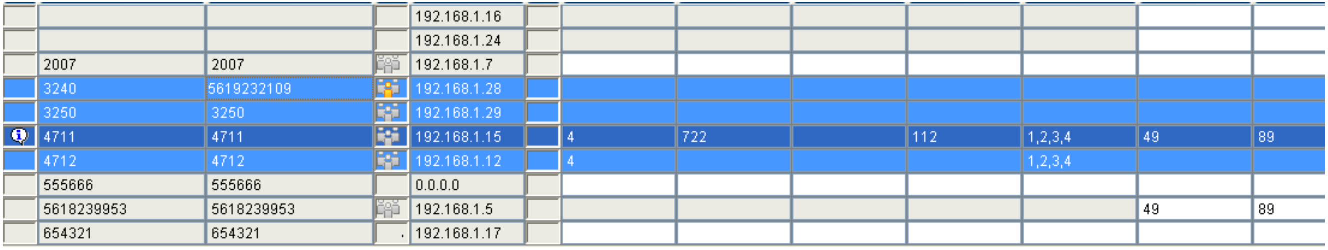


				192.168.1.16								
				192.168.1.24								
	2007	2007		192.168.1.7								
	3240	5619232109		192.168.1.28								
	3250	3250		192.168.1.29								
ⓘ	4711	4711		192.168.1.15		4	722		112	1,2,3,4	49	89
	4712	4712		192.168.1.12		4				1,2,3,4		
	555666	555666		0.0.0.0								
	5618239953	5618239953		192.168.1.5							49	89
	654321	654321	.	192.168.1.17								

Select additional IP devices to which the changes should also apply:

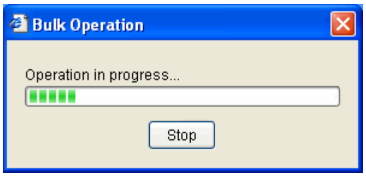
- Hold the <SHIFT> button down and click the top and bottom rows to mark all the rows in between (including the selected rows).
- Hold the <CTRL> button down and click individual entries to add or remove them from the selection.
- If you select **Edit** - **Select All** in the menu bar, you can add all selection entries.

All additional entries are shown in light blue.



				192.168.1.16								
				192.168.1.24								
	2007	2007		192.168.1.7								
	3240	5619232109		192.168.1.28								
	3250	3250		192.168.1.29								
ⓘ	4711	4711		192.168.1.15		4	722		112	1,2,3,4	49	89
	4712	4712		192.168.1.12		4				1,2,3,4		
	555666	555666		0.0.0.0								
	5618239953	5618239953		192.168.1.5							49	89
	654321	654321	.	192.168.1.17								

Click Save to apply the data.

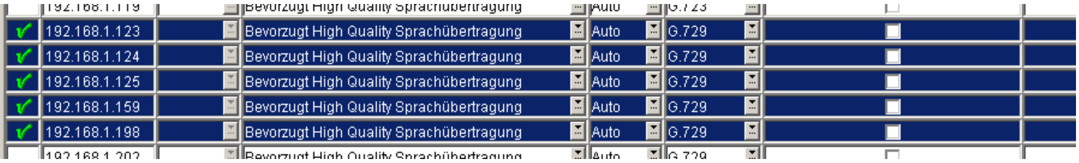


Bulk Operation

Operation in progress...

If you click **Stop**, the changes to the current workpoint are completed, but no additional data is transferred. To proceed, start the entire procedure anew.

After the data has been successfully transferred, a green check mark appears beside each updated entry. A note icon is displayed for entries where the job is not yet complete.



	192.168.1.119	Bevorzugt High Quality Sprachübertragung	Auto	G.723	□
✓	192.168.1.123	Bevorzugt High Quality Sprachübertragung	Auto	G.729	□
✓	192.168.1.124	Bevorzugt High Quality Sprachübertragung	Auto	G.729	□
✓	192.168.1.125	Bevorzugt High Quality Sprachübertragung	Auto	G.729	□
✓	192.168.1.159	Bevorzugt High Quality Sprachübertragung	Auto	G.729	□
✓	192.168.1.198	Bevorzugt High Quality Sprachübertragung	Auto	G.729	□
	192.168.1.202	Bevorzugt High Quality Sprachübertragung	Auto	G.729	□

Individual Layout of Table View

The user can accommodate the table view to his individual needs. These settings are stored user-specific in the DLS database, so that the individual settings are available to the user on each client.

To alter the order of table columns, click on the title of a column with the left mouse key and drag the column to the desired position.

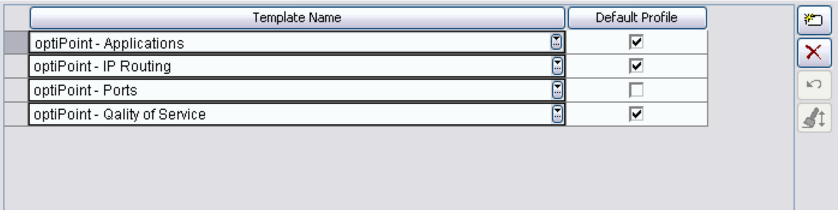
To adjust the width of a column, move the mouse pointer to one of the margins of the column title. As soon as the pointer changes to a double arrow, press the left mouse key and drag the margin to the desired position.

Furthermore, you can determine which columns are to be displayed und which columns shall have a fixed position. For this purpose, click on the column title using the right mouse key. In the context menu which is opening up now, you can define the desired settings.

> It is possible that the individual table view settings are reset on a DLS update, if objects in the database are modified during the update.

Multiple objects

Certain objects, on the other hand, allow you to create and display several different entries per object (for example, with Profile Management > Device Profile > "Templates" Tab).



Template Name	Default Profile
optiPoint - Applications	☑
optiPoint - IP Routing	☑
optiPoint - Ports	□
optiPoint - Qality of Service	☑

The buttons have the following meaning:

Inserts a new entry.

Deletes all selected entries.

Cancels the last changes to selected entries and removes a selection.

Transfers the content of the selected row (row containing the cursor) to all selected entries.

The selected row is marked in gray in the left column. This column may contain one of the following symbols:

- * (asterisk): The entry has been changed but the changes have not yet been saved.
- + (Plus): The entry has been added to but the additions have not yet been saved.
- - (Minus): The entry has been deleted but the deletion has not yet been saved.

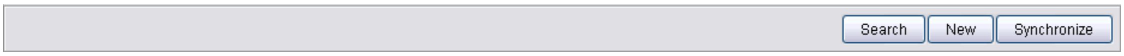
If any of these symbols is displayed, you can undo the change with ↶.

The following applies when transferring data from one row to another:

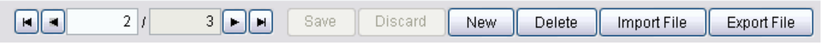
- Data is moved from the current row (the row with the cursor).
- The data is transferred to all marked rows.
- Hold the `<SHIFT>` button down and click the top and bottom rows to mark all the rows in between (including the selected rows).
- Hold the `<CTRL>` button down and click individual rows to add or remove them from the selection.
- Click the ⇅ button to transfer the data (all target rows are marked with an * (asterisk) until you save the changes).

5.4.2.5 Action Buttons

Action buttons vary depending on the content area and can be used to perform various actions.



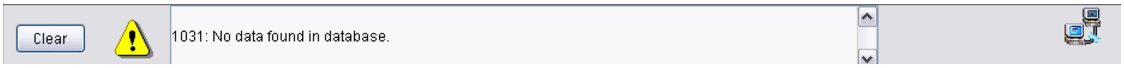
In **Object** and **Table** view, navigation buttons are shown for selecting data records. If one element is selected, the number of the selected data record is shown in the field to the left. In the window to the right, the total number of data records in the table is shown. If several elements are selected, the highest number of the selected data records is shown in the field to the left. In the field to the right, the total number of data records in the table is shown, followed by the number of selected data records in brackets.



For additional information on operating the DLS interface, refer to Section 15.1, "First Steps: Changing IP Device Parameters".

5.4.2.6 Message Windows

The message window displays status and error messages after an action is started and shows the progress of the action.



1031: No data found in database.

Messages are categorized by icons:

⚠ A warning message is shown, for example, if a search was unsuccessful.

⊗ An error message is shown, for example, if you enter an invalid value.

You can delete all messages that were output at any time with **Clear**.

A progress bar is displayed on the right for certain actions, such as, scanning IP devices.

You can change the size of the message window by clicking and dragging the separator between the message window and the remaining work area.

6 Administration

Call: Main Menu > Administration

Basic settings for operating the DLS are made in the **Administration** area.

This menu contains the following submenus:

- Account Management
- Server Configuration
- Cluster Configuration
- Display Logging Data
- Alarm Configuration
- Backup/Restore
- File Server
- Workpoint Interface Configuration
- Automatic SPE Configuration
- Automatic Certificate Deployment
- Automatic Archiving
- Automatic Upload Diagnosis- and Security Log Files
- Trace Configuration
- Server Licenses

6.1 Account Management

This area features the following components:

- Account Configuration
- Policy Settings
- Roles and Rights

For maintenance issues it is helpful to delegate tasks to multiple persons. These may obtain different accounts. For security reasons it is not wanted that each account has access to every area of the DLS. Hence, the several areas can be allowed or disallowed individually.

To each administrative function, an access right is assigned, and only accounts with this access right are allowed to call this function. In some cases, multiple functions are combined in a single right, for instance, "Key Distribution" and "Change Security Mode" are combined in the 'modify' right of the same screen 'Voice over IP Security V1'. Also, the right to create jobs comprehends the right to edit jobs, like, e. g., update the job status or reset the job.

There is no right which disallows an access explicitly.

The DLS offers a role concept. Each role groups bundles a number of rights. It is possible to define as much roles as necessary.

Some important roles are preconfigured and cannot be changed or deleted, only the default description text can be modified. These system rolesare primarily used as patterns for self-defined roles. Not each of these roles makes sense when used all by themselves.

To each account, as many roles as needed can be assigned. The resulting right is the sum of all rights of all assigned roles.

After a new installation of the DLS, an 'admin' account exists, which has all rights based on system defined roles. This account remains undeleteable and it's name remains unchangeable, and the system roles cannot be removed from it.

With an update installation from a DLS without Account Management to a DLS with Account Management, an 'admin' account with all system defined roles is created. Therefore, the admin account has all rights. To all other accounts, the INFO role is assigned. This enables them to open all screens and to search for all data, but all other functions are disabled. All other roles and rights have to be set manually.

With future DLS upgrades, new functions and new masks will be accessible by system roles only. New rights must be added to user defined roles manually. Therefore it is recommended to set rights by combination of system roles and small user defined roles, rather than copying and modifying system roles.

Example

Goal: An account shall receive editing rights (except bulk-change and create-template) for gateways only.

- Variant A: Define a new role completely based on empty rights table.
- Variant B: Define a new role based on EDIT_ONE and additionally set the 'Search' right in every relevant mask (Gateway Configuration, QoS Data Collection, VoIP Security V1).
- Variant C: Define a new role with 'Search' right for all gateway masks (Gateway Configuration, QoS Data Collection, VoIP Security V1) PLUS system role EDIT_ONE.

Only in variant C, the account automatically obtains the right to use newly added functions in the three gateway masks.

ⓘ Changes on currently used roles will take effect after next login.

6.1.1 Account Configuration

Call: Administration > Account Management > Account Configuration

Here you can configure additional accounts, change passwords, and add or remove roles to/ from existing accounts. If multi-tenancy is installed, one or more tenants can be assigned to an account.

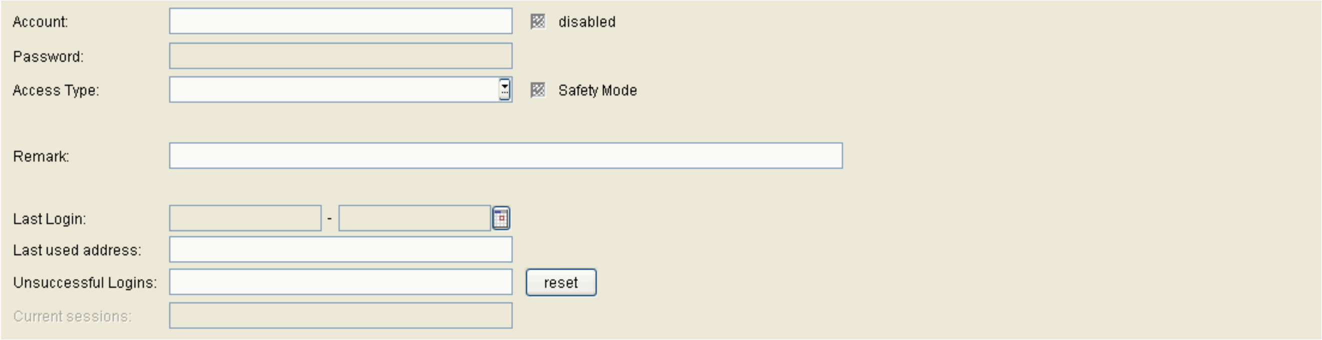
Only those accounts which have the account handling right are authorized to edit accounts, i. e. set up new accounts, or change, or delete existing ones.

If multi-tenancy is used, it is recommended to assign the account management role only to those accounts which have editing rights for **all** tenants. If an account does not have permissions for all tenants, it cannot see all tenants that have been set up. Thereby, the user of this account might try to set up a new account with a name that already exists. In such a case, an accordant error message will appear, and the account will not be set up.

This area features the following components:

- General Data
- Possible Action Buttons
- "Roles" Tab
- "Rights" Tab
- "Tenants" Tab

General Data



Account:		☒ disabled
Password:		
Access Type:		☒ Safety Mode
Remark:		
Last Login:	-	
Last used address:		
Unsuccessful Logins:		reset
Current sessions:		

Account:

Name of the account.

disabled

This checkbox is activated if this account is disabled.

Password:

New (modified) password for this account.

The password should contain at least six characters and should be non-trivial. Unsuitable entries include words that can be found in dictionaries and lexica. Ideally, you should choose a combination of numbers, special characters, and letters that do not contain a personal reference.

Access Type:

Select the allowed interfaces to the DLS server.

Possible options:

- **DLS-GUI**
  Access to the DLS server is exclusively permitted via the DLS user interface.
- **DLS API (Webservice Interface)**
  Access to the DLS server is permitted exclusively via the programming interface.

> For information on using the DLS program interface (DLS API), see Section 16.10, "Operating the DLS via the Program Interface (DlsAPI)"

Safety Mode

If this checkbox is activated, configuration changes which may cause an IP Device malfunction must be acknowledged in an additional dialog window.

Remark:

Field for general information.

Last Login

Shows the date and time of the last successful login.

Last used address

Address from which the last login (both successful and unsuccessful) was initiated.

Unsuccessful Logins

Number of unsuccessful logins since last successful login.

reset

Resets the number of unsuccessful logins in order to unlock this account.

Current Sessions

Shows the number of current sessions.

Possible Action Buttons

Search

Searches for all registered accounts that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new account.

Save

Saves the data entered/modified.

Discard

Discards any unsaved changes.

Delete

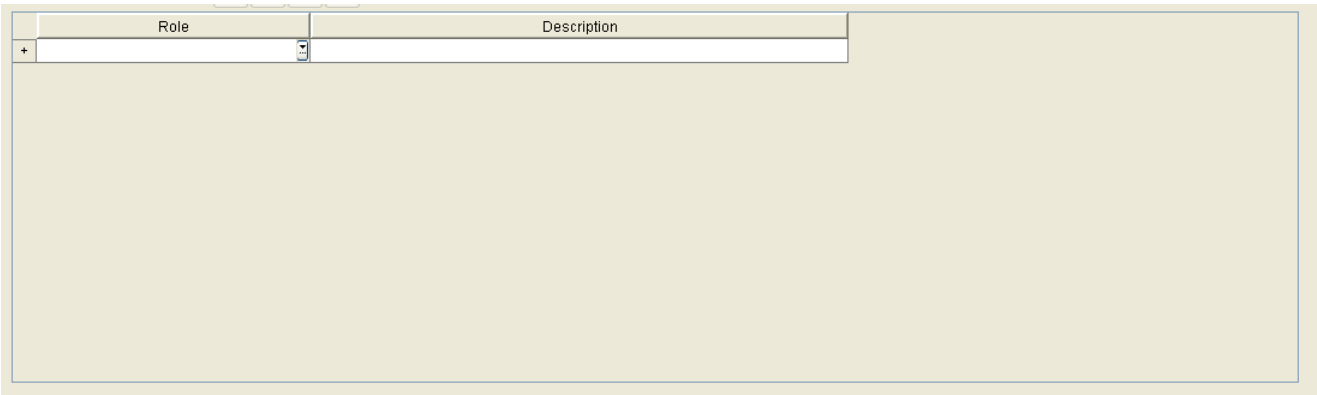
Deletes one or more accounts (multiple selections possible in Table view) except 'admin' account.

Refresh

Refreshes the content of the relevant page.

6.1.1.1 "Roles" Tab

Call: Administration > Account Management > Account Configuration > "Roles" Tab



Role

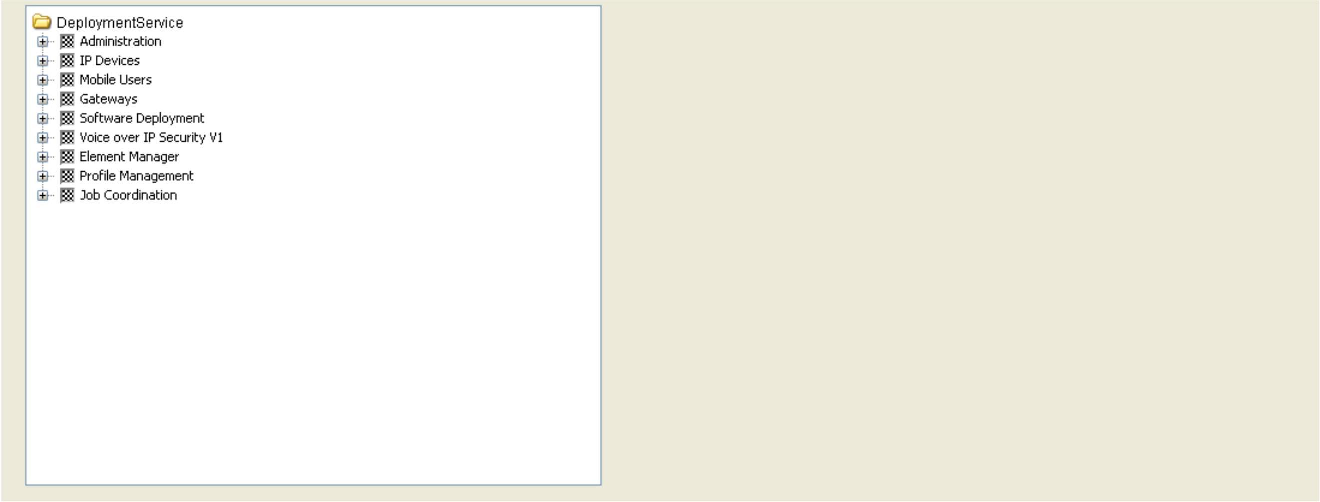
Name of roles which are assigned to this account. System defined roles cannot be removed from the 'admin' account.

Description

Detailed description of this role.

6.1.1.2 "Rights" Tab

Call: Administration > Account Management > Account Configuration > "Rights" Tab

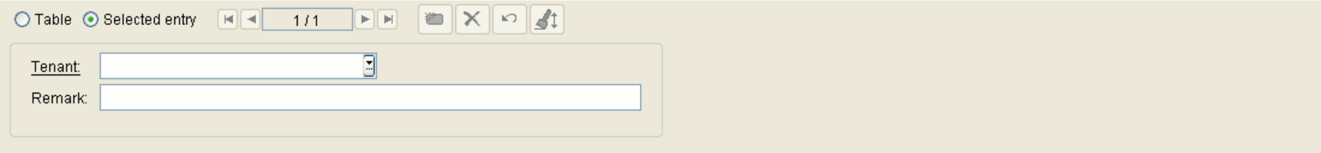


Here, the sum of all rights from the different roles is displayed for each account.

6.1.1.3 "Tenants" Tab

Call: Administration > Account Management > Account Configuration > "Tenants" Tab

> This tab is available only if the DLS multi tenancy function is installed. See chapter Section 16.16.1, "Install/Deinstall Multi-Tenancy".



Tenant:
Remark:

Tenant

Name of tenants which are assigned to this account.

Remark

Information on the tenant.

6.1.2 Policy Settings

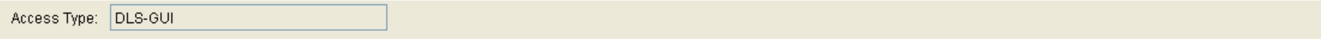
Call: Administration > Account Management > Policy Settings

In this area, the policy for the DLS users (accounts) is defined, such as length, or special character content.

This area features the following components:

- General Data
- Possible Action Buttons
- "Password Policy" Tab
- "Login Policy" Tab
- "Session Policy" Tab

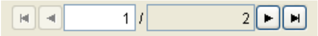
General Data



Access Type: DLS-GUI

Access Type:

Shows the interface to the DLS server that is relevant for these policy settings. To switch to another access type, use the navigation in the action button area:



Possible valuse:

- **no access**
  This user account is disabled.
- **DLS-GUI**
  Access to the DLS server is exclusively permitted via the DLS user interface.
- **DLS API (Webservice Interface)**
  Access to the DLS server is permitted exclusively via the programming interface.

> For information on using the DLS program interface (DLS API), see Section 16.10, "Operating the DLS via the Program Interface (DlsAPI)"

Possible Action Buttons

Discard

Discards any unsaved changes.

Save

Saves the data entered/modified.

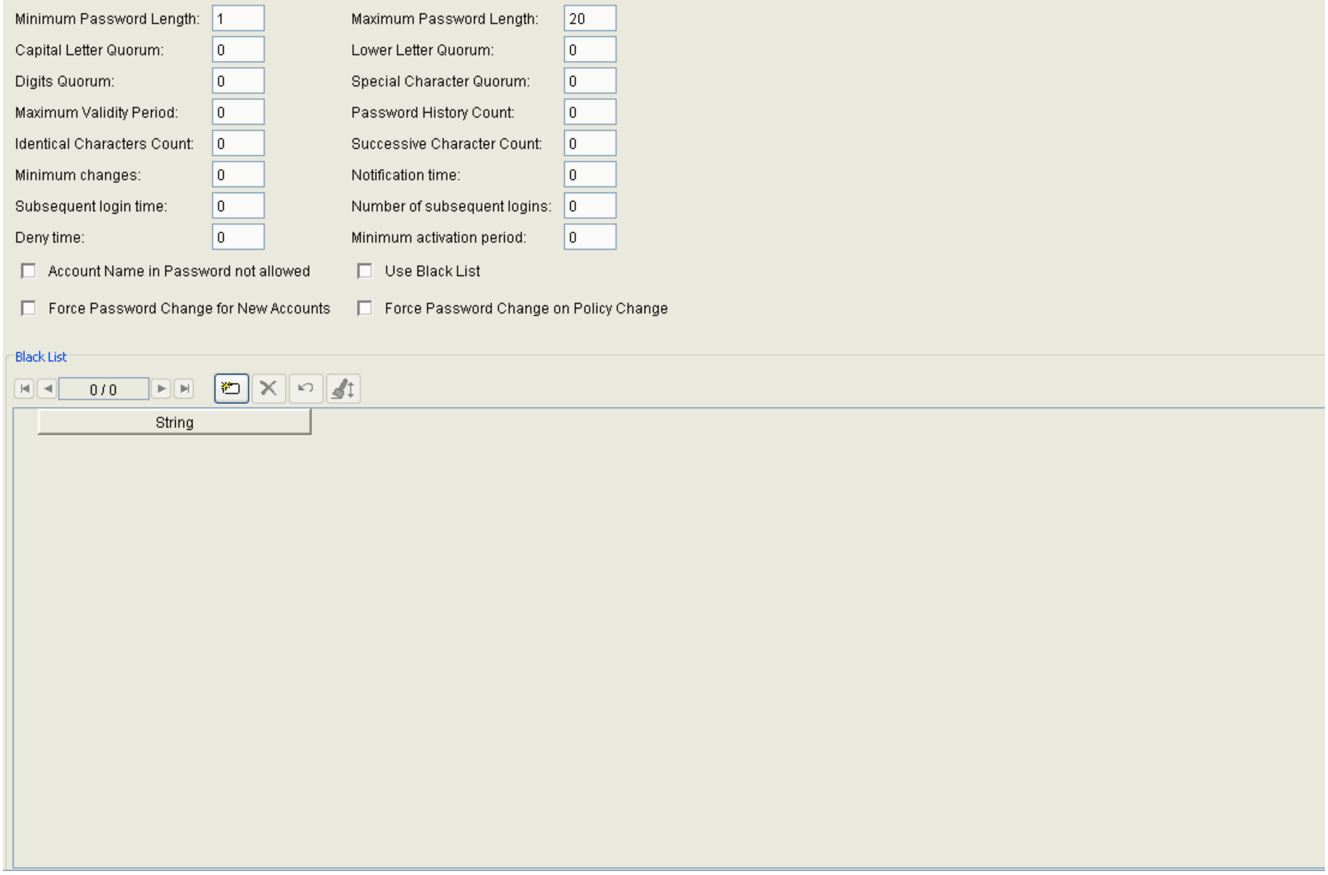
Refresh

Refreshes the content of this mask from the database.

6.1.2.1 "Password Policy" Tab

Call: Administration > Account Management > Policy Settings > "Password Policy" Tab

In this area, the password policy for the DLS user accounts is defined, such as length, or special character content.



Minimum Password Length:	1	Maximum Password Length:	20
Capital Letter Quorum:	0	Lower Letter Quorum:	0
Digits Quorum:	0	Special Character Quorum:	0
Maximum Validity Period:	0	Password History Count:	0
Identical Characters Count:	0	Successive Character Count:	0
Minimum changes:	0	Notification time:	0
Subsequent login time:	0	Number of subsequent logins:	0
Deny time:	0	Minimum activation period:	0

□ Account Name in Password not allowed   □ Use Black List

□ Force Password Change for New Accounts   □ Force Password Change on Policy Change

Minimum Password Length

Minimum password length.

Value range: **1** - **20**

Default: **1**

Maximum Password Length

Maximum password length.

Value range: **1** - **20**

Default: **20**

Capital Letter Quorum

Minimum count of capital letters in the password.

Value range: **0** - **20**

Default: **0** (= no check)

Lower Letter Quorum

Minimum count of lower case letters in the password.

Value range: **0** - **20**

Default: **0** (= no check)

Digits Quorum

Minimum count of numeric characters in the password.

Value range: **0** - **20**

Default: **0** (= no check)

Special Character Quorum

Minimum count of special characters in the password.

Value range: **0** - **20**

Default: **0** (= no check)

Maximum Validity Period

Maximum age of password in days, must be greater than the **Notification Time** value.

Value range: **0** - **180**

Default: **0** (= no check)

Password History Count

Count of stored old passwords which cannot be used again.

Value range: **0** - **10**

Default: **0** (= no check)

Identical Characters Count

Allowed length of a sequence of identical characters.

Value range: **0** - **20**

Default: **0** (= no check)

Successive Character Count

Count of ascending or descending characters in a sequence.

Value range: **0** - **20**

Default: **0** (= no check)

Minimum changes

Minimum number of characters that must be altered at password change.

Value range: **0** - **20**

Notification time

Period before password expiration within which the users are notified of a password change that will become due. Value must be less than the **Maximum Validity Period** value.

Value range: **0** - **30**

Subsequent login time

Grace period in days within which the use of an expired password may be continued.

Value range: **0** - **30**

Number of subsequent logins

Number of logins at which the use of an expired password may be continued.

Value range: **0** - **3**

Deny time

Interval in days during which a password my not be selected again as a new password by the same account.

Value range: **0** - **180**

Default: **0** (=no check)

Minimum activation period

Minimum time interval in hours that must pass before an existing password can be updated.

Value range: **0** - **168**

Account Name in Password not allowed

If this check box is set, the DLS will check whether the account name is part of the password, neither in correct nor in reversed sequence. If this is the case, the password will not be accepted. Default: no check.

Use Black List

If this check box is set, the desired password will be checked against the black list (see **String** parameter). Default: no check.

Force Password Change for New Accounts

If this check box is set, the password must be changed with the first logon of a newly registered account.

The concerning GUI user is able to login with the pre-defined password; after this, he will be prompted by a message window to change the password. Before then, all other functions are locked.

A concerning API user will not be able to logon initially. For this purpose, a GUI user with the appropriate account management rights must change the password of the API account. Default: not set (no password change required).

Force Password Change on Policy Change

If this check box is set, a password must be changed with the next logon in case it does not conform to the current password policy.

The concerning GUI account is able to login to DLS GUI with its old password; after this, he will be prompted by a message window to change the password. Before then, all other functions are locked.

A concerning API user will not be able to logon initially. For this purpose, a GUI user with the appropriate account management rights must change the password of the API account. Default: set (password change is required).

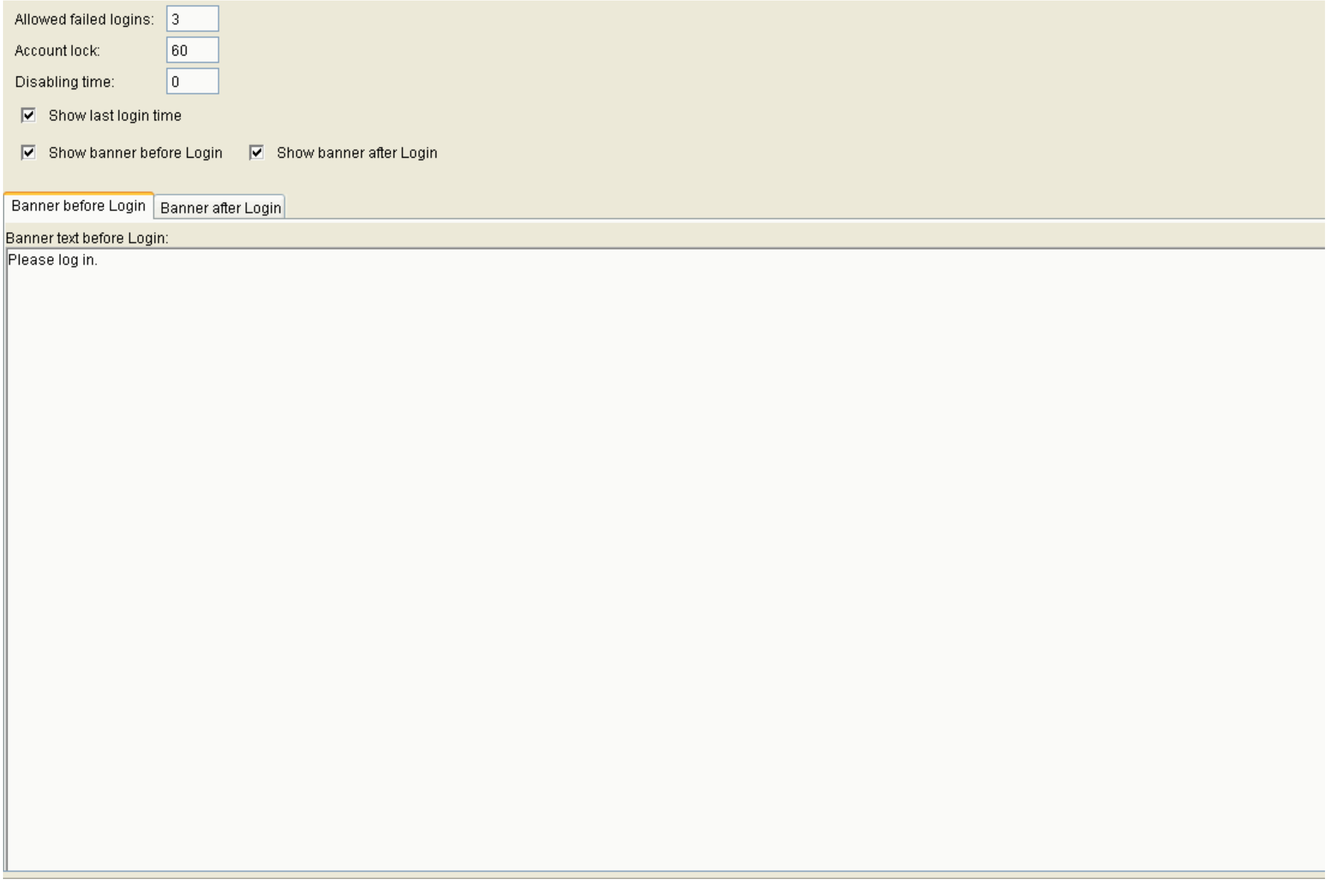
Black List

String

List of customer defined strings which may not be contained in new defined passwords (Black list). The check will be case insensitive.

6.1.2.2 "Login Policy" Tab

Call: Administration > Account Management > Policy Settings > "Login Policy" Tab



Allowed failed logins: 3

Account lock: 60

Disabling time: 0

☑ Show last login time

☑ Show banner before Login ☑ Show banner after Login

Banner text before Login:

Please log in.

Allowed failed logins

Allowed number of consecutive failed logins. When this number is exceeded, the account is locked for the time specified in **Account lock**.

Value range: **2** - **5**

Account lock

When the allowed number of failed logins (**Allowed failed logins**) has been exceeded, the account will be locked for the time span specified here.

Value range: **0** - **300**

Disabling time

When an account has not been used for the number of days specified here, it will be disabled.

Value range: **0** - **180**

Show last login time

When active, the time of the last login is shown after each successful login in a separate dialog box.

Show banner before Login

When active, the pre-login banner is shown after the DLS client has been started.

Show banner after Login

When active, the post-login banner is shown after every login.

Banner before Login

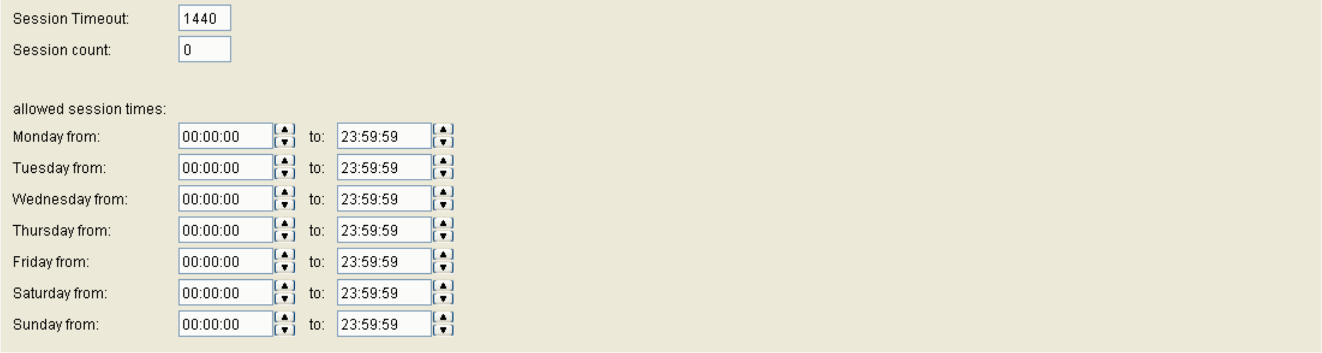
Text for the pre-login banner which is shown after DLS client startup. It is recommended to provide a bilingual text.

Banner after Login

Text for the post-login banner which is shown after every login. It is recommended to provide a bilingual text.

6.1.2.3 "Session Policy" Tab

Call: Administration > Account Management > Policy Settings > "Session Policy" Tab



Session Timeout:	1440		
Session count:	0		
allowed session times:			
Monday from:	00:00:00	to:	23:59:59
Tuesday from:	00:00:00	to:	23:59:59
Wednesday from:	00:00:00	to:	23:59:59
Thursday from:	00:00:00	to:	23:59:59
Friday from:	00:00:00	to:	23:59:59
Saturday from:	00:00:00	to:	23:59:59
Sunday from:	00:00:00	to:	23:59:59

Session Timeout

In case of inactivity, sessions will be closed after the time span specified here (in minutes).

Value range: **5** - **999999**

Default value: **1440**

Session Count

Allowed number of sessions for an account at the same time.

(**0** = no limit)

Allowed session times

Outside of these periods, no account is allowed to login, except the admin account.

Monday ... Sunday from... to

Defines start time and end time of the allowed session time periods for each day.

6.1.3 Roles and Rights

Call: Administration > Account Management > Roles and Rights

Here you can define new roles with the appropriate rights or modify existing ones. System defined roles cannot be modified or deleted.

There are some system defined default roles which cannot be modified or deleted:

Role	Rights	Weight
ACCOUNT_MGM	All existing rights for the **Account Configuration** area.	90
EDIT_BULK	All editing rights (new, delete, and edit) for all masks, except: • Roles and Rights • Account Configuration • all template activities This role is appropriate for the standard administrator. As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	60
EDIT_GENERAL_ONE	All editing rights for non system related screens without the bulk change possibility. As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	20
EDIT_ONE	Like EDIT_BULK, yet without the possibility for multiple selection.	40
EDIT_SYSTEM	All editing rights for system related screens (like Backup/Restore) except: • **Roles and Rights** • **Account Configuration** As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	30
INFO	Right to view and search data in all available masks, no editing right.	10
INFO_GENERAL	Right to view and search all non-system related screens (like Backup/Restore), no editing rights.	0
INFO_SYSTEM	Right to view and search all system related screens (like Backup/Restore), no editing rights.	5
ROLE_MGM	All existing rights for the **Roles and Rights** area.	99

Role	**Rights**	**Weight**
SECURITY_MGM	Right to handle security settings separately. During installation, all security-relevant functions are assigned to this system role; this cannot be changed. This role is assigned to the master admin account. Each account having the both roles ACCOUNT_MGM and SECURITY_MGM can assign the SECURITY_MGM to other accounts. Accounts having only one of the mentioned roles cannot assign SECURITY_MGM to other accounts. Each account having the both roles ROLE_MGM and SECURITY_MGM can assign security relevant functions to non-system roles. Accounts having only one of the mentioned roles cannot do this. Only accounts having the right to execute security relevant functions are able to see these functions in the DLS GUI.	100
TEMPLATE_MGM	Right to edit templates. Valid in all areas in which templates are available. As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	50

To be able to create roles, you need an account that contains the role ROLE_MGM. You can assign a user defined name and a random combination of rights to any new role.

As soon as a role is displayed in the **Roles and Rights** mask, you can copy it by clicking **New**, providing a new name under **Role name** and subsequently clicking on **Save**.

To add roles to accounts or remove roles from accounts, you need an account which contains the role ACCOUNT_MGM.

This area features the following components:

- General Data
- Possible Action Buttons
- "Rights" Tab
- "Policy Settings" Tab

General Data

Role name:

Name of role, to which rights will be assigned.

System defined role

Shows whether this is a system defined role. Such roles cannot be edited or deleted.

Description:

Detailed description of the role.

Displayed in object view only.

Role Weight

If at least one of the roles assigned to the account has password policy settings of its own, the settings of the role with the highest weight are valid and overwrite the equivalent global policy settings for that account. For weight values of system defined roles see the Roles-Weight-Rights table above. These values cannot be changed.

All weights of customer defined roles can be changed by those accounts which have the ROLE_MGM role. The default weight for customer defined roles is **0**.

Displayed in table view only.

Value range: **0** - **100**

Use System Policy

If activated, all specific policy settings for this role are ignored.

Displayed in table view only.

Possible Action Buttons

Search

Searches for all rights that match the search criteria.

When searching for rights, the checkboxes may have following meanings:

☑ Search for active rights.

☐ Search for inactive right.

▨ Right will not be considered when searching.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new account.

Save

Saves the data entered/modified.

Discard

Discards any unsaved changes.

Delete

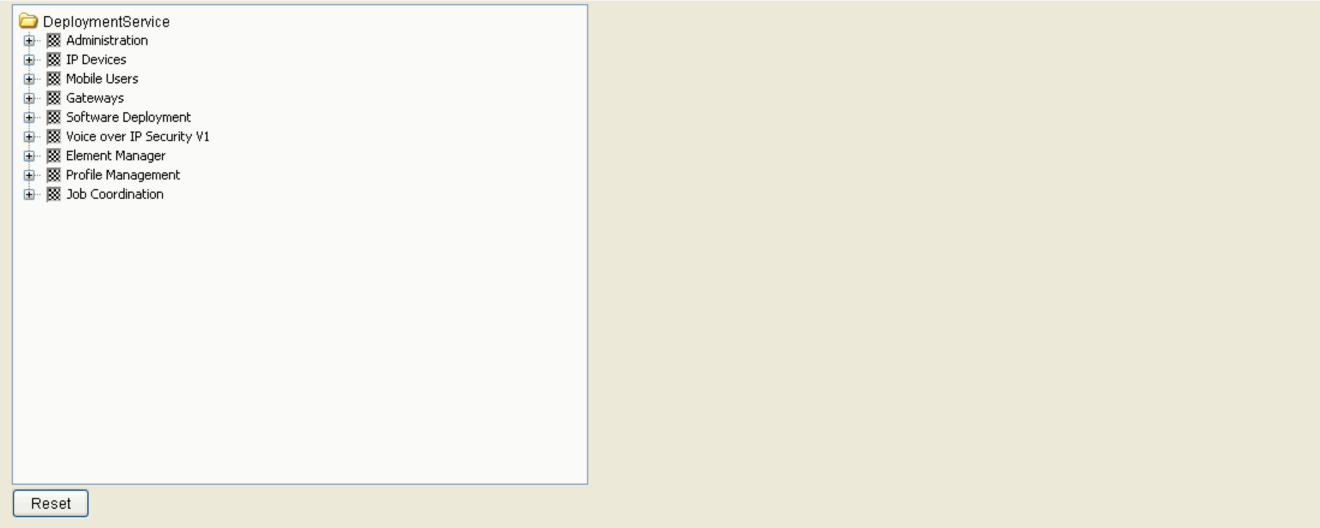
Deletes one or more rights (multiple selections possible in Table view).

Refresh

Refreshes the content of the relevant page.

6.1.3.1 "Rights" Tab

Call: Administration > Account Management > Roles and Rights > "Rights" Tab



Rights:

The rights will be defined on function level.

Possible options:

☑ Area: Right is active for this area. Submenu: Rights is active in all areas of this submenu.

☐ Area: Right is not active for this area. Submenu: Right is not active in any area of this submenu.

▣ Submenu: Right is active in at least one area of this submenu.

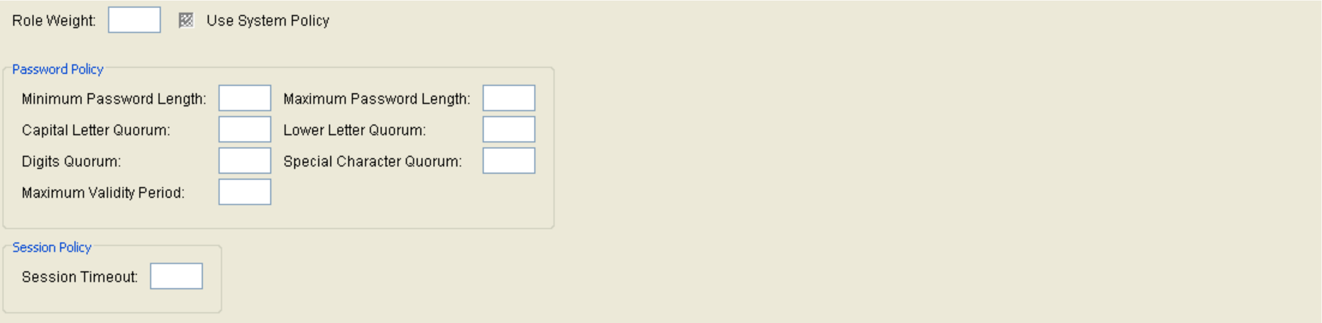
▨ Right is undefined.

Reset

Clicking this button resets all fields to inactive.

6.1.3.2 "Policy Settings" Tab

Call: Administration > Account Management > Roles and Rights > "Policy Settings" Tab



Role Weight

The extensive the rights of a role are, the higher its weight should be. Role dependent settings will be passed on to accounts.

Value range: **1** - **100**

Use System Policy

If activated, the global system policy settings will be used instead of the role specific settings.

Password Policy

Minimum Password Length

Minimum length of a valid password.

Value range: **1** - **20**

Default: **1**

Maximum Password Length

Maximum length of a valid password.

Value range: **1** - **20**

Default: **20**

Capital Letter Quorum

Number of capital letters the password must contain.

Value range: **0** - **20**

Default: **0** (= no check)

Lower Letter Quorum

Number of lower letters the password must contain.

Value range: **0** - **20**

Default: **0** (= no check)

Digits Quorum

Number of digits the password must contain.

Value range: **0** - **20**

Default: **0** (= no check)

Special Character Quorum

Number of special characters the password must contain.

Value range: **0** - **20**

Default: **0** (= no check)

Maximum Validity Period

Maximum validity period of a password in days.

Value range: **0** - **180**

Default: **0** (= no check)

Session Policy

Session Timeout

When there has been no activity for the period (in minutes) specified here, the session will be closed. If the value is 0, there will be no check.

Value range: **5** - **999999**

Default: **1440**

6.2 Server Configuration

This menu item consists of the following areas:

- Tenants
- Location
- P&P Settings
- FTP Server Configuration
- HTTPS Server Configuration
- Network Drive Configuration
- Infrastructure Policy
- API Notifications
- XML Applications
- Options

6.2.1 Tenants

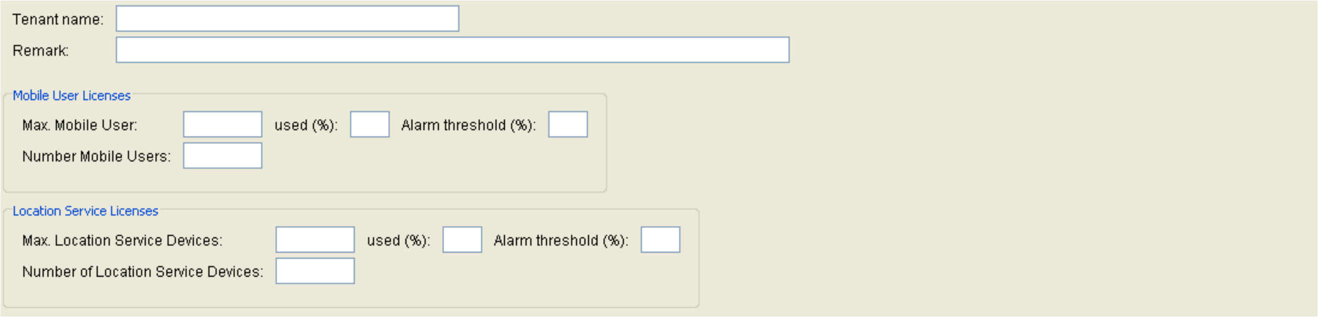
Call: Main Menu > Administration > Server Configuration > Tenants

> ⓘ This screen is visible only if multi tenancy is installed (see also Section 16.16.1, "Install/Deinstall Multi-Tenancy").

This area features the following components:

- General Data
- Possible Action Buttons
- "Locations" Tab

General Data



Tenant name:

Remark:

Mobile User Licenses

Max. Mobile User: used (%): Alarm threshold (%):

Number Mobile Users:

Location Service Licenses

Max. Location Service Devices: used (%): Alarm threshold (%):

Number of Location Service Devices:

Tenant Name

Unique name of the tenant.

Remark

Information on the tenant.

Mobile User Licenses

Max. Mobile User

Allowed maximum number of Mobile Users for this tenant.

Number of Mobile Users

Number of registered Mobile Users for this tenant.

used (%)

Indicates how many percent of existant basic device licenses are used currently.

Alarm threshold

Specify the percentage of used mobile user licenses that should generate a license alarm.

Location Service Licenses

Max. Location Service Devices

Allowed maximum number of location service devices for this tenant.

Number of Location Service Devices

Number of IP Devices supplied with IP Infrastructure data by means of Location Service.

used (%)

Indicates how many percent of existant location service licenses are used currently.

Alarm threshold (%)

Specify the percentage of used location service licenses that should generate a license alarm.

Possible Action Buttons

Search

Searches the database for configured tenants that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Thus, existing entries can be deleted in the **Search** view before new search criteria are entered.

New

Creates a new data record for a tenant.

Save

Saves the field contents to the database.

Discard

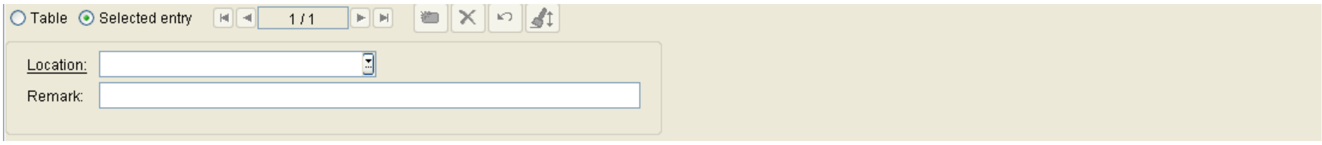
Discards any changes entered.

Refresh

Updates the window using the database.

6.2.1.1 "Locations" Tab

Call: Main Menu > Administration > Server Configuration > Tenants > "Locations" Tab



Location:
Remark:

Location

Name of the location.

Remark

Description of the location.

6.2.2 Location

The location groups devices according to common properties:

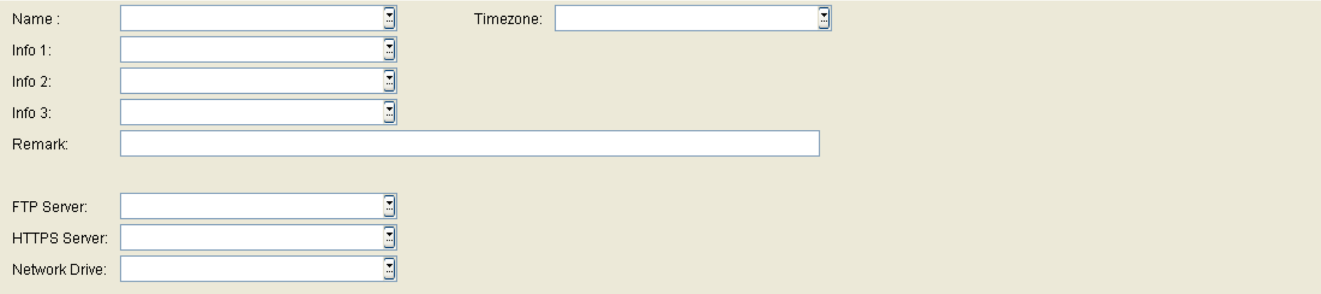
- IP address range;
- connection to a particular system/PBX;
- E.164 numbers with a specific pattern.

For each location, you can set an FTP server, time limitations in software deployment, and infrastructure policies .

This area features the following components:

- General Data
- Possible Action Buttons
- "IP Ranges" Tab
- "Reg-Addresses" Tab
- "E.164 Patterns" Tab
- "Business Groups" Tab
- "Infrastructure Policies" Tab
- "SW Deployment Restrictions" Tab
- "Certificate Deployment Restrictions" Tab
- "Tenants" Tab

General Data



Name:

Location name.

Timezone:

Defines timezone for location. For possible values, please consult the choice list.

Info 1:

Additional optional Information of location, e.g. address information.

Info 2:

Additional optional Information of location, e.g. address information.

Info 3:

Additional optional Information of location, e.g. address information.

Remark:

Remark

FTP Server:

FTP server for the location.

HTTPS Server:

HTTPS server for the location.

Network Drive:

Network drive for the location.

Possible Action Buttons

Search

Searches the database for configured locations that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new data record for a location.

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

Updates the window using the database.

Export Location

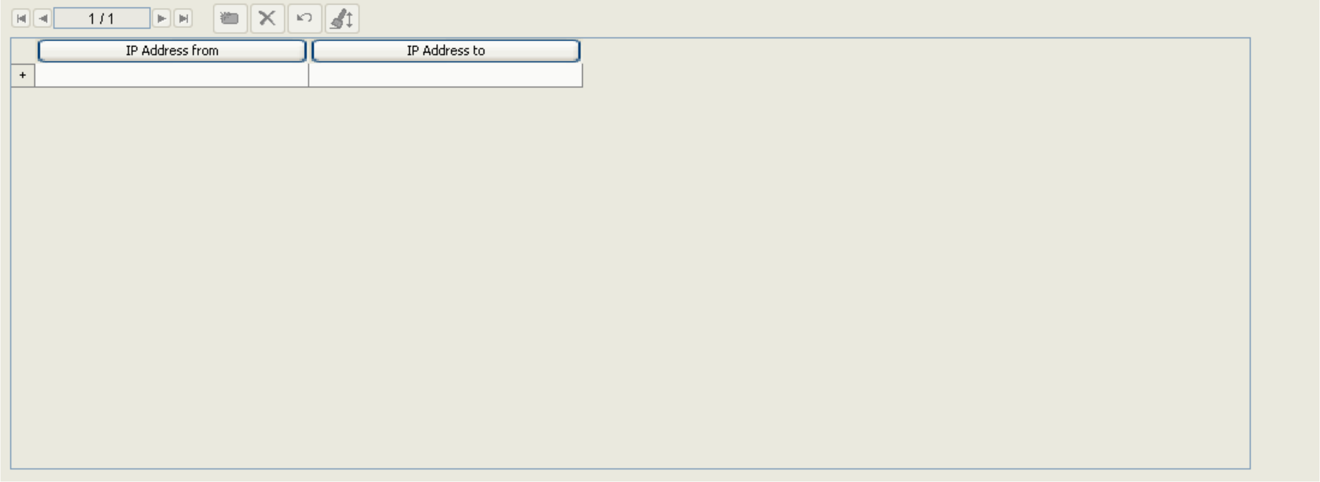
Export the selected locations to a file in zip format.

Import location

Import locations from a file in zip format.

6.2.2.1 "IP Ranges" Tab

Call: Main Menu > Administration > Server Configuration > Location > "IP Ranges" Tab



IP Address from

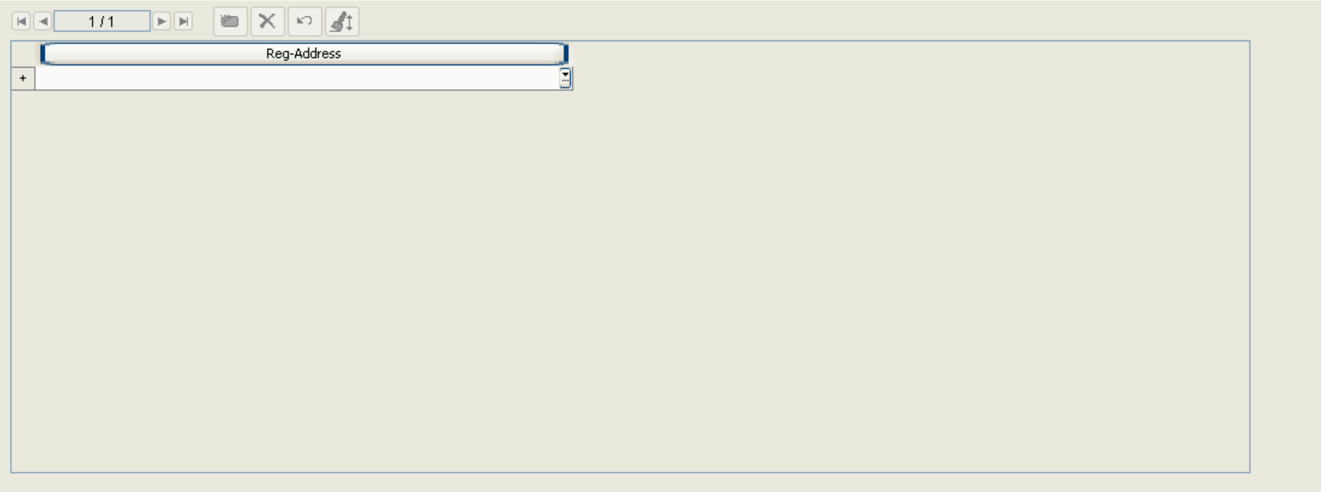
Lowest value for the IP range associated with this location.

IP Address to

Highest value for the IP range associated with this location.

6.2.2.2 "Reg-Addresses" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Reg-Addresses" Tab

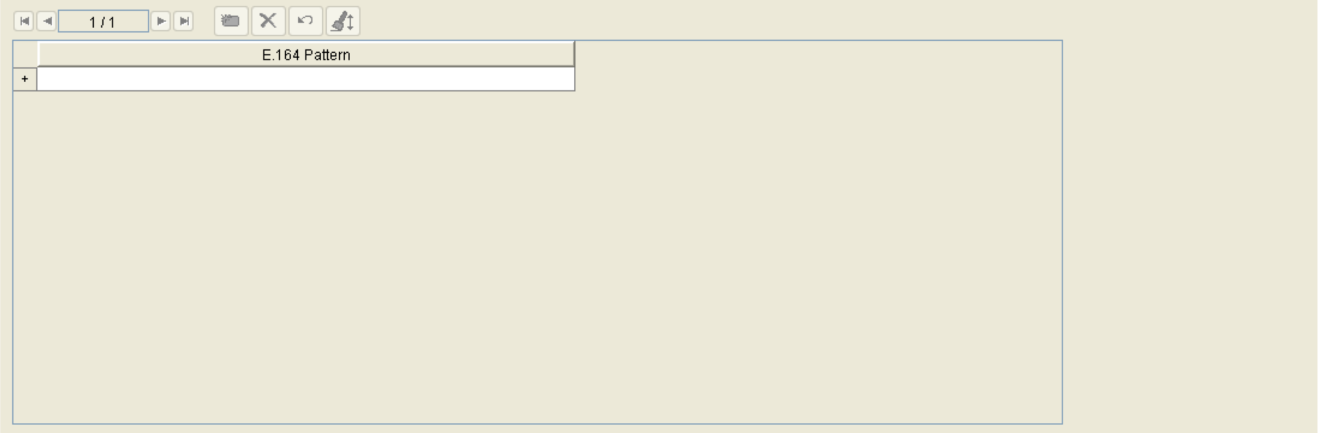


Reg-Address

IP addresses or host names of the PBX, gateway, or SIP server associated with this location.

6.2.2.3 "E.164 Patterns" Tab

Call: Main Menu > Administration > Server Configuration > Location > "E.164 Patterns" Tab



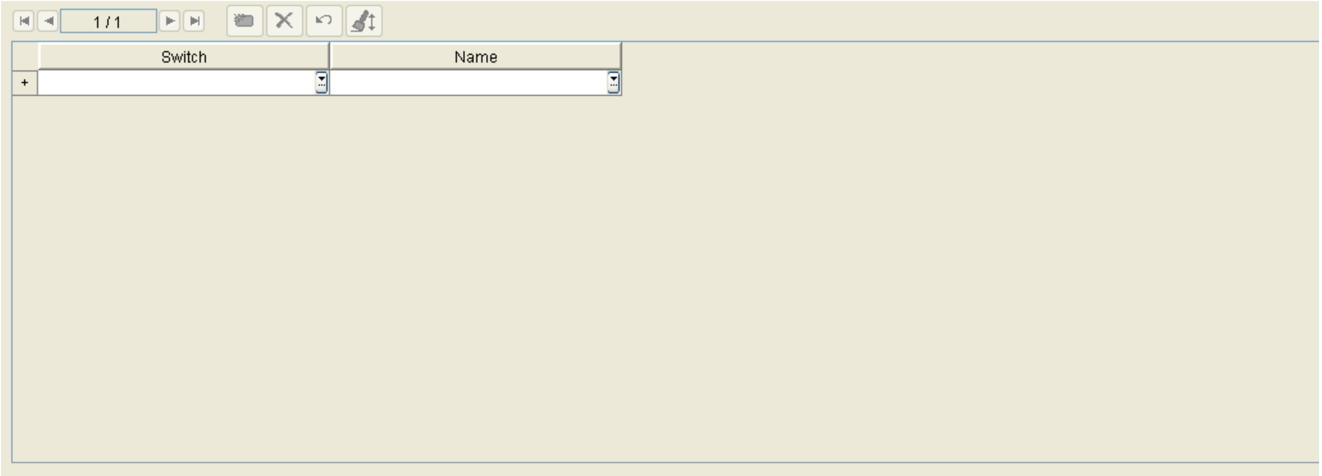
E.164 Pattern

E.164 number pattern corresponding to this location. Regular expressions with the symbol * can be used.

Example: **4989722***.

6.2.2.4 "Business Groups" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Business Groups" Tab



Switch

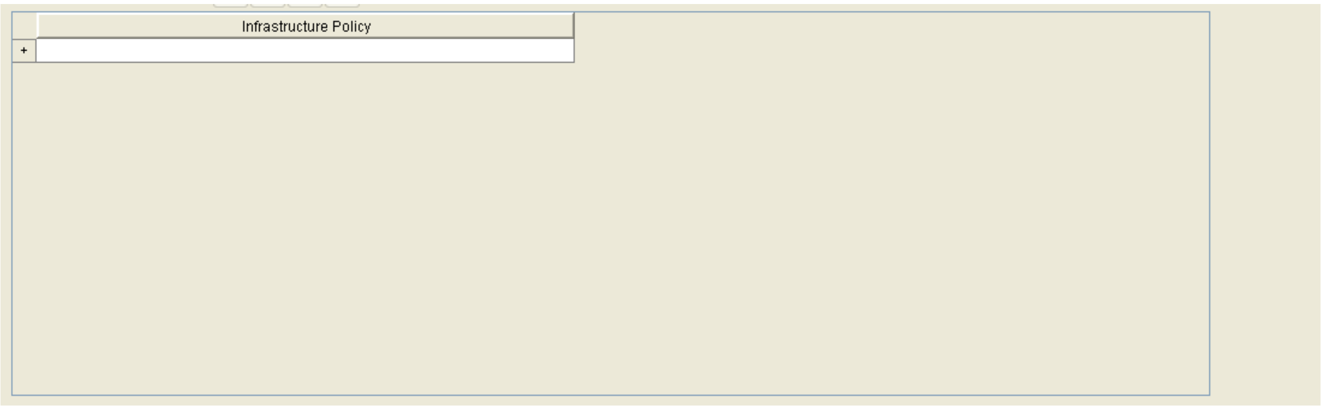
Name of the switch at which the business group is configured.

Name

Name of the business group.

6.2.2.5 "Infrastructure Policies" Tab

Call: Main Menu > Administration > Server Configuration >Infrastructure Policy > "Infrastructure Policies" Tab



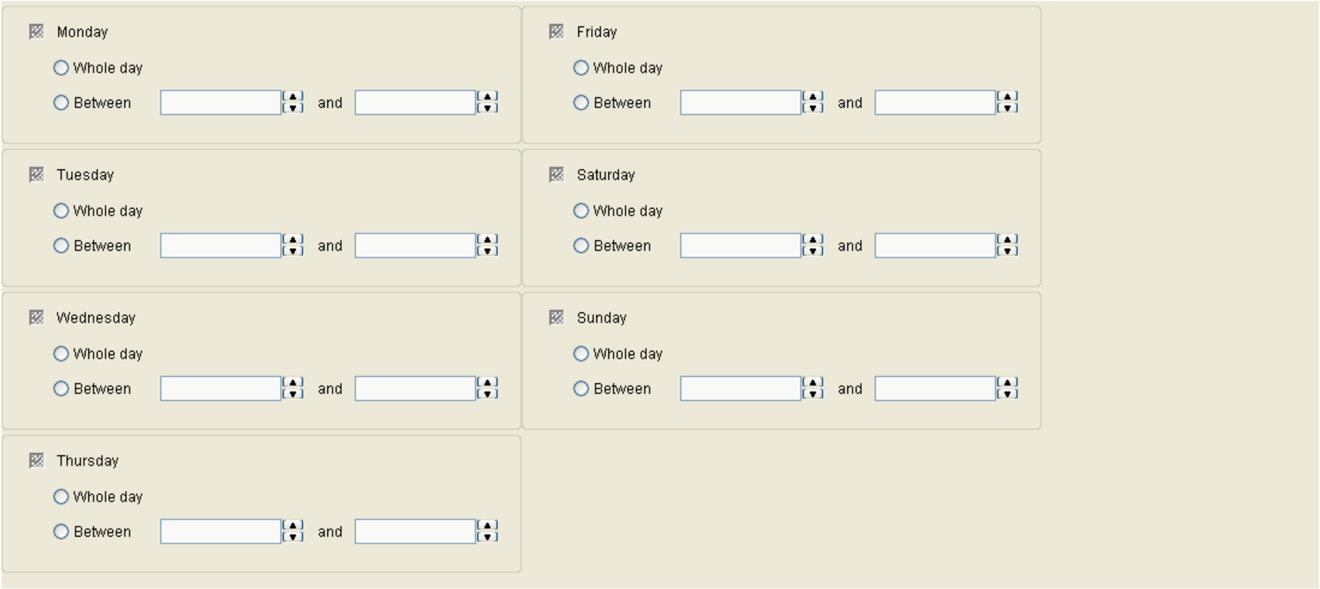
	Infrastructure Policy
+	

Infrastructure Policy

Location will be considered on infrastructure policy change for a device via DLSAPI or by means of the XML application "Location Services".

6.2.2.6 "SW Deployment Restrictions" Tab

Call: Main Menu > Administration > Server Configuration > Location > "SW Deployment Restrictions" Tab



Monday ... Sunday

Check box for specifying the weekdays on which no or only limited software deployment should be performed.

Whole day

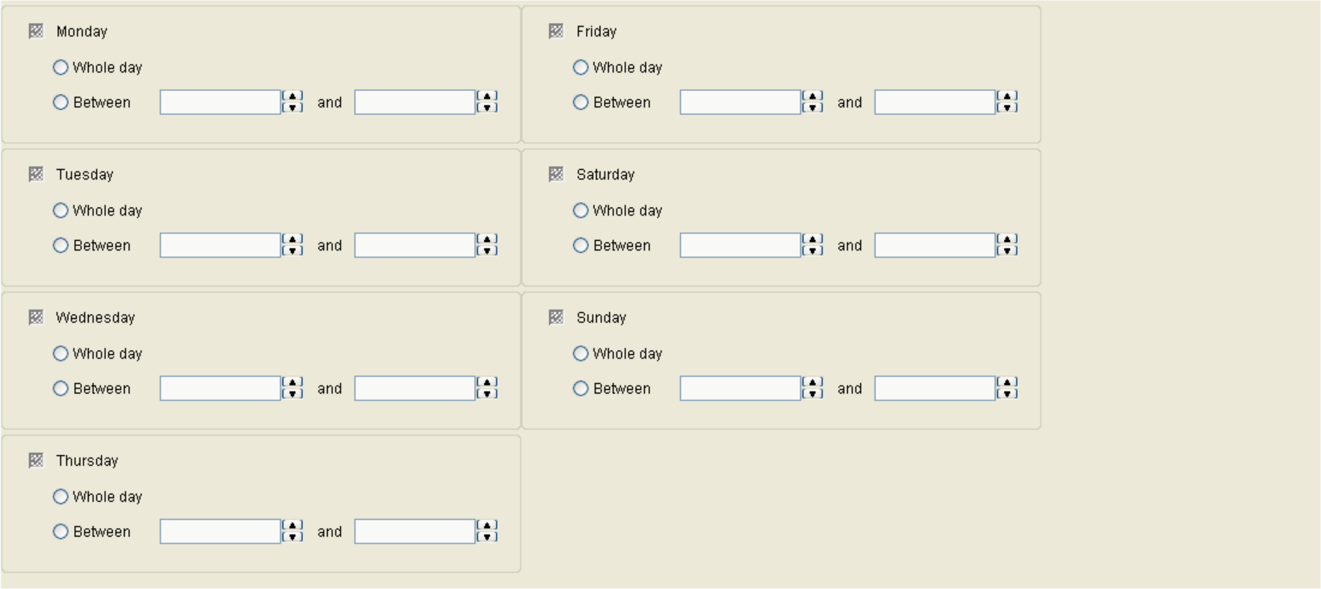
Check box for activating the option to prevent software distribution on the specific day.

Between ... and ...

Check box for activating the option to prevent software distribution during a particular period of time on the specific day. The start and end of the time segment can be defined.

6.2.2.7 "Certificate Deployment Restrictions" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Certificate Deployment Restrictions" Tab



☒ Monday
○ Whole day
○ Between ▲▼ and ▲▼

☒ Tuesday
○ Whole day
○ Between ▲▼ and ▲▼

☒ Wednesday
○ Whole day
○ Between ▲▼ and ▲▼

☒ Thursday
○ Whole day
○ Between ▲▼ and ▲▼

☒ Friday
○ Whole day
○ Between ▲▼ and ▲▼

☒ Saturday
○ Whole day
○ Between ▲▼ and ▲▼

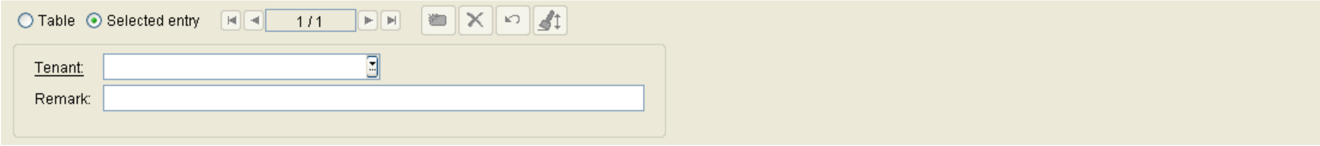
☒ Sunday
○ Whole day
○ Between ▲▼ and ▲▼

For parameter descriptions, see Section 6.2.2.6, ""SW Deployment Restrictions" Tab".

6.2.2.8 "Tenants" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Tenants" Tab

> This tab is available only if the multi-tenancy function of the DLS is installed. See also Section 16.16.1, "Install/Deinstall Multi-Tenancy".



Tenant:
Remark:

Tenant

Name of the tenant.

Remark

Information on the tenant.

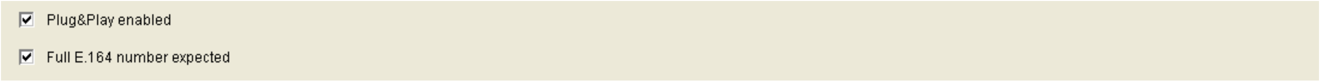
6.2.3 P&P Settings

Call: Main Menu > Administration > Server Configuration > P&P Settings

This area features the following components:

- General Data
- Possible Action Buttons
- "P&P Number Pool" Tab
- "Standard Profile" Tab

General Data



☑ Plug&Play enabled

☑ Full E.164 number expected

Plug&Play enabled

When activated, Plug&Play is enabled for all devices.

Full E.164 Nummer expected

If this switch is activated, the DLS expects the full E.164 call number of an IP Device for Plug&Play resp. autoconfiguration, in order to find the corresponding virtual device.

Possible Action Buttons

Discard

Discards any unsaved changes.

Save

Saves the changes.

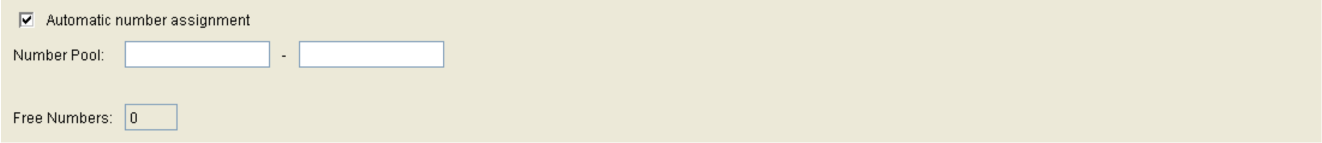
Refresh

Refreshes the screen contents from the database.

6.2.3.1 "P&P Number Pool" Tab

Call: Main Menu > Administration > Server Configuration > P&P Settings > "P&P Number Pool" Tab

Define how the E.164 number should be used in the case of autoconfiguration.



☑ Automatic number assignment

Number Pool: ____ - ____

Free Numbers: 0

Automatic number assignment

If activated, Plug&Play automatically assigns an E.164 call number from the number pool to the IP device.

Number Pool

Band of successive fully qualified E.164 numbers, which is defined by entering the first and last number.

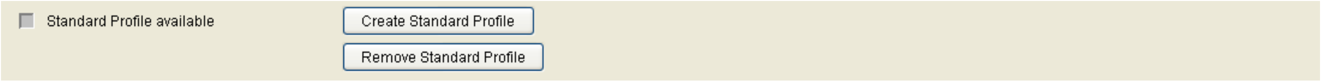
Free Numbers

Number of E.164 call numbers from the pool which have not been assigned yet.

6.2.3.2 "Standard Profile" Tab

Call: Main Menu > Administration > Server Configuration > P&P Settings > "Standard Profile" Tab

Determine how the E.164 number shall be used for autoconfiguration.



Standard Profile available

This check box is active when the standard profile exists.

Create Standard Profile

Creates a standard profile for IP Phones und IP Clients. This profile contains pre-defined templates.

Remove Standard Profile

Removes the standard profile.

6.2.4 FTP Server Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "Tenants" Tab

General Data

Call: Main Menu > Administration > Server Configuration > FTP Server Configuration.

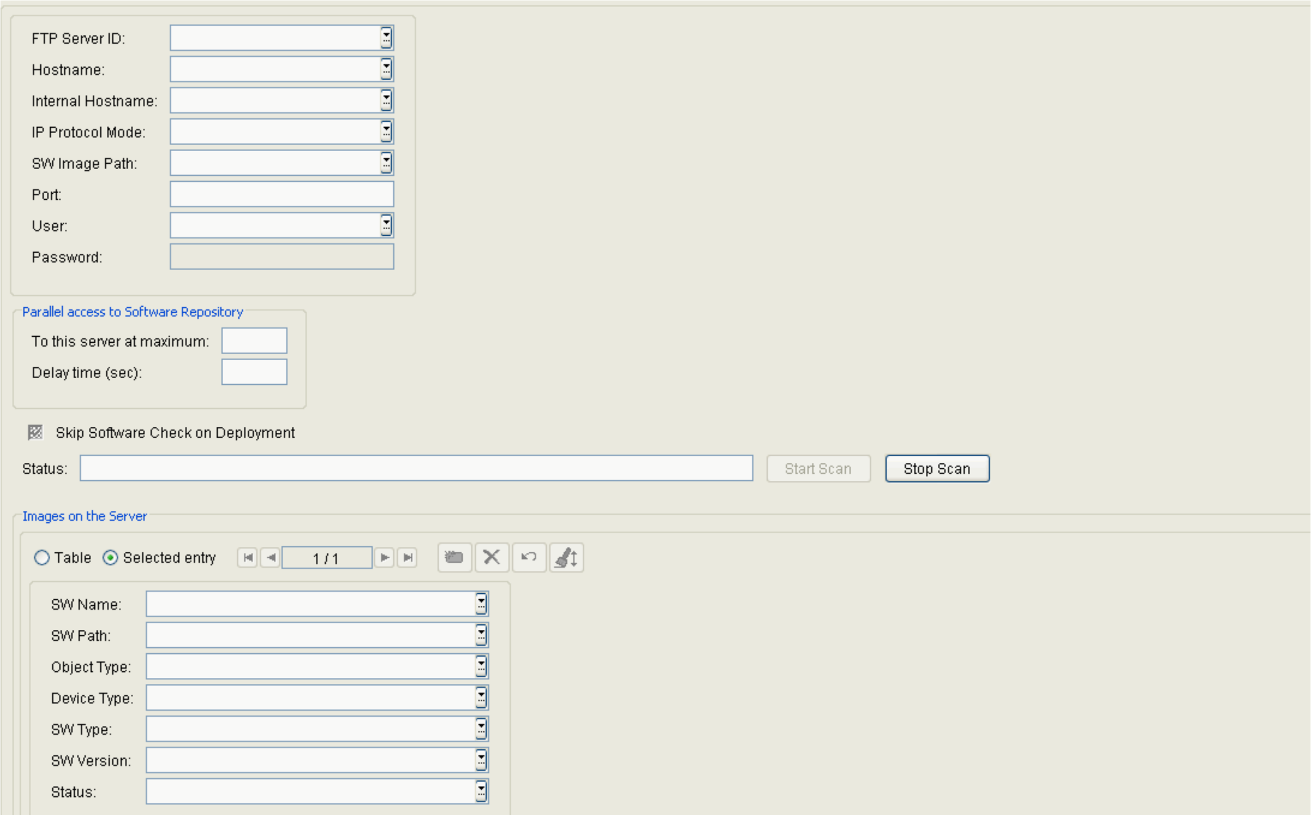
In this area, you can configure access data for one or more FTP servers. All FTP servers detected by the **Search** routine are listed in **Table** view. Moreover, you can read all files which are existant on the FTP server and relevant for IP devices into the DLS database. After this, the data are available for deployment.

For each file on the FTP server, one object per possible usage is created. For instance, a WAV file may be used as ringtone or as hold music. If there is, for instance, a file named "notify.wav", the objects "notify.wav (OpenStage,RINGTONE)" and "notify.wav (OpenStage,MOH)" would be created.

> The entries depend on the configuration of the FTP server in use at the time.
> For more information on configuring FTP servers, see Section 4.10.1, "FTP Server".

An FTP server is necessary to load files to a device - phone software images or on-hold music, for example. You must also configure at least one FTP server for the DLS to register the available phone software images.

> In contrast to IP phone software and files (which must be present on an FTP server), software and files for IP clients are provided on a network drive and configured as described in **Network Drive Configuration**.



FTP Server ID:

Unique name used to manage and address each FTP server configured.

Hostname:

Host name or IP address of the FTP server (accessible by IP Devices).

Internal Hostname

If specified, this host name or IP address will be used for scan and SW check by the DLS.

IP Protocol Mode

The FTP server is supporting this IP protocol version.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

SW Image Path:

Path to the software image relative to the directory root of the FTP server. If the data is located directly in the directory root, enter / (slash).

Port:

The default port number for FTP is 21 and cannot be changed.

User:

User name for read-only access to the FTP server. Read-only access is used by the IP Device to access the software.

Password:

Password for read-only access to the FTP server. This entry is optional.

Parallel access to Software Repository

To this server at maximum:

Maximum number of simultaneous accesses to the server. This value corresponds to the number of simultaneous software distribution actions (software deployment jobs) to the devices. The value must be less than the maximum number of simultaneous connections for which the FTP server is configured.

Value range: **1 - 500**.

Default: **10**.

Delay time (sec):

Time between two distribution jobs. The value set should only be increased if the LAN infrastructure is slow (or exceptionally, in the case of a moderately fast connection to the FTP server).

Value range: **1 - 3000** seconds.

Default: **10**.

Skip Software Check on Deployment

If this switch is active, the file containing the phone software is not examined before deployment.

Status:

Status of s server action.

Possible values:

- **Scanning...**
- **Finished**
- **Stopped**

Start Scan

Start a search for software and data files on the FTP server. Entries concerning files which are not available on the server will be deleted in the DLS database.

Stop Scan

Stop scanning the FTP Server for software and data files.

Images on the Server

If a scan has been executed, information on all software and data files found during the scan is displayed here.

SW Name:

Name of the file.

SW Path:

Directory path and file name.

Object Type:

Type of file.

Examples: **Software Image**, **Logo File**, **Screen Saver**.

Device Type:

Device type, for which the file is appropriate.

Examples: **optiPoint 410**, **OpenStage Hi**.

SW Type:

Type of the phone software.

Examples: **Siemens SIP**, **Siemens HFA**.

SW Version:

Version ot the phone software.

Status:

Status of the phone software.

Example: **version info missing**.

Valid

Activated if the file is valid.

Possible Action Buttons

Search

Searches the database for FTP servers already installed.

Clear Window

Deletes the data entered in the window.

Save

Saves the data entered/modified.

Discard

Discards any changes made.

New

Creates a new FTP server.

Delete

Deletes the FTP server currently listed in Object view.

Test FTP Parameters

Tests the connection to the current FTP server configured. The result is displayed in the status window.

Refresh

Updates the field content using the database.

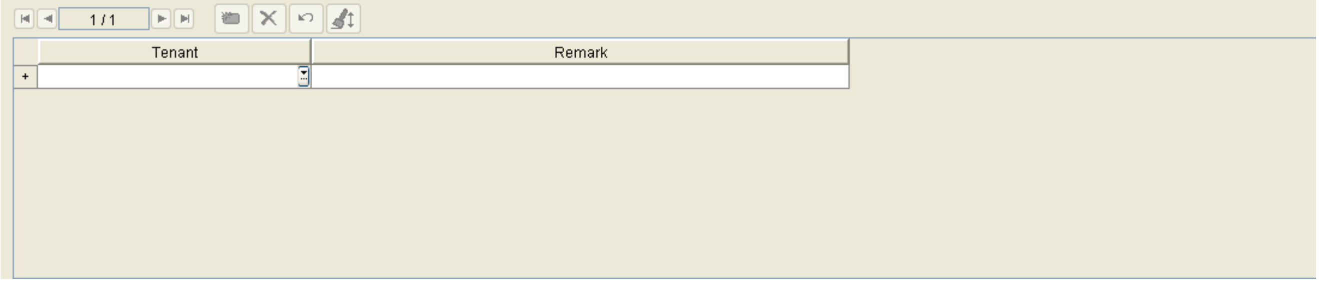
Scan all

All assigned FTP servers will be scanned. A progress bar shows the status of the current server scan. This scan can be cancelled like a single scan by clicking the button **Stop Scan**.

6.2.4.1 "Tenants" Tab

Call: Main Menu > Administration > Server Configuration > FTP Server Configuration > "Tenants" Tab

This tab is available only if the multi-tenancy function of the DLS is installed. See also Section 16.16.1, "Install/Deinstall Multi-Tenancy".



Tenant

Name of the tenant.

Remark

Information on the tenant.

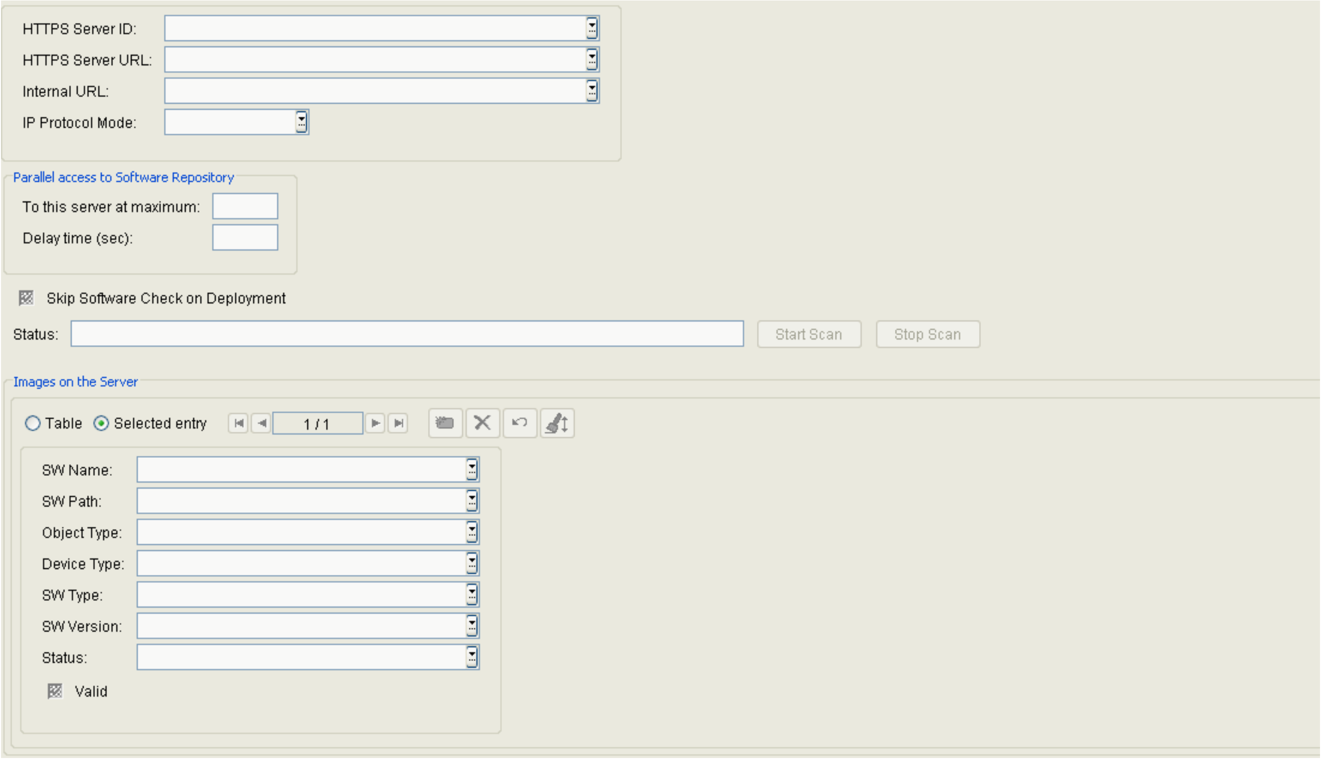
6.2.5 HTTPS Server Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "Tenants" Tab

General Data

Call: Main Menu > Administration > Server Configuration > HTTPS Server Configuration



HTTPS servers can only be used for OpenStage devices.

In this area, you can configure access data for one or more HTTPS servers. All HTTPS servers detected by the search routine are listed in **Table** view.

An HTTPS server can be used instead of an FTP server to load data, such as, on-hold music or phone software images onto an OpenStage device. You must also configure at least one HTTPS server for the DLS to register the available phone software images.

The entries depend on the configuration of the HTTPS server in use at the time.

In contrast to the IP phone software that must be loaded on an HTTPS server, the software for IP clients is provided on a network drive as described under Windows Network Drive Configuration.

If the multi-tenancy function of the DLS has been installed, the following component is available in this area:

- "Tenants" Tab

HTTPS Server ID

Unique name used to address each HTTPS server configured.

HTTPS Server URL

URL of the HTTPS server (accessible by IP Devices).

Internal Hostname

If specified, this host name or IP address will be used for scan and SW check by the DLS.

IP Protocol Mode

The HTTPS server is supporting this IP protocol version.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Parallel access to Software Repository

To this server at maximum:

Maximum number of simultaneous accesses to the server. This value corresponds to the number of simultaneous software distribution actions (software deployment jobs) to the devices. The value must be less than the maximum number of simultaneous connections for which the FTP server is configured.

Value range: **1 - 500**.

Default: **10**.

Delay time (in seconds):

Time between two distribution jobs. The value set should only be increased if the LAN infrastructure is slow (or exceptionally, in the case of a moderately fast connection to the FTP server).

Value range: **1 - 3000** seconds.

Default: **10**.

Skip Software Check on Deployment

If this switch is active, the file containing the phone software is not examined before deployment.

Status:

Status of s server action.

Possible values:

- **Scanning...**
- **Finished**
- **Stopped**

Start Scan

Start a search for software and data files on the HTTPS server. Entries concerning files which are not available on the server will be deleted in the DLS database.

Stop Scan

Stops scanning the HTTPS Server for software and data files.

Images on the Server

If a scan has been executed, information on all software and data files found during the scan is displayed here.

SW Name:

Name of the file.

SW Path:

Directory path and file name.

Object Type:

Type of file.

Examples: **Software Image**, **Logo File**, **Screen Saver**.

Device Type:

Device type, for which the file is appropriate.

Examples: **optiPoint 410**, **OpenStage Hi**.

SW Type:

Type of the phone software.

Examples: **Siemens SIP**, **Siemens HFA**.

SW Version:

Version ot the phone software.

Status:

Status of the phone software.

Example: **version info missing**.

Valid

Activated if the file is valid.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Search

Searches the database for HTTPS servers already configured.

Clear Window

Deletes the data entered in the window.

New

Creates a new HTTPS server.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Test

Tests the connection to the current HTTPS server configured. The result is displayed in the status window.

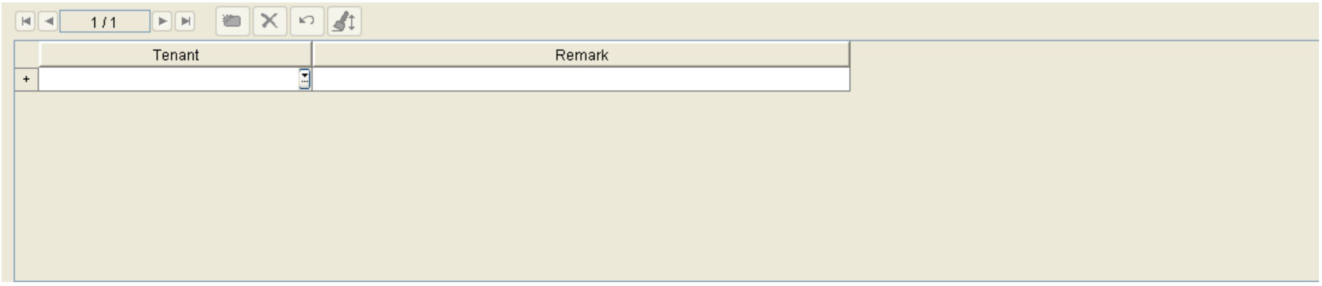
Scan all

All assigned HTTP servers will be scanned. A progress bar shows the status of the current server scan. This scan can be cancelled like a single scan by clicking the button **Stop Scan**.

6.2.5.1 "Tenants" Tab

Call: Main Menu > Administration > Server Configuration > HTTPS Server Configuration > "Tenants" Tab

> This tab is available only if the multi-tenancy function of the DLS is installed. See also Section 16.16.1, "Install/Deinstall Multi-Tenancy".



Tenant

Name of the tenant.

Remark

Information on the tenant.

6.2.6 Network Drive Configuration

Call: Main Menu > Administration > Server Configuration > Network Drive Configuration.

This area features the following components:

- General Data
- Possible Action Buttons
- "Tenants" Tab

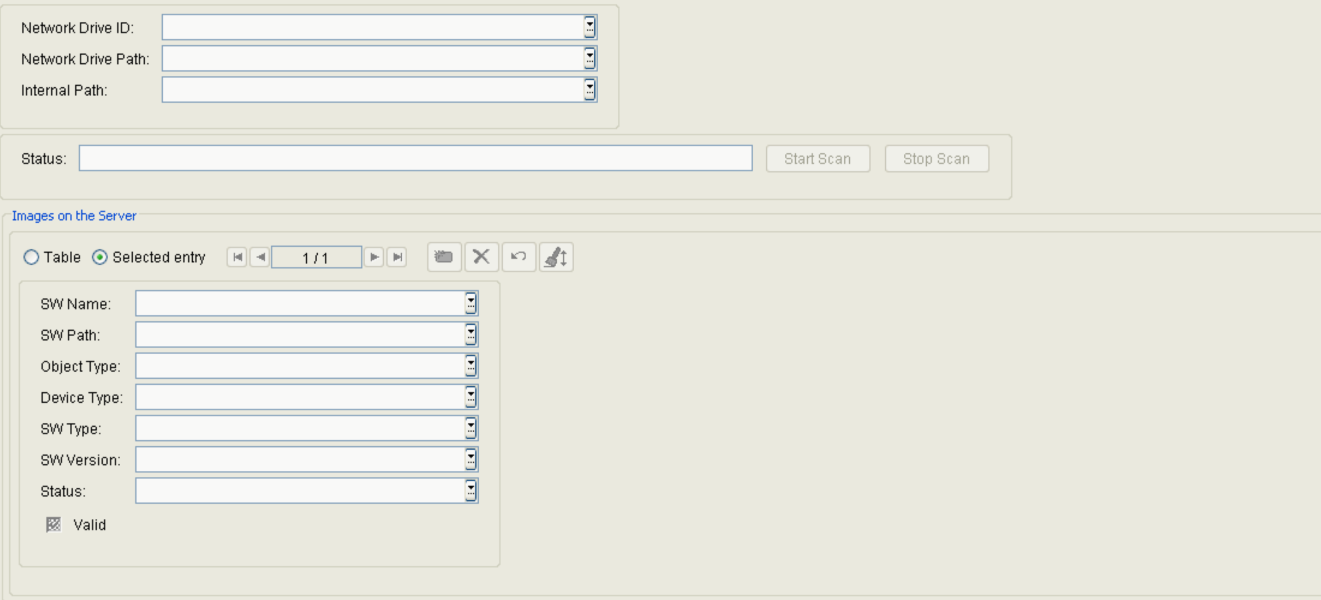
General Data

In this area, you can configure one or more network drives.

> Deployment via a network drive is not available in the onboard variants of DLS on OpenScape Voice systems.

> The information here is only necessary for the distribution of IP client software. Access to the software for IP phones is via FTP/HTTPS. The server is configured in the **FTP Server Configuration** or **HTTPS Server Configuration** area.
>
> Authorizations for accessing the network release must be set on the *[DLS server name]\system* to guarantee access for the DLS Web server running by default as the service.
>
> If these authorizations cannot be extended or if the authorizations for access to the network releases are limited to a user group, then you must ensure that the DLS runs in the user context that is also included in this user group or that can access this network release.
>
> The user context can be modified as follows (Windows XP, for example):
> **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services** > **DeploymentService** > [right-click] **Properties** > **Log On** tab.

Enter the data necessary for the Windows network drive.



Network Drive ID:

Unique name for addressing the network drive configured.

Network Drive Path:

Computer name or IP address where the drive is released and the path of the released directory. The directory must be accessible by IP Clients.

Internal Path

If specified, this path will be used for scan by the DLS.

Status:

Status of s server action.

Possible values:

- **Scanning...**
- **Finished**
- **Stopped**

Start Scan

Start a search for software and data files on the network drive. Entries concerning files which are not available on the server will be deleted in the DLS database.

Stop Scan

Stops scanning the network drive for software and data files.

Images on the Server

If a scan has been executed, information on all software and data files found during the scan is displayed here.

SW Name:

Name of the file.

SW Path:

Directory path and file name.

Object Type:

Type of file.

Examples: **Software Image**, **Logo File**, **Screen Saver**.

Device Type:

Device type, for which the file is appropriate.

Examples: **optiPoint 410**, **OpenStage Hi**.

SW Type:

Type of the phone software.

Examples: **Siemens SIP**, **Siemens HFA**.

SW Version:

Version ot the phone software.

Status:

Status of the phone software.

Example: **version info missing**.

Valid

Activated if the file is valid.

Possible Action Buttons

Save

Saves the data entered/modified.

Discard

Discards any changes made.

New

Creates a new network drive.

Delete

Deletes the network path currently listed in Object view.

Refresh

Updates the field content using the database.

Scan all

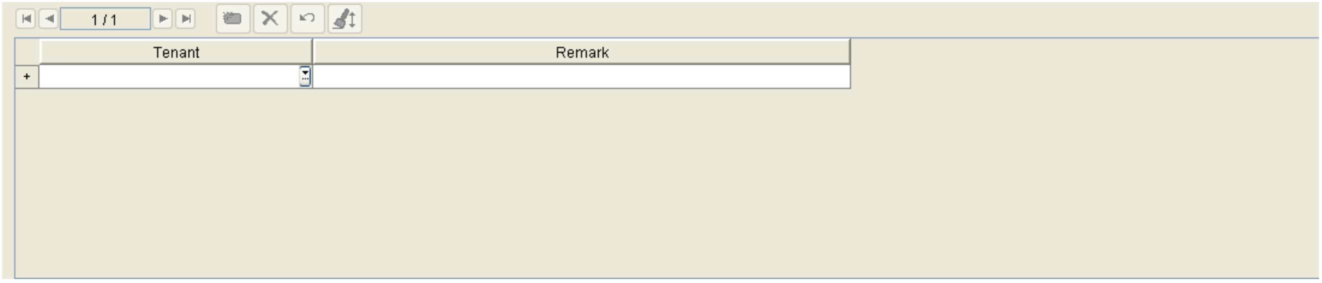
All assigned network drives will be scanned. A progress bar shows the status of the current scan.

This scan can be cancelled like a single scan by clicking the button **Stop Scan**.

6.2.6.1 "Tenants" Tab

Call: Main Menu > Administration > Server Configuration > Network Drive Configuration > "Tenants" Tab

> This tab is available only if the multi-tenancy function of the DLS is installed. See also Section 16.16.1, "Install/Deinstall Multi-Tenancy".



Tenant

Name of the tenant.

Remark

Information on the tenant.

6.2.7 Infrastructure Policy

Call: Main Menu > Administration > Server Configuration > Infrastructure Policy

This mask supports the mapping to an infrastructure policy according to the switch IP address, the switch port and the network policy. The mapping follows the order of the entries, i. e. the first matching entry will define the resulting infrastructure policy.

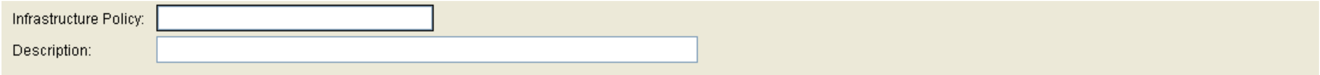
It is possible to enter regular expressions for the attributes mapped to the infrastructure policy. An empty mapping attribute means that it is not relevant for the mapping.

To trigger automatic adaptation, the infrastructure policy must be used as criterion for a location (see **Administration** > **Server Configuration** > **Location** >**"Infrastructure Policies" Tab**.

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "Infrastructure Policies" Tab
- "Infrastructure Policy Table" Tab

General Data



Infrastructure Policy:

Description:

Infrastructure Policy:

Name of the infrastructure policy.

Description:

Description of the infrastructure policy.

Possible Action Buttons

Depending on the statud of the DLS, various action buttons are available.

Search

Searches the database for configured IP infrastructure policies.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the Search view before new search criteria are entered.

New

Creates a new data record for IP infrastructure policies.

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

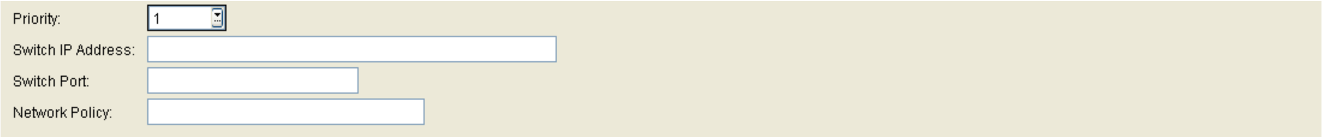
Updates the window using the database.

Apply

Applies IP infrastructure table to already existing IP Devices.

6.2.7.1 "Infrastructure Policy Table" Tab

Call: Main Menu > Administration > Server Configuration > Infrastructure Policy > "Infrastructure Policy Table" Tab



Priority:	1
Switch IP Address:	
Switch Port:	
Network Policy:	

Priority:

The matching policy will be assigned according to the priority entered here.

Switch IP address:

IP address of the switch where the IP Phone is plugged in.

Regular Expressions may be used.

Switch Port:

Port number of the switch where the IP Phone is plugged in.

Regular Expressions may be used.

Network Policy:

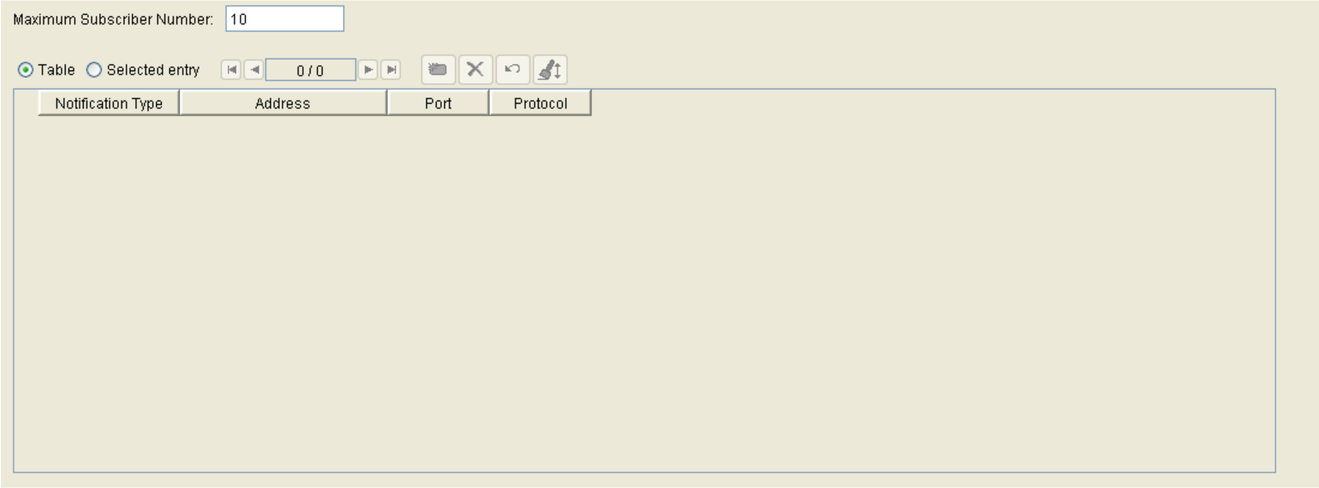
Network Policy assigned to IP Phone.

Regular Expressions may be used.

6.2.8 API Notifications

Call: Main Menu > Administration > Server Configuration > API Notifications

This screen offers an overview on the current subscribers to API notifications. The administrator can restrict the maximum number of subscriptions and also delete entries.



Maximum Subscriber Number: 10

● Table ○ Selected entry

Notification Type	Address	Port	Protocol

Maximum Subscriber Number:

If this number is reached, the attempt to subscribe to notifications will fail.

Notification Type

Type of notification.

Possible values:

- **inventoryInfo**
  New IP Phones and E.164 changes will be notified.
- **serverStart**
  Notification on DLS server start.

Address

Target IP address for notification.

Port

Target port for notification.

Protocol

Protocol used for notification: UDP.

6.2.9 XML Applications

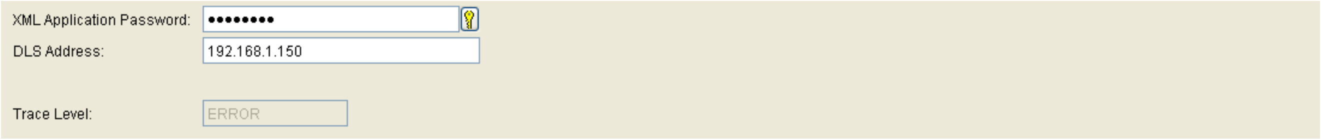
Call: Main Menu > Administration > Server Configuration > XML Applications

XML applications are configured here.

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "Deployment Service" Tab
- "Location Service" Tab
- "News Service" Tab
- "MakeCall" Tab

General Data



XML Application Password: •••••••••

DLS Address: 192.168.1.150

Trace Level: ERROR

XML Applications Password

Common password of all password protected XML applications.

DLS Address

IP address of the DLS, or, in a multi-node installation, the IP address of the DLS cluster.

Trace Level

Trace Level for XML Applikationen which are running as self-contained web applications. The trace data are stored under
`<Installation directory>\Tomcat5\webapps\XMLApplications\log\dlsXMLAppsLog.txt`

Possible Options:

- **ERROR**
- **INFO**
- **DEBUG**

Possible Action Buttons

Discard

Discards any changes entered.

Save

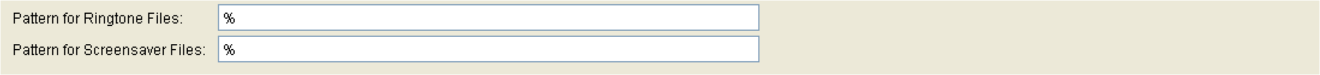
Saves the field contents to the database.

Refresh

Updates the window using the database.

6.2.9.1 "Deployment Service" Tab

Call: Main Menu > Administration > Server Configuration > XML Applications > "Deployment Service" Tab



Pattern for Ringtone Files:	%
Pattern for Screensaver Files:	%

Pattern for Ringtone Files

Pattern for the partially qualified selection of ringtone files available from the FTP or HTTPS Server.

Example: ***SEN*New*Devices***

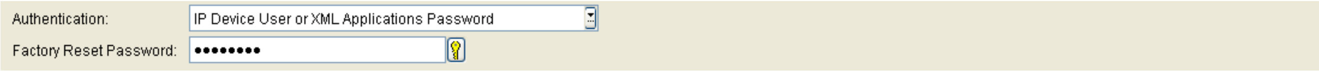
Pattern for Screensaver Files

Pattern for the partially qualified selection of screensaver files available from the FTP or HTTPS Server.

Example: ***SEN*New*Devices***

6.2.9.2 "Location Service" Tab

Call: Main Menu > Administration > Server Configuration > XML Applications > "Location Service" Tab



Authentication: IP Device User or XML Applications Password

Factory Reset Password: ••••••••

Authentication

Select a password to execute this XML application.

Possible options:

- **IP Device User Password**

> If the call number of the OpenStage end device is to be changed, this is the password of that virtual device to which the new call number is assigned.

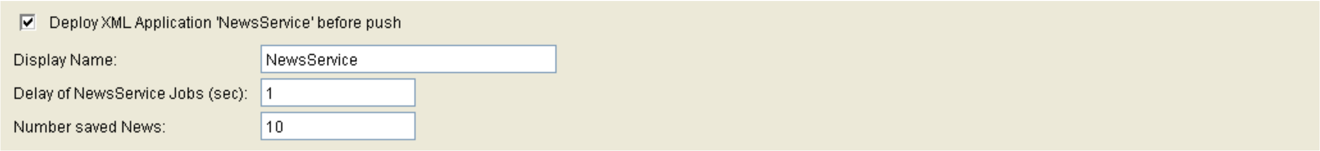
- **XML Applications Password**
- **IP Device User Password or XML Applikations Password**

Factory Reset Password

Password to execute a factory reset on OpenStage end devices. At this, the factory setting are restored.

6.2.9.3 "News Service" Tab

Call: Main Menu > Administration > Server Configuration > XML Applications > "News Service" Tab



☑ Deploy XML Application 'NewsService' before push

Display Name:	NewsService
Delay of NewsService Jobs (sec):	1
Number saved News:	10

Deploy XML Application 'News Service' before push

When activated, the XML application 'NewsService' will be deployed before first execution, if it is not yet configured at the end device.

Display Name:

This name is shown on the end device display for the XML application 'NewsService' if it has been automatically deployed.

Delay of News Service Jobs (sec):

Delay of jobs in seconds after bulk change operations. This is the minimal time interval between the sending of the same message to two different end devices. Notifications are not delayed.

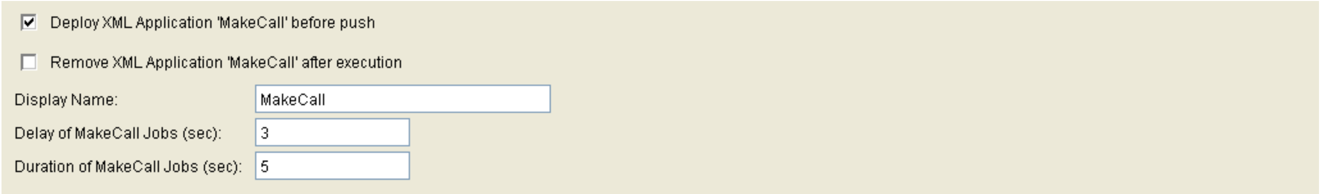
Value range: **1** - **300**

Number saved News:

Number of news which have already been sent via the XML application 'NewsService', and which have been saved. As soon as the number is exceeded, the oldest news message is deleed.

6.2.9.4 "MakeCall" Tab

Call: Main Menu > Administration > Server Configuration > XML Applications > "MakeCall" Tab



☑ Deploy XML Application 'MakeCall' before push

□ Remove XML Application 'MakeCall' after execution

Display Name: MakeCall

Delay of MakeCall Jobs (sec): 3

Duration of MakeCall Jobs (sec): 5

Deploy XML Application ’MakeCall’ before push

Switch to activate the first deployment of the News Service application.

Whe activated, the XML application ’MakeCall’ is deployed before the first execution, if it is not yet configured at the end device.

Remove XML Application ’MakeCall’ after execution

When activated, the XML application ’MakeCall’ is removed from the end device after it has been executed.

Display Name:

This name is shown on the end device display for the XML application ’MakeCall’ if it has been automatically deployed.

Delay of MakeCall Jobs (sec):

Minimal time interval in seconds between the initiating of a call from two different end devices; is needed for bulk changes.

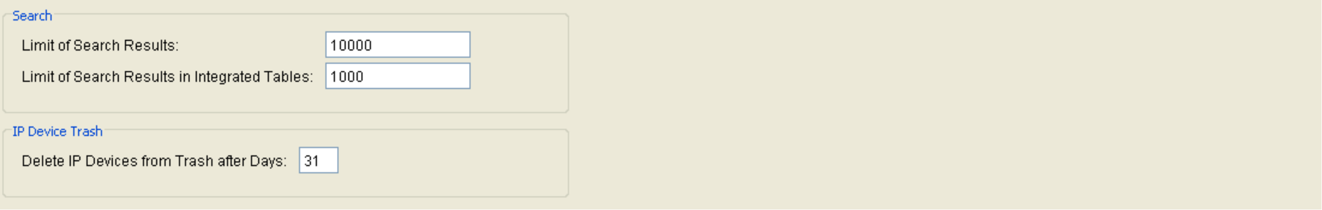
Value range: **1** ... **500**

Duration of MakeCall jobs (sec):

This duration is equivalent to the sum from the time needed for initiating the call and the time needed for the call proper.

6.2.10 Options

Call: Main Menu > Administration > Server Configuration > Options



Search

Limit of Search Results: 10000

Limit of Search Results in Integrated Tables: 1000

IP Device Trash

Delete IP Devices from Trash after Days: 31

Search

Limit of Search Results

Maximum number of records displayed when a search is done.

> Changed values first will be used not until the DLS Client has been restarted.

Limit of Search Results in Integrated Tables

Maximum number of records displayed in integrated tables when a search is done.

> Changed values first will be used not until the DLS Client has been restarted.

IP Device Trash

Delete IP Devices from Trash after Days

Number of days after which IP Devices marked to be deleted will be deleted completely from the DLS database.

Value range:

1 ... **365**

Possible Action Buttons

Discard

Discards any unsaved changes.

Save

Saves the changes.

Refresh

Refreshes the screen contents from the database.

6.3 Cluster Configuration

Call: Main Menu > Administration > Cluster Configuration

This menu item consists of the following areas:

- Deployment Server
- Cluster Settings

6.3.1 Deployment Server

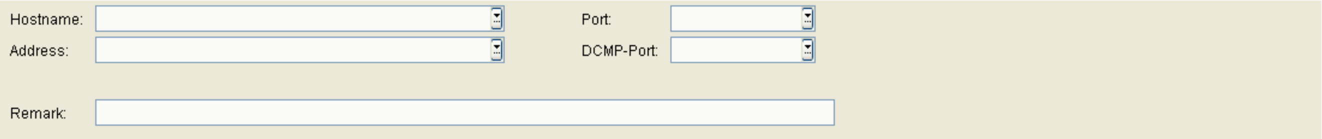
Call: Main Menu > Administration > Cluster Configuration > Deployment Server

This area is used for monitoring and controlling the DLS server installed in the cluster. You can also stop, start or restart the deployment service running on the individual servers here. The requirement for this is that they are registered as cluster nodes in the DLS database. Active nodes log back on at five-minute intervals.

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

General Data



Hostname:

Name of the node within the cluster.

Address:

IP address, domain, or host name of the DLS.

Remark:

Field for general information.

Port:

Port of the DLS.

DCMP-Port:

Port of the DCMP (DLS Communication Management Proxy).

Possible Action Buttons

Search

Searches the database for configured servers that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

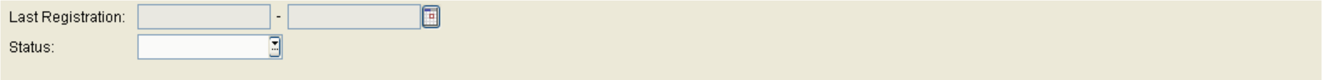
Updates the window using the database.

Deployment Service

Opens a dialog window to start, stop or restart the Deployment Service at the selected node.

6.3.1.1 "Info" Tab

Call: Main Menu > Administration > Cluster Configuration > Deployment Server > "Info" Tab



Last Registration:	-
Status:	

Last Registration

Last time the node registered at the cluster.

Status

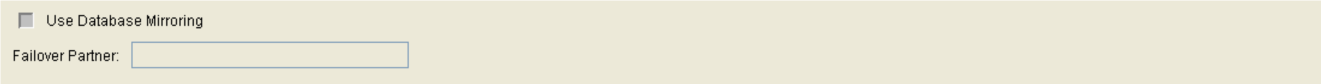
Status of the node within the cluster.

Possible values:

- **Active**
  The node is active.
- **Inactive**
  The node has either logged itself on as inactive or was recognized as inactive by other nodes in the cluster.

6.3.2 Cluster Settings

Call: Main Menu > Administration > Cluster Configuration > Cluster Settings



□ Use Database Mirroring

Failover Partner:

Use Database Mirroring

Switch on database mirroring. This is helpful only if MS SQL database mirroring has been configured for the DLS database.

Failover Partner

IP address of the mirroring instance for the DLS database.

6.4 Display Logging Data

Call: Main Menu > Administration > Display Logging Data

This menu item consists of the following areas:

- Activity and Error Log
- Audit and Security Log
- P&P Import Protocols
- Alarm Protocol

6.4.1 Activity and Error Log

Call: Main Menu > Administration > Server Configuration > Display Logging Data > Activity and Error Log

Specify which events should be logged and how long events should be saved.

You can select filters to view a specific range of logged data. The filtered data is displayed in a separate browser window.

This area features the following components:

- Possible Action Buttons
- "Configuration" Tab
- "Protocol" Tab

Possible Action Buttons

Save

Saves all settings made.

Discard

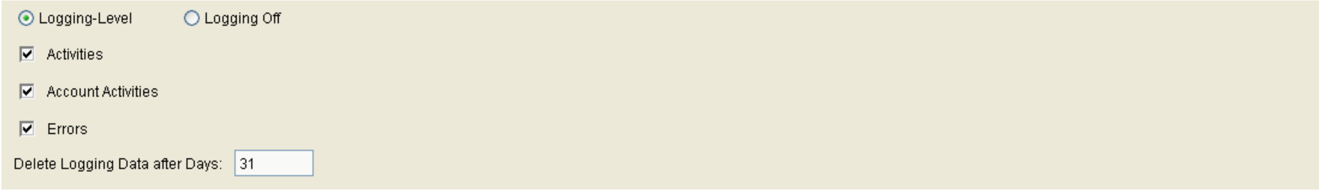
Discards any changes entered.

Refresh

Updates the window using the database.

6.4.1.1 "Configuration" Tab

Call: Main Menu > Administration > Display Logging Data > Activity and Error Log > "Configuration" Tab



● Logging-Level ○ Logging Off

☑ Activities

☑ Account Activities

☑ Errors

Delete Logging Data after Days: 31

Logging-Level

Check box for activating logging.

Logging off

Check box for deactivating logging.

Activities

All DLS activities must be logged in the Activities log.

Account Activities

All account activities must be logged in the Account Activities log.

Errors

The Errors log only records failed actions and internal errors, such as, license violations or SQL database errors.

Delete Logging Data after Days:

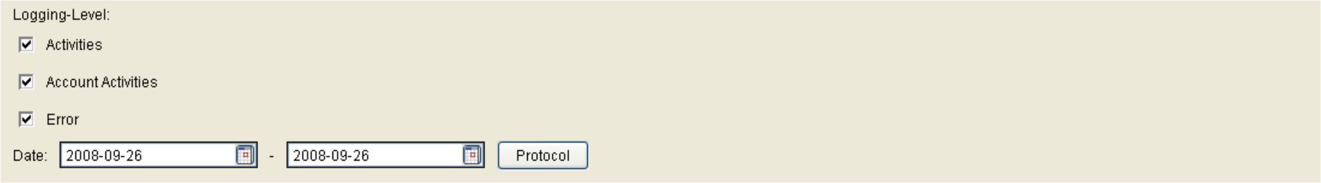
Number of days the logged events should remain saved before they are automatically deleted.

Value range: 1 ... 365 days.

Default: 31

6.4.1.2 "Protocol" Tab

Call: Main Menu > Administration > Display Logging Data > Activity and Error Log > "Protocol" Tab



Logging-Level:

☑ Activities

☑ Account Activities

☑ Error

Date: 2008-09-26 - 2008-09-26

Logging-Level

Activities

All DLS activities must be logged in the Activities log.

Account Activities

All account activities must be logged in the Account Activities log.

Error

The Errors log only records failed actions and internal errors, such as, license violations or SQL database errors.

Date:

Period of time during which the log data should be displayed (for a calendar, see Section 5.4.2.4, "Time field with calendar button").

Protocol

Starts outputting logging data. The filtered data is displayed in a separate browser window.

6.4.2 Audit and Security Log

This functionality is available on the GUI depending on the roles and rights of the account.

Call: Main Menu > Administration > Server Configuration > Display Logging Data > Audit and Security Log

This area features the following components:

- Possible Action Buttons
- "Configuration" Tab
- "Protocol" Tab

Possible Action Buttons

Discard

Discards any changes entered. Not applicable for the "Protocol" Tab.

Save

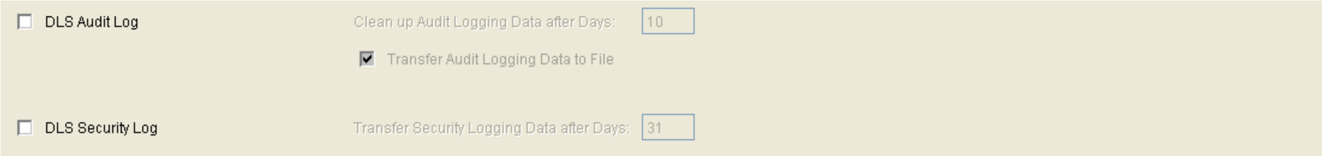
Saves all settings made. Not applicable for the "Protocol" Tab.

Refresh

Updates the window using the database.

6.4.2.1 "Configuration" Tab

Call: Main Menu > Administration > Display Logging Data > Audit and Security Log > "Configuration" Tab



☐ DLS Audit Log

Clean up Audit Logging Data after Days: 10

☑ Transfer Audit Logging Data to File

☐ DLS Security Log

Transfer Security Logging Data after Days: 31

DLS Audit Log

When active, all DLS activities invoked by an account are logged.

Clean up Audit Logging Data after Days

Number of days until the autit related log data is deleted or transferred to a file.

Value range: **1** ... **365**

Transfer Audit Logging Data to File

When active, the audit related logging data will be transferred to a file after the time configured in **Clean up Audit Logging Data after Days**.

DLS Security Log

When active, all security relevant activities are logged.

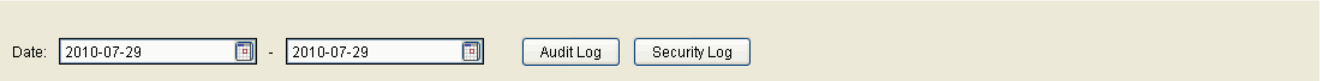
Transfer Security Logging Data after Days

Number of days until the security related log data is transferred to a file.

Value range: **1** ... **365**

6.4.2.2 "Protocol" Tab

Call: Main Menu > Administration > Display Logging Data > Audit and Security Log > "Protocol" Tab


Date: 2010-07-29 - 2010-07-29

Date

Log data that has been created in the time period specified here will be displayed.

Audit Log

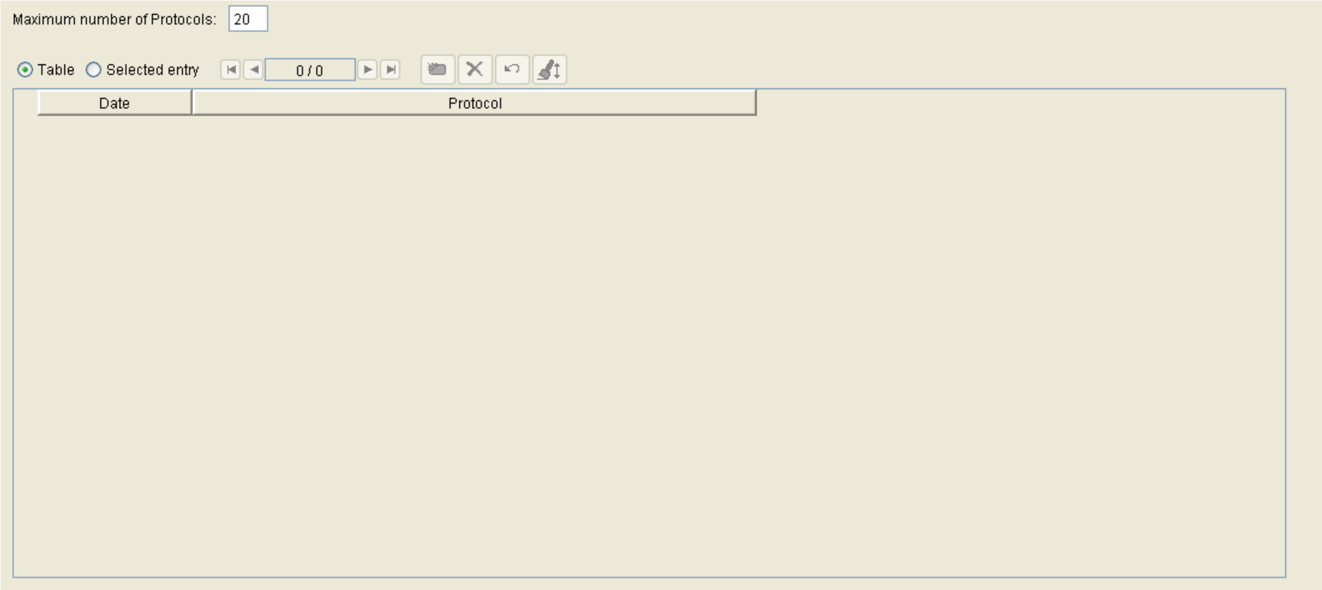
Button to start the display of DLS audit log data.

Security Log

Button to start the display of DLS security log data.

6.4.3 P&P Import Protocols

Call: Main Menu > Administration > Display Logging Data > P&P Import Protocols



Maximum number of Protocols: 20

For information on general interface operation, see Section 5.4.2, "Work Area".

Maximum number of Protocols:

The maximum number of protocols created when importing plug&play data.

Value range: **1** ... **40**.

Date

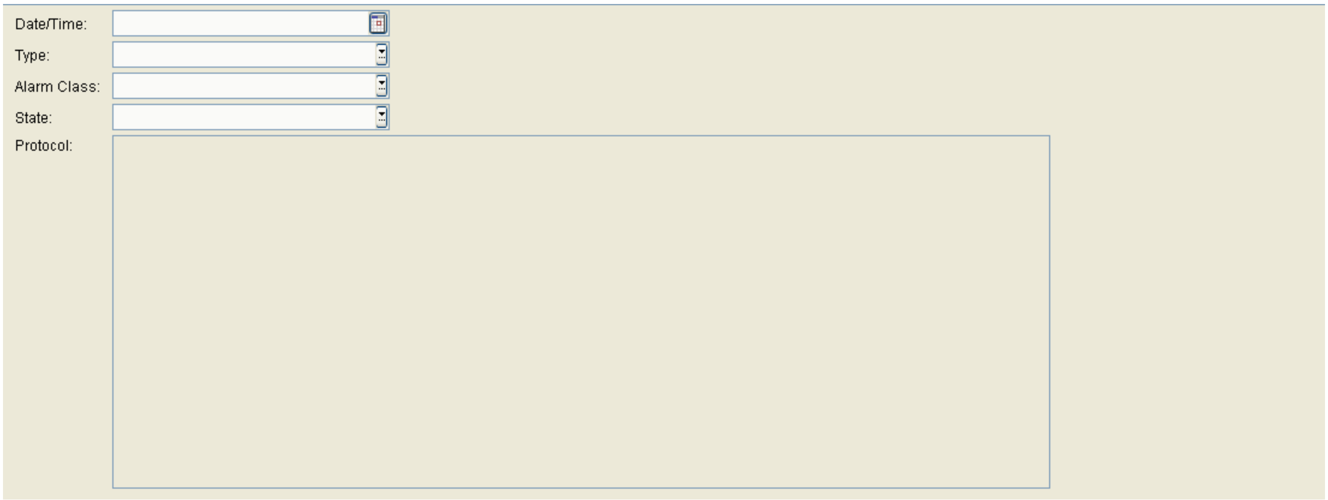
Protocol creation date.

Protocol

Plug&Play import protocol.

6.4.4 Alarm Protocol

Call: Main Menu > Administration > Display Logging Data > Alarm Protocol



Date/Time:

Type:

Alarm Class:

State:

Protocol:

Date/Time

Date/Time at which the action has started.

Alarm Class

Alarm class of the alarm.

Type

Type of alarm.

State

State of the action.

Possible Options:

- **running**
- **pending**
- **finished**
- **failed**
- **timeout**

Protocol

Protocol of the execution.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Refresh

Refreshes the content of the relevant page.

6.5 Alarm Configuration

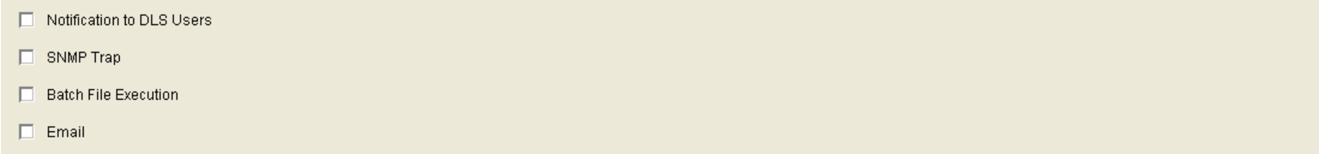
Call: Main Menu > Administration > Alarm Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "Alarm Classes" Tab
- "Notification" Tab
- "SNMP" Tab
- "Batch File" Tab
- "Email" Tab
- "Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data



□ Notification to DLS Users

□ SNMP Trap

□ Batch File Execution

□ Email

Notification to DLS Users

When active, logged on DLS users will be notifed of an alarm, depending on the individual settings in the "Alarm Classes" Tab. For this purpose, the DLS users must be selected for notification by means of the "Notification" Tab. The alarm notification is displayed in the title bar of the DLS window.

SNMP Trap

When active, an SMNP trap is sent to the server determined in the "SNMP" Tab, depending on the individual settings in the "Alarm Classes" Tab.

Batch File Execution:

When active, the batch file specified in the "Batch File" Tab is executed, depending on the individual settings in the "Alarm Classes" Tab.

Email:

When active, an Email is sent using data specified in the "Email" Tab, depending on the individual settings in the "Alarm Classes" Tab.

Possible Action Buttons

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

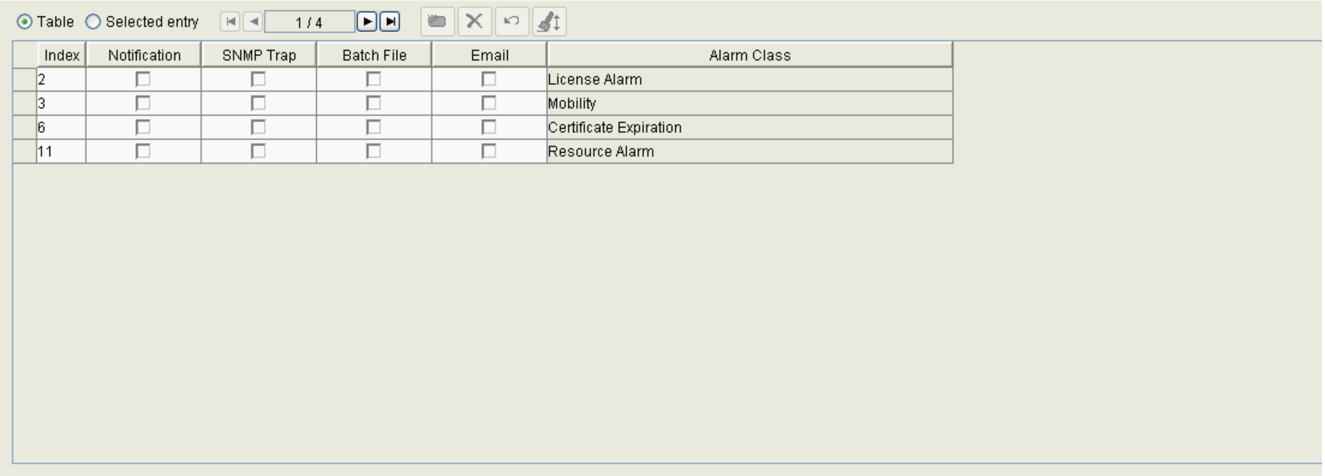
Refresh

Refreshes the content of the relevant page.

6.5.1 "Alarm Classes" Tab

Call: Main Menu > Administration > Alarm Configuration > "Alarm Classes" Tab

Here, the actions for specific alarm classes are selected. The composition of this list depends on the startup settings of the DLS and cannot be modified. The possible actions are user notification, SNMP Trap, execution of a batch file, and the sending of an Email. However, whether the actions are actually executed depends on the check boxes under **General Data**. So, for instance, if **Email** is deactivated under **General Data**, the individual setting in the alarm class table is no longer considered.



Index	Notification	SNMP Trap	Batch File	Email	Alarm Class
2	□	□	□	□	License Alarm
3	□	□	□	□	Mobility
6	□	□	□	□	Certificate Expiration
11	□	□	□	□	Resource Alarm

Index

Index for the alarm action to be triggered (notification, batch file, SNMP trap, or Email).

Notification

If this check box and the **Notification to DLS Users** check box in the **General Data** area are activated, the DLS users listed in the "Notification" Tab are notified according to this alarm class.

SNMP Trap

If this check box as well as the check box **SNMP Trap** under **General Data** is active, the SNMP trap will be sent to the receiver configured for this alarm class.

Batch File

If this check box and the **Batch file execution** check box in the **General Data** area are activated, the configured command file for this alarm class is executed.

Email

If this check box and the **Email** check box in the **General Data** area are activated, the configured e-mail for this alarm class is executed.

Alarm Class

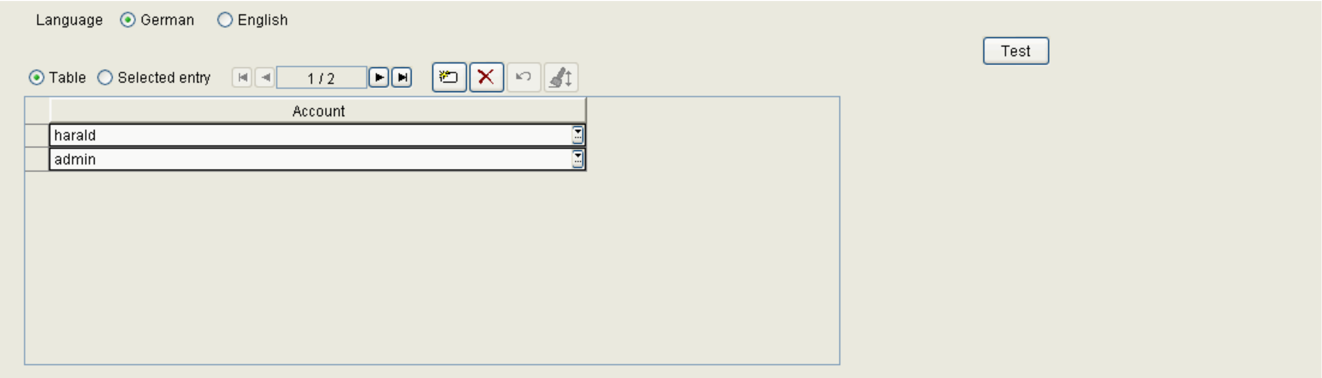
Functional area within which an alarm shall be triggered in case of an error. The list cannot be modified; it depends on the startup settings of the DLS.

Possible values:

- **DLS Service**
- **License Expiration**
- **SIP Mobility**
- **Key Distribution**
- **Certificate Expiration**
- **DCMP**
- **DLS Cluster**
- **Element Manager Synchronization**
- **Policy Alarm**
- **Test Alarm**
- Resource Alarm
  Corresponds with the threshold **Minimum free space** under **Administration** > **File Server**.
- **Signaling and Payload Encryption**
- **IP Device Communication**
- **IP Device File Upload**
- **IP Device Fault Report**

6.5.2 "Notification" Tab

Call: Main Menu > Administration > Alarm Configuration > "Notification" Tab



Language ● German ○ English

● Table ○ Selected entry 1 / 2

Account
harald
admin

Language

The language of the text in the notification alarm.

Possible options:

- **German**
- **English**

Account

The DLS user accounts which shall be notified by the alarms selected in the "Alarm Classes" Tab are entered here.

Test

Tests the notification. The result of the test can be checked under **Administration** > **Display Logging Data** > **Alarm Protocol**.

6.5.3 "SNMP" Tab

Call: Main Menu > Administration > Alarm Configuration > "SNMP" Tab

In case of alarm, a SNMP trap is sent. Not every protocol data unit is supported, especially not GET/SET requests. However, the SNMP partial tree created by the DLS can be read and processed by a trap receiver.

The DLS uses the following part of the MIB to generate traps:

```
hiPathApplicationStatusChange NOTIFICATION-TYPE OBJECTS { hostname,
appName, appState, evtHistory-Date, evtHistoryDescr,
hiPathTrapSeverity} STATUS current DESCRIPTION "A hiPathApplicationS-
tatusChange trap a status change of a HiPath enabled application.
This trap is sent, if a process which is not of service type, causes
trouble. If the error state disappears there shall be a hiPathAppli-
cationStatusChange trap too."::= { hiPathTrapGroup 6 }
```

The parameters have the following meanings resp. values:

`hostname`: Host name of the DLS server.

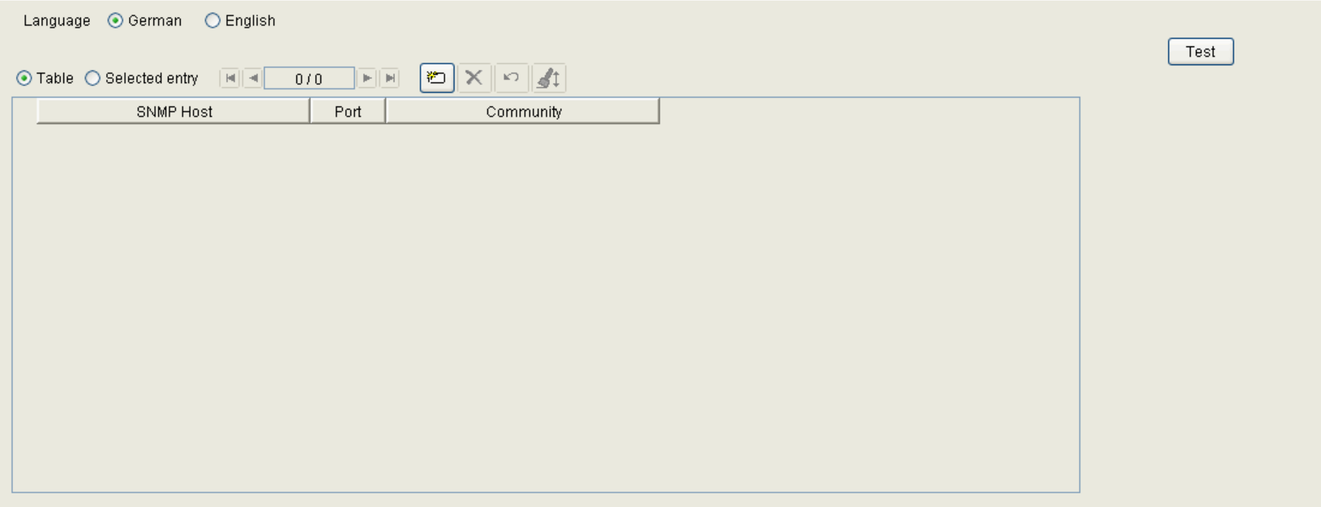
`appName`: "DLS"

`appState`: 3 (= warning)

`evtHistory-Date`: Date of trap occurence.

`evtHistory-Descr`: Description text (as passed by `createHiPathApplicationStatusChange()`).

`hiPathTrapSeverity`: 3 (= warning)



Language

Language of the description text for the SNMP trap.

Possible Options:

- **German**
- **English**

Test

Sends a test SNMP trap. The result of the test can be checked under **Administration** > **Display Logging Data** > **Alarm Protocol**.

SNMP Host

Name of the SNMP Server (manager).

Port

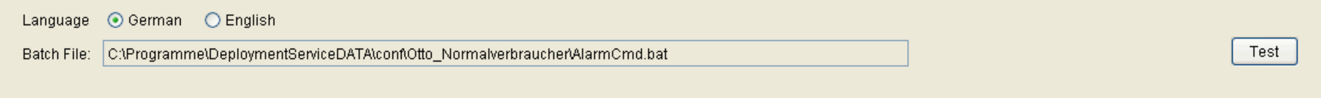
Port of the SNMP server (manager).
Default: **162**

Community

Community / password for the SNMP server (manager).

6.5.4 "Batch File" Tab

Call: Main Menu > Administration > Alarm Configuration > "Batch File" Tab



Language ● German ○ English

Batch File: C:\Programme\DeploymentServiceDATA\conf\Otto_Normalverbraucher\AlarmCmd.bat

Language

The language of the alarm message text.

Possible options:

- **German**
- **English**

Batch File:

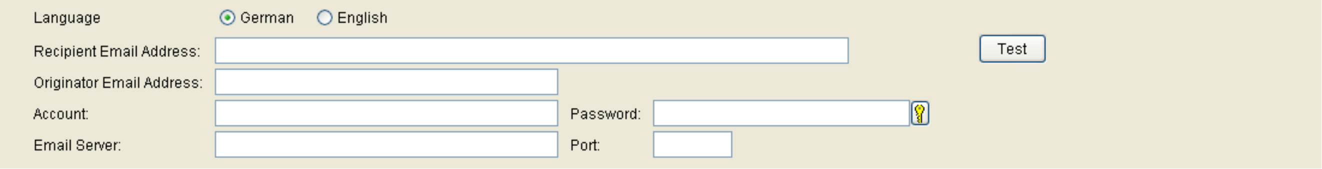
Path and name of the batch file which is executed when an alarm is triggered. After DLS installation, the path and file name reference a sample file which also contains rules for creating a command.

Test

Tests the execution of the batch file. The result of the test can be checked under **Administration** > **Display Logging Data** > **Alarm Protocol**.

6.5.5 "Email" Tab

Call: Main Menu > Administration > Alarm Configuration > "Email" Tab



Language ● German ○ English

Recipient Email Address:

Originator Email Address:

Account:

Password:

Email Server:

Port:

Language

The language of the alarm message text.

Possible options:

- **German**
- **English**

Recipient Email Address:

Email address of the alarm mail recipient.

Test

Tests the Email send operation using the account data entered. The result of the test can be checked under **Administration** > **Display Logging Data** > **Alarm Protocol**.

Originator Email Address:

Email address(es) that appear as the originator address when the mail is sent. One or more addresses can be entered, up to a maximum of 255 characters, separated by ";" "," or " " (space).

Account:

Name of the Email account.

Password:

Password for this Email account.

Email Server:

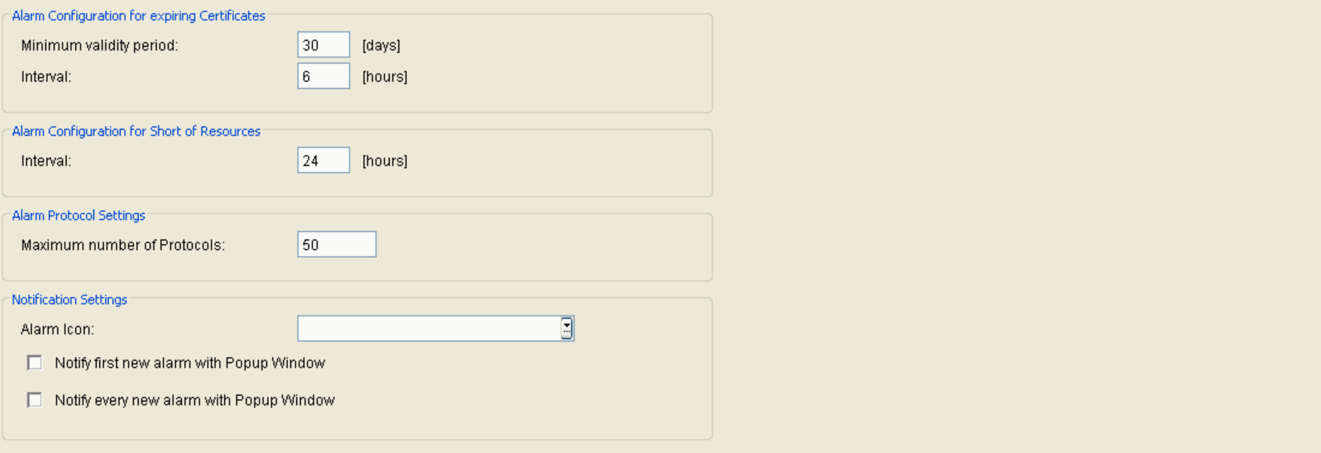
Name of the SMTP server that is to be used for alarm Emails.

Port:

Port number of the SMTP server. If no value is entered, port 25 is used by default.

6.5.6 "Settings" Tab

Call: Main Menu > Administration > Alarm Configuration > "Settings" Tab



Alarm Configuration for expiring Certificates

Minimum validity period: 30 [days]

Interval: 6 [hours]

Alarm Configuration for Short of Resources

Interval: 24 [hours]

Alarm Protocol Settings

Maximum number of Protocols: 50

Notification Settings

Alarm Icon:

□ Notify first new alarm with Popup Window

□ Notify every new alarm with Popup Window

Alarm Configuration for Expiring Certificates

Minimum validity period: [days]

An alarm is issued if a certificate expires during this time period.

Value range: **1** - **60**.

Interval: [hours]

The remaining certificate validity period is checked in the interval specified here.

Value range: **1** - **60**.

Default value: **6**

Alarm Configuration for Short of Resources

Interval [hours]

The supply of resources is checked in the interval specified here.

Value range: **1** - **48**

Alarm Protocol Settings

Maximum number of Protocols:

Maximum number of lines in the protocol.

Value range: **1** - **100000**

Notification Settings

Alarm Icon:

Choice list of icons for notifying the DLS user of alarms which are not closed yet. The icon is displayed in the title bar of the DLS window.

Notify first new alarm with Popup Window

When active, the first new alarm is signaled by means of a popup window, if all prior alarms have been closed before.

Notify every new alarm with Popup Window

When active, every new alarm is signaled by means of a popup window, if no popup window is not already open.

6.6 Backup/Restore

Call: Main Menu > Administration > Backup/Restore

> ⓘ This function is not available in the onboard variants of DLS on OpenScape Voice systems. In this case, the DLS file is backed up using the comprehensive OpenScape Voice Backup/Restore function.

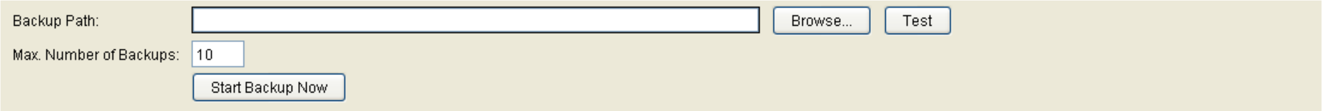
This area features the following components:

- General Data
- Possible Action Buttons
- "Backup" Tab
- "Restore" Tab
- "Protocol" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

Refer to Section 15.8.1, "Automatic Data Backups" for more information on Backup/Restore.

General Data



Max. Number of Backups: 10

Backup Path:

File path where the backup is saved on the DLS server. If the DLS uses a remote database for its data, a directory path on the database server must be entered. It must be reachable by the DLS server. The format must also be usable locally on the database server, e. g.
`\\<IP-Address DB Server>\C$\<Backup Pfad on DB Server on drive C>`

Browse...

Click this button to open a dialog window that you can use to select an existing backup directory. To navigate to the subdirectories of a directory, double click on the directory name. To navigate up to the next higher directory level, double click on "..\". In order to select a directory, highlight it with a single click and, afterwards, click **Open**.

Test

Click Test to verify that the path is valid (accessible).

Max. Number of Backups:

Number of backup files managed. When you create a new backup file, the oldest one is deleted.

Value range: **1** ... **99**.

Start Backup Now

If you click this button, a backup is executed immediately, independently of the automatic, periodic backup setting. This does not use the backup path stored in the database, but the current backup path as it appears in the mask (which may have changed and not yet been saved). This allows you to save an individual backup at a location different from the location where the periodic backups are stored.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

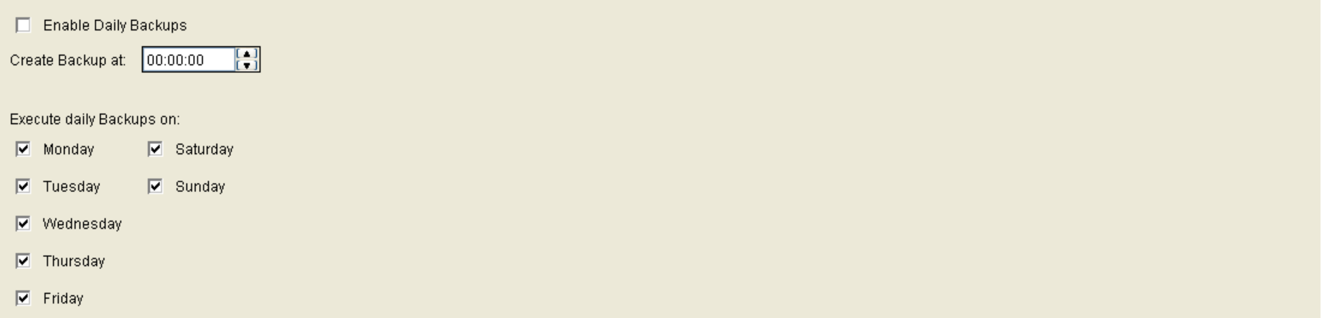
Refresh

Refreshes the content of the relevant page.

6.6.1 "Backup" Tab

Call: Main Menu > Administration > Backup/Restore > "Backup" Tab

For more information, see Section 15.8.1.1, "Configuring Automatic Backups".



□ Enable Daily Backups

Create Backup at: 00:00:00

Execute daily Backups on:

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Enable Daily Backups

Select to activate a daily backup.

Next Backups on:

Time (date and time) of the next scheduled backup (for information on the calender, see Section 5.4.2.4, "Time field with calendar button").

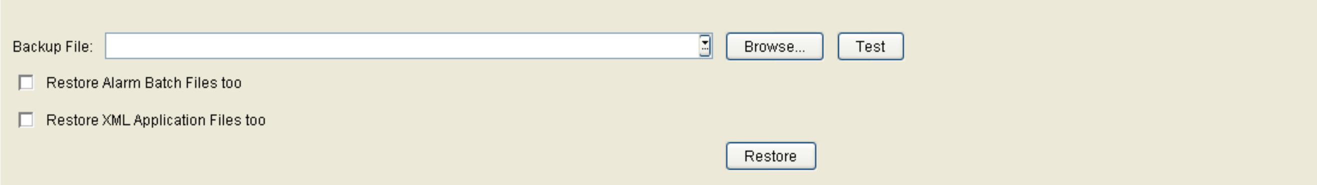
Execute daily Backups on:

If the **Enable Daily Backups** check box is active, use these check boxes to restrict backup to specific days of the week.

6.6.2 "Restore" Tab

Call: Main Menu > Administration > Backup/Restore > "Restore" Tab

For more information, see Section 15.8.1.2, "Restoring Backups".


Backup File:
Browse...
Test
☐ Restore Alarm Batch Files too
☐ Restore XML Application Files too
Restore

Backup File:

Path and file name for restoring a backup on the DLS server. If backups have already been successfully restored, you can enter them using the choice list.

Restore Alarm Batch Files too:

If switch is activated, the stored alarm batch files will be restored.

Restore XML Application Files too:

If switch is activated, the customer specific XML application files will be restored to the directory
`<Installation directory>/XMLApplications/data/custom`

If switch is not activated, the customer specific XML Application Files will be copied to the directory
`<Installation directory>/XMLApplications/data/custom_old`

See also

Browse...

Click this button to open a window where you can select an existing backup file. The path and file name are entered in **Backup File**.

Test

Click this button to verify that the backup file is valid (accessible).

Restore

When you click this button, a restore is executed. A dialog window will ask whether Plug&Play is to be switched off after restore or not. If Plug&Play has been switched off, it is possible to switch it on again via **Administration** > **Server Configuration** > **P&P Settings** > **Plug&Play nabled**. Beforehand, it must be ensured that all IP devices are registered in the DLS database.

This does not use the backup file stored in the database, but the current backup file as it appears in the mask (which may have changed and not yet been saved).

ℹ When database mirroring (see Section 4.6, "SQL Database Mirroring Setup") is active, no restore of backups is possible.

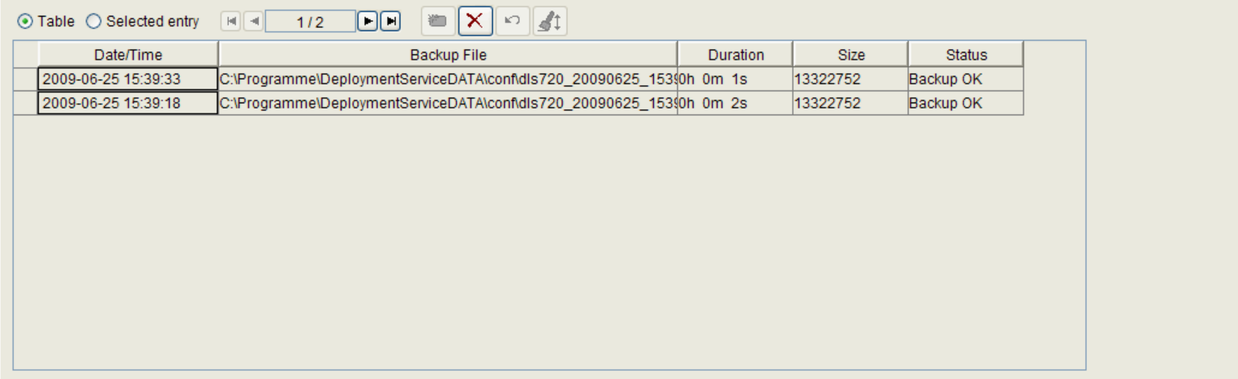
ℹ There are some basic server configuration data which will never be restored as e.g.
- the base configuration
- the license settings
in order to guarantee a proper operation after any restore.

ℹ During a restore, **all** users are momentarily disconnected from the DLS database as the restore process requires exclusive access to the database. These users must log on again.

6.6.3 "Protocol" Tab

Call: Main Menu > Administration > Backup/Restore > "Protocol" Tab

For more information, see Section 15.8.1.3, "Monitoring Backups".



● Table ○ Selected entry 1 / 2

Date/Time	Backup File	Duration	Size	Status
2009-06-25 15:39:33	C:\Programme\DeploymentServiceDATA\conf\dls720_20090625_153	0h 0m 1s	13322752	Backup OK
2009-06-25 15:39:18	C:\Programme\DeploymentServiceDATA\conf\dls720_20090625_153	0h 0m 2s	13322752	Backup OK

Date/Time

Backup time.

Backup File

Backup file name.

Duration

Duration of the backup process in hours, minutes, and seconds.

Size

Size of the backup file in bytes.

Status

Status of the backup/restore.

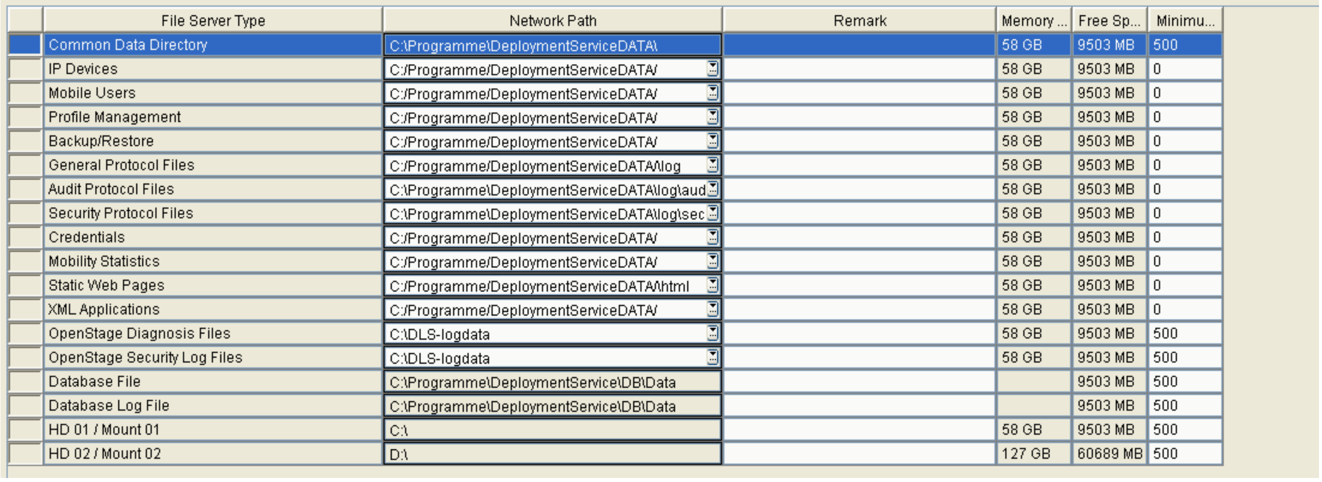
Possible values:

- **Backup OK**
- **Backup failed**
- **deleted**
- **Restore OK**
- **Restore failed**

6.7 File Server

Call: Main Menu > Administration > File Server

You can use this menu item to set the default network drives or local folders for saving DLS data.



	File Server Type	Network Path	Remark	Memory ...	Free Sp...	Minimu...
	Common Data Directory	C:\Programme\DeploymentServiceDATA\		58 GB	9503 MB	500
	IP Devices	C:/Programme/DeploymentServiceDATA/		58 GB	9503 MB	0
	Mobile Users	C:/Programme/DeploymentServiceDATA/		58 GB	9503 MB	0
	Profile Management	C:/Programme/DeploymentServiceDATA/		58 GB	9503 MB	0
	Backup/Restore	C:/Programme/DeploymentServiceDATA/		58 GB	9503 MB	0
	General Protocol Files	C:/Programme/DeploymentServiceDATA/\log		58 GB	9503 MB	0
	Audit Protocol Files	C:\Programme\DeploymentServiceDATA\log\aud		58 GB	9503 MB	0
	Security Protocol Files	C:\Programme\DeploymentServiceDATA\log\sec		58 GB	9503 MB	0
	Credentials	C:/Programme/DeploymentServiceDATA/		58 GB	9503 MB	0
	Mobility Statistics	C:/Programme/DeploymentServiceDATA/		58 GB	9503 MB	0
	Static Web Pages	C:/Programme/DeploymentServiceDATA/\html		58 GB	9503 MB	0
	XML Applications	C:/Programme/DeploymentServiceDATA/		58 GB	9503 MB	0
	OpenStage Diagnosis Files	C:\DLS-logdata		58 GB	9503 MB	500
	OpenStage Security Log Files	C:\DLS-logdata		58 GB	9503 MB	500
	Database File	C:\Programme\DeploymentService\DB\Data			9503 MB	500
	Database Log File	C:\Programme\DeploymentService\DB\Data			9503 MB	500
	HD 01 / Mount 01	C:\		58 GB	9503 MB	500
	HD 02 / Mount 02	D:\		127 GB	60689 MB	500

File Server Type

Defines which DLS data should be saved on this file server.

Possible values:

- **IP Devices**
- **Mobile Users**
- **Profile Management**
- **Backup/Restore**
- **Protocol Files**
- **Credentials**
- **Mobility Statistics**
- **Static web pages**
- **XML Applications**
- **Common Data Directory**
  This network path has been entered during installation of the DLS and cannot be changed by means of this mask.
- **OpenStage Diagnosis Files**
- **OpenStage Security Log Files**
- **Database File**
  Shows the path where the DLS database is stored. The network name is relative to the SQL server and cannot be changed by means of this mask. Available only on systems with Microsoft SQL Server as database.

- **Database Log File**
  Shows the path where the transaction log of the DLS database is stored. The network name is relative to the SQL server and cannot be changed by means of this mask. Available only on systems with database type Microsoft SQL Server.
- **DLS Audit Log Files**
- **DLS Security Log Files**
- **HD 01 / Mount 01**
  Shows either necessary devices with system data (on Linux based systems) or all available or mounted devices (on Windows based systems). The network path cannot be changed by means of this mask.
- **...**
- **HD 20 / Mount 20**
  Shows either necessary devices with system data (on Linux based systems) or all available or mounted devices (on Windows based systems). The network path cannot be changed by means of this mask.

Network Path

Network path or local folder for saving DLS data.
Example: `\\MyFileServer\DlsFiles\Protocols`

Remark

Field for general information.

Memory Capacity

Displays the overall memory capacity of this network drive in gigabytes.

Free Space

Displays the available space on this network drive in megabyte. If this value is lower than the **Minimum Free Space**, this field is marked with a yellow border.

Minimum Free Space

Enter the minimum free space that must remain, in megabytes. If the value of **Free Space** falls below this value, an alarm will be triggered corresponding to the alarm configuration (see Section 6.5, "Alarm Configuration").

Value range: **0** ... **15000**

0 = no check

Acquisition Time

Date and time of acquisition of the additional information about **Memory Capacity [GB]** and **Free Space [MB]**. These values are stored once a week; the entries cannot be deleted.

Only available in object view, cannot be changed or deleted.

Memory Capacity [GB]

Shows the memory capacity at **Acquisition Time**.

Only available in object view, cannot be changed or deleted. The value is stored once a week.

Free Space [MB]

Shows the free space at **Acquisition Time**.

Only available in object view, cannot be changed or deleted. The value is stored once a week.

6.8 Workpoint Interface Configuration

Call: Main Menu > Administration > Workpoint Interface Configuration

This area features the following components:

- Possible Action Buttons
- "Secure mode" Tab
- "DCMP" Tab
- "HTTP-Proxy" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Refresh

Refreshes the content of the relevant page.

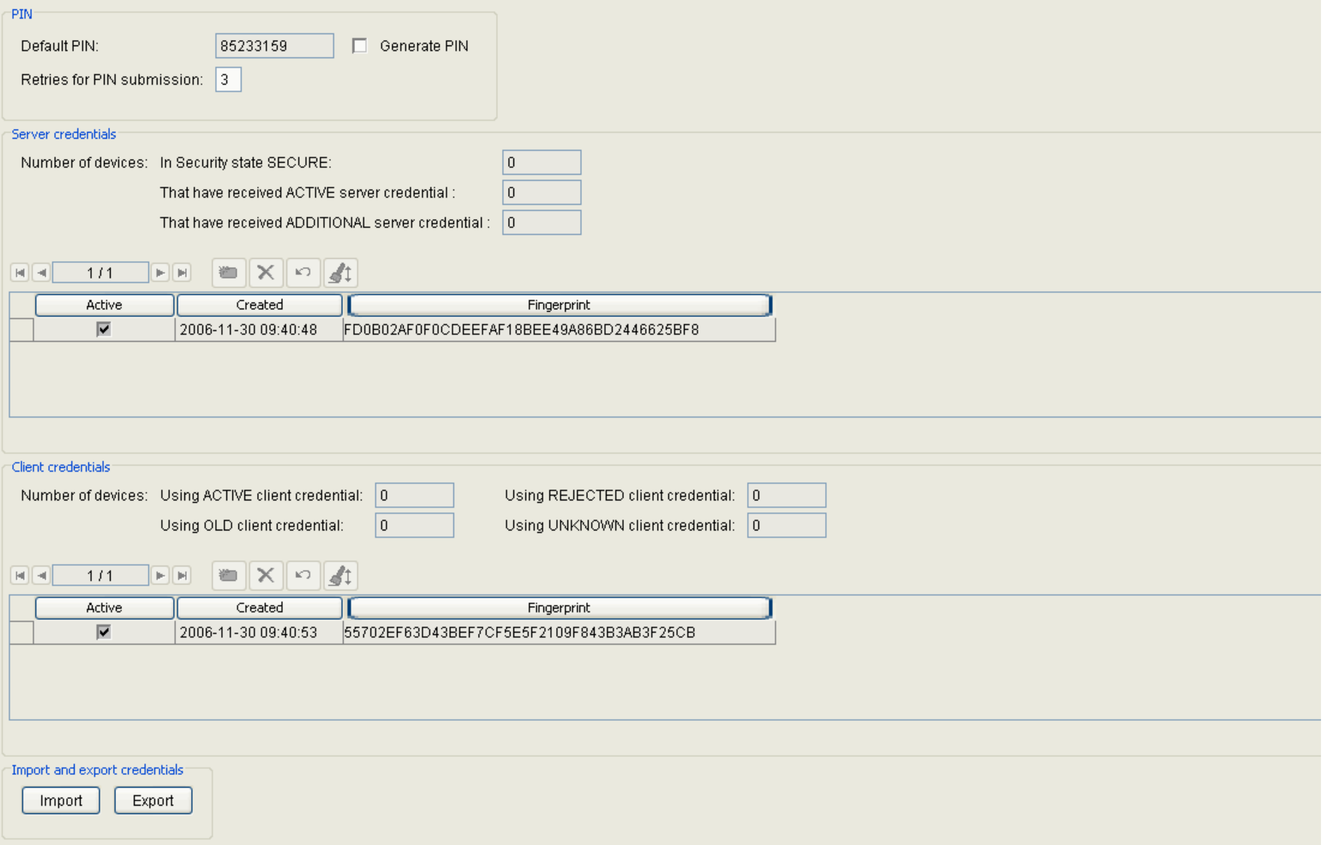
6.8.1 "Secure mode" Tab

Call: Main Menu > Administration > Workpoint Interface Configuration > "Secure mode" Tab

The components for secure communication (secure mode) between the DLS and IP Devices are configured here. Server credentials and client credentials are required for mutual authentication. You may also be asked to enter a PIN at the device.

> For smooth secure mode operation, please ensure that the time and date on the OpenStage phone conforms with that on the DLS.

> Secure mode is presently only available on OpenStage phones.



PIN

Default PIN: 85233159 ☐ Generate PIN

Retries for PIN submission: 3

Server credentials

Number of devices: In Security state SECURE: 0

That have received ACTIVE server credential : 0

That have received ADDITIONAL server credential : 0

1 / 1

Active	Created	Fingerprint
☑	2006-11-30 09:40:48	FD0B02AF0F0CDEEFAF18BEE49A86BD2446625BF8

Client credentials

Number of devices: Using ACTIVE client credential: 0 Using REJECTED client credential: 0

Using OLD client credential: 0 Using UNKNOWN client credential: 0

1 / 1

Active	Created	Fingerprint
☑	2006-11-30 09:40:53	55702EF63D43BEF7CF5E5F2109F843B3AB3F25CB

Import and export credentials

PIN

Default PIN:

PIN created automatically by DLS to allow encrypted transfer of server credentials to the IP Device. This PIN is used by IP Devices with the "Default PIN" mode.

Generate PIN

If this check box is activated and you click **Save**, DLS creates a new default PIN. This PIN or, optionally, an individual PIN must be entered at the IP Device to decrypt the server credentials delivered by DLS. The PIN is used by IP Devices with **Insecure** security status.

Retries for PIN submission:

Specifies the number of failed attempts permitted when entering the PIN at the IP Device.

Server Credentials

Number of devices:

In Security state SECURE:

Number of devices in the SECURE security status.

That have received ACTIVE server credential:

Number of devices that have received the active server credential.

That have received ADDITIONAL server credential:

Number of devices that have received the ADDITIONAL security credential.

Active

Displays whether a server credential is active or inactive. The DLS always authenticates itself on a device in secure mode using the active server credential.

A maximum of one additional server credential can be created in preparation for exchanging the active server credential.

Created

Time the credential was created.

Fingerprint

This fingerprint (hash value) uniquely identifies the credential (also in different DLS entities). The fingerprint is part of the name of the export file (see also the "Export" field).

New

Creates an additional (inactive) server credential. Only one additional server credential may be created.

Once an additional server credential is created, it is sent to all devices in secure mode. When this additional server credential has been activated, the devices can also be successfully authenticated on DLS.

Activate

Activates the additional (inactive) server credential. When activation is complete, DLS queries are denied by all devices to which this credential has not yet been sent.

Delete

Deletes the additional (inactive) server credential.

Client credentials

Number of devices:

Using ACTIVE client credential:

Number of (secure) devices that identify themselves using the active client credential.

Using OLD client credential:

Number of (secure) devices that identify themselves using an outdated client credential.

Using REJECTED client credential:

Number of (secure) devices whose client credential was denied. Credentials not found in the list are denied.

Using UNKNOWN client credential:

Number of (secure) devices in which the client credential used for identification is not known.

Active

Displays whether a client credential is active or outdated.

There is always exactly one active client credential. DLS also accepts devices that authenticate themselves using an outdated client credential. In this case, the device is automatically sent the current active client credential. The next time, it authenticates itself using the active client credential.

Created

Date the credential was created.

Fingerprint

Hash value for uniquely identifying the credential.

New

Creates a new client credential. This new client credential is automatically activated and the client credential previously active is deactivated and becomes outdated. When a new client credential is created, it is sent to all devices.

Delete

Deletes all inactive (outdated) client credentials. When the outdated client credentials have been deleted, DLS no longer accepts devices that identify themselves using an outdated client credential.

Import and export credentials

Import

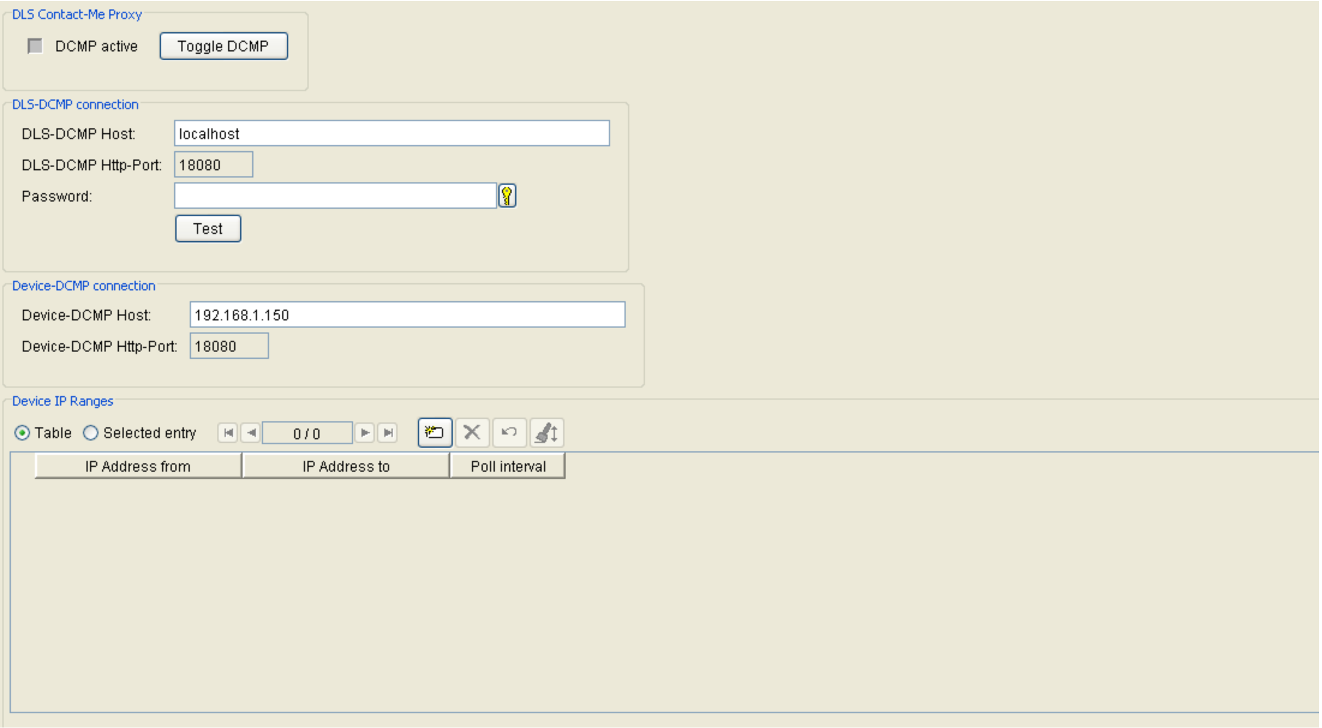
Imports client and server credentials from a password-protected file. This import replaces existing credentials.

Export

Exports client and server credentials to a file.

6.8.2 "DCMP" Tab

Call: Main Menu > Administration > Workpoint Interface Configuration > "DCMP" Tab



DLS Contact-Me Proxy

□ DCMP active

DLS-DCMP connection

DLS-DCMP Host: localhost

DLS-DCMP Http-Port: 18080

Password:

Device-DCMP connection

Device-DCMP Host: 192.168.1.150

Device-DCMP Http-Port: 18080

Device IP Ranges

● Table ○ Selected entry 0 / 0

IP Address from	IP Address to	Poll interval

DLS Contact-Me Proxy

DCMP active

Activates DCMP globally. When DCMP is globally deactivated, no devices can be reached via DCMP.

Toggle DCMP

Switches DCMP activation and creates jobs for affected devices.

DLS-DCMP connection

DLS-DCMP Host:

Host name or IP address of the DCMP server. The DCMP server host must be reachable for DLS.

DLS-DCMP HTTP-Port:

DCMP server’s HTTP port for connecting DLS and DCMP.

Password:

Password for DLS access to the DCMP server.

Test

Tests the connection between DLS and the DCMP server using the current values stored for host, port, and password. When you change these values, you must save the changes before testing the DLS connection.

Device-DCMP connection

Device-DCMP Host:

Host name or IP address of the DCMP server. The DCMP server host must be reachable for devices activated by DCMP. In contrast to the DCMP-DLS connection, do not use "localhost" or "127.0.0.1" as the DCMP server host when both are running on the same host.

Device-DCMP HTTP-Port

DCMP server’s HTTP port for connecting telephones and DCMP.

Device IP Ranges

IP Address from:

Lower limit of IP addresses that are administered by DCMP.

IP Address to:

Upper limit of IP addresses that are administered by DCMP

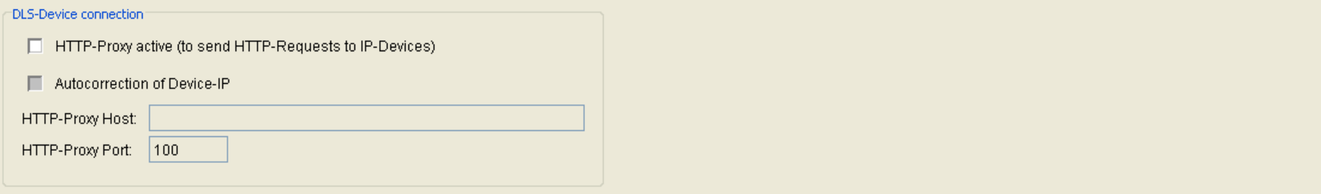
Poll Interval:

The time between two consecutive polls at DCMP (in minutes).

6.8.3 "HTTP-Proxy" Tab

Call: Main Menu > Administration > Workpoint Interface Configuration > "HTTP-Proxy" Tab

The settings made in this tab are necessary if the end devices can be reached by the DLS only via an HTTP proxy.



DLS-Device connection

□ HTTP-Proxy active (to send HTTP-Requests to IP-Devices)

□ Autocorrection of Device-IP

HTTP-Proxy Host:

HTTP-Proxy Port: 100

DLS-Device Connection

HTTP-Proxy active (to send HTTP-Requests to IP Devices)

If this checkbox is active, an HTTP proxy is used to send HTTP requests from the DLS to IP Devices.

Autocorrection of Device-IP

Automatic correction of the devices’ IP address with the request address (only if HTTP-Proxy is enabled). In case an HTTP proxy is used, this option is deactivated at first in order to avoid that the IP address of the devices is replaced with the IP address of the HTTP proxy. It is recommended not to activate this switch.

HTTP-Proxy Host

IP address or DNS name of the HTTP proxy to be used for sending HTTP requests from the DLS to the IP Devices.

HTTP-Proxy Port

Port of the HTTP proxy used to send HTTP requests from the DLS to IP Devices.

6.9 Automatic SPE Configuration

This area enables the automatical configuration of PKI based Signaling and Payload Encryption (SPE). This is especially useful when there is no client PKI.

The DLS supports the generation and deployment of CA Certificates (CA= Certificate Authority) for administered IP Devices (Gateways and end devices). When activating this CA Certificate for each administered gateway, a SPE certificate will be generated and deployed.

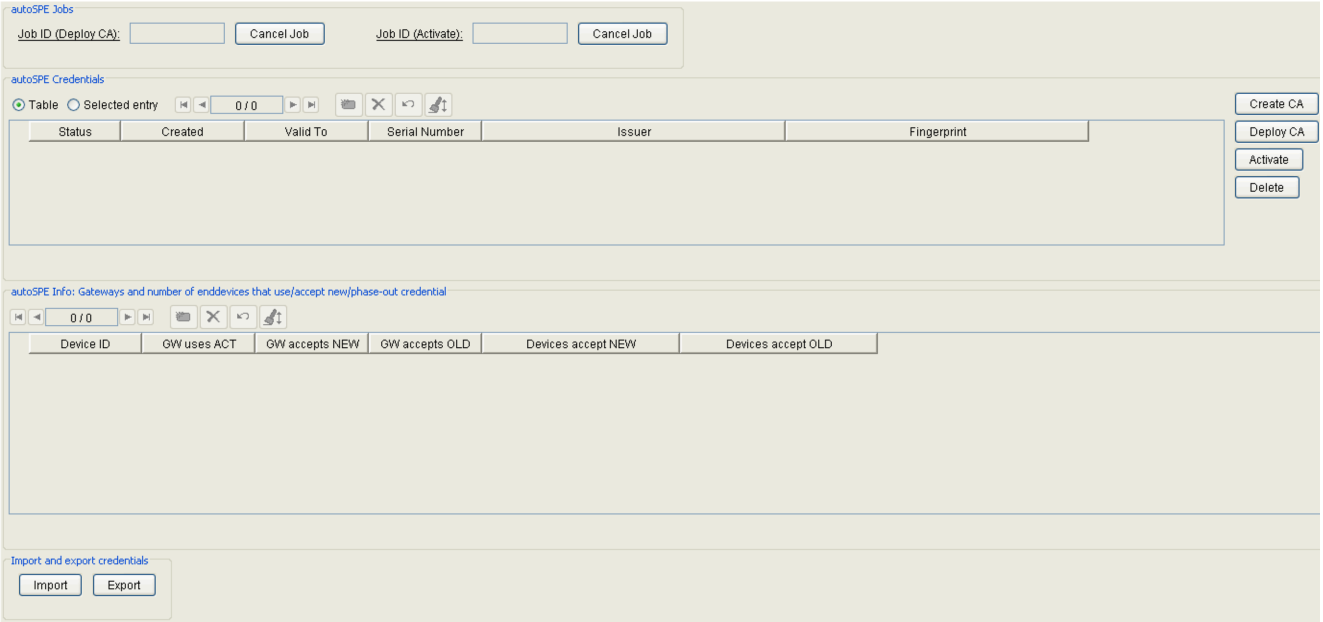
Via export and import, it is possible to migrate CA certificates from one DLS to another.

This area features the following components::

- Possible Action Buttons
- "CA Administration" Tab
- "Issuer Administration" Tab
- "Settings" Tab

6.9.1 "CA Administration" Tab

Call: Main Menu > Administration > Automatic SPE Configuration > "CA Administration" Tab



Status	Created	Valid To	Serial Number	Issuer	Fingerprint

Device ID	GW uses ACT	GW accepts NEW	GW accepts OLD	Devices accept NEW	Devices accept OLD

autoSPE Jobs

Job ID (Deploy CA)

For the deployment of CAs, a job is started. A unique job ID is assigned to this job in order to identify it. Via this field, it is possible to jump to the job control (see Section 14.1, "Job Control") to control the status of the job.

Job ID (Activate)

For the activation of CAs, a job is started. A unique job ID is assigned to this job in order to identify it. Via this field, it is possible to jump to the job control (see Section 14.1, "Job Control") to control the status of the job.

Cancel Job

With this button, the particular job can be canceled.

autoSPE Credentials

Status

Displays the status of the credential.

Possible values:

- **created**

- **deployed**
- **activated**
- **phase-out**

Created

Date of creation for the credential.

Valid to

Expiry date for new autoSPE credentials (possible maximum duration until 12/31/2037).

Serial number

Serial number for the CA certificate.

Issuer

Issuer of the credential.

Fingerprint

The fingerprint of CA certificate is unique and identifies the credential, also over disparate DLS instances. The fingerprint is also used as a part of the file name for export (see the **Export** button).

Create CA

Creates a new credential for SPE, i. e. first, a new CA certificate, and then, a certificate with this CA signature is created. the status of the new credential is "created".

Deploy CA

Deploays a new credential for SPE, that is, the CA certificate is distributed to the corresponding IP devices. The table is updated, and the status for the credential is changed to "deployed".

Activate

Activates a new credential for SPE, that is, the Ca certificate is distributed to the gateways. The table is update, and the status for the new credential is changed to "acitvated", while the status of the previously active credential is changed to "phase-out".

Delete

Deletes a credential that is no longer necessary, i. e. a credential in "created" or "deployed" status, or or the activated credential (in case only one credential exists) or the phase-out credential (in case more than one credential exist). After this, the table is updated.

autoSPE Info: Gateways and number of enddevices that use/accept new/phase-out credential

Device ID

Displays the device ID of the gateway.

GW usese ACT

GW uses NEW

Indicates whether the gateway uses the new credential, i. e. if the credential is activated.

Possible values:

- **yes**
- **no**

GW accepts NEW

Indicates whether the gateway accepts the new credential.

Possible values:

- **yes**
- **no**

GW accepts OLD

Indicates whether the gateway accepts the phased-out credential.

Possible values:

- **yes**
- **no**

Devices accept NEW

Shows the number of devices which accept the new credential, as well as the total number of devices connected to the gateway. Furthermore, the coverage in percent is displayed. Example: 3/5 (=60%) implies that three of five devices connected to the gateway accept the new credential, which is commensurate with 60%.

Devices accept OLD

Shows the number of devices which accept the phased-out credential, as well as the total number of devices connected to the gateway. Furthermore, the coverage in percent is displayed. Example: 3/5 (=60%) implies that three of five devices connected to the gateway accept the phase-out credential, which is commensurate with 60%.

Import und Export der Credentials

Import

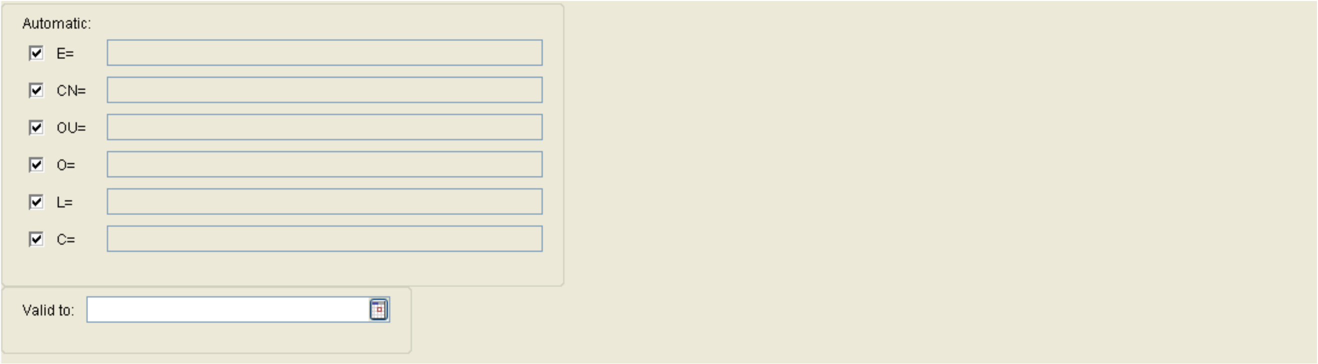
Reads the autoSPE credentials and the autoSPE configuration from a file and replaces the complete present autoSPE configuration including the deployment to the gateways and devices.

Export

Writes the current autoSPE configuration to a file. This can be used for backup purposes and for a migration to a different DLS.

6.9.2 "Issuer Administration" Tab

Call: Main Menu > Administration > Automatic SPE Configuration > "Issuer Administration" Tab



Automatic:

☑ E=

☑ CN=

☑ OU=

☑ O=

☑ L=

☑ C=

Valid to:

The data of the certificate issuer are administered here.

The user can either apply the default settings pre-defined in the DLS, or provide his own particulars. If the associated check box is activated, the default settings are applied; otherwise, the user specified data are applied.

Automatic

E=

E-Mail address of the issuer.

Example: **hipath_security_office@siemens.com**

CN=

Common Name of the issuer.

Example: **Siemens Enterprise Communication Security Office**.

OU=

Organizational Unit of the issuer.

Example: **Siemens Enterprise Systems**.

O=

Organization of the issuer.

Example: **Siemens Enterprise Communication GmbH & Co. KG**.

L=

Location of the issuer.

Example: **München**.

C=

Country of the issuer.

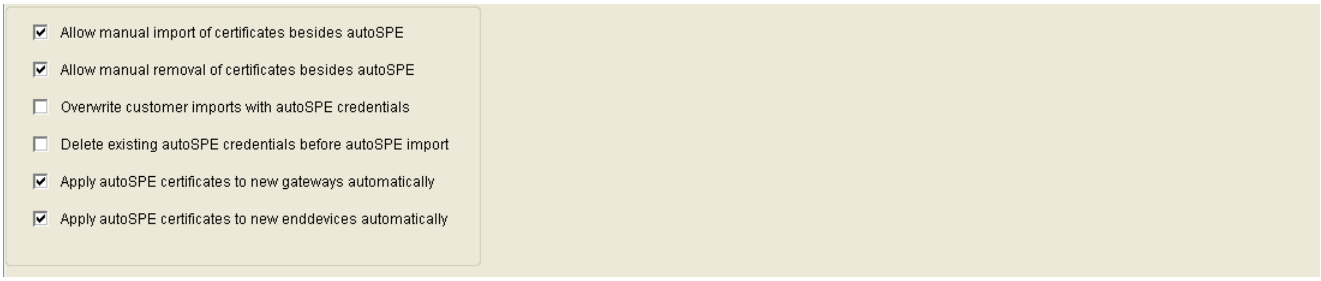
Example: **DE**.

Valid to

Maximum validity for new autoSPE credentials.

6.9.3 "Settings" Tab

Call: Main Menu > Administration > Automatic SPE Configuration > "Settings" Tab



☑ Allow manual import of certificates besides autoSPE

☑ Allow manual removal of certificates besides autoSPE

□ Overwrite customer imports with autoSPE credentials

□ Delete existing autoSPE credentials before autoSPE import

☑ Apply autoSPE certificates to new gateways automatically

☑ Apply autoSPE certificates to new enddevices automatically

Allow manual import of certificates besides autoSPE

If the check box is active, a certificate can be imported manually, f. e. if the deployment via autoSPE has failed.

Allow manual removal of certificates besides autoSPE

If the check box is active, a certificate can be removed manually.

> ⓘ Certificates that have been removed manually can only be re-imported manually.

Overwrite customer imports with auto SPE credentials

autoSPE handles up to 2 server-side CA certificates (index 0 and 1). However, up to 16 server-side CA certificates (index 0 to 15) can be imported by the user. If autoSPE is activated, it overwrites the indices 0 and 1 with its own CA certificates.

If the check box is active, the indices 2 to 15 are removed during this process. Otherwise, only the indices 0 and 1 are overwritten with autoSPE certificates, while the remaining indices are left untouched.

Delete existing autoSPE credentials during autoSPE import

All existing credentials will be deleted before an import.

Apply autoSPE certificates to new gateways automatically

If activated, new gateways will be provided automatically with existing autoSPE Certificates. Otherwise, gateways will be supported with certificates via **IP Devices** > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)** > **Import Certificate**.

Apply autoSPE certificates to new enddevices automatically

If activated, new enddevices will be provided automatically with existing autoSPE certificates. Otherwise, enddevices will be supported with certificates via **IP Devices** > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)** > **Import Certificate**.

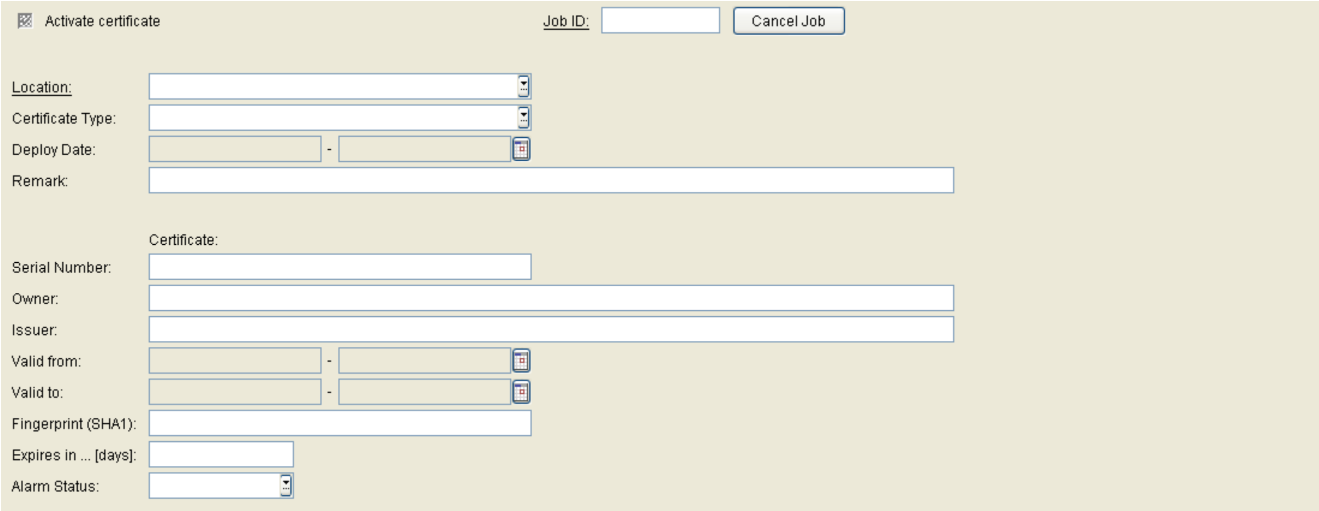
6.10 Automatic Certificate Deployment

Call: Main Menu > Administration > Automatic Certificate Deployment

This area provides the possibility to set up a certificate deployment schedule by assigning certificates to existing locations, i.e. a set of IP phones, and run scheduled jobs to deploy these certificates automatically.

It is possible to prevent autodeployment for an IP phone by enabling the **Automatic Certificate Deployment disabled** checkbox in **IP Devices** > **IP Device Management** > **IP Device Configuration**.

> To remove the certificates from all IP phones of a location, deploy an empty certificate.



Activate certificate

The certificate will be activated for automatic certificate deployment. After activation, the Jobs corresponding to the devices will be generated. Activated entries cannot be changed.

A certificate deployment task will be stopped/deactivated by unsetting this check box. The jobs already generated but not executed (state: active or running) will not be cancelled. To cancel all jobs belonging to a task, press the **Cancel Job** button. The certificate relating to this task will no longer be deployed to newly registered IP Devices.

Job ID:

For the activation of certificates, a job is started. A unique job ID is assigned to this job in order to identify it. Via this field, it is possible to jump to the job control (see Section 14.1, "Job Control") to control the status of the job.

Cancel Job

With this button, all jobs belonging to this certificate deployment task with active or running status will be cancelled.

Location:

Location where the certificate deployment will be executed. Locations can be assigned as described under Section 6.2.2, "Location".

Certificate Type:

Type of certificate.

Possible options:

- **RADIUS Server CA Certificate 1**
- **RADIUS Server CA Certificate 2**
- **Phone Certificate**

Deploy Date:

Date when certificate deployment will be started.

Remark:

Remark (free text).

Certificate:

The following certificate parameters are displayed only.

Serial Number:

Serial number of the certificate.

Owner:

Owner of the certificate.

Issuer:

Issuer of the certificate.

Valid from:

The certificate will be valid from this point in time.

Valid to:

The certificate will be valid until this point in time.

Fingerprint (SHA1):

Test algorithm SHA1 (160 bits/20 characters) for the security certificate.

Expires in [days]:

The certificate expires in ... days.

Alarm Status:

Current alarm status of imported certificate.

Possible values:

- **valid**
- **soon running out**
- **expired**

6.11 Automatic Archiving

Call: Main Menu > Administration > Automatic Archiving

This feature enables the user to archive the data of selected IP devices in a time-controlled manner. The archived data will be stored in a .zip-file. If the file is not present, it will be created during the 1st archiving of data; if it is already present, the archive data will be added to this existing .zip-archive. For each IP Device that is to be archived, a proper file will be allocated within the .zip archive.

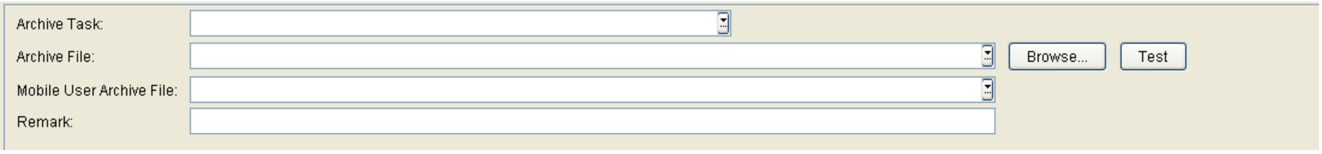
Each new archive entry overwrites an already existing entry for the same IP Device without notification. History data (backups of an already existing file of the .zip archive) will be kept where the maximum number of kept history data can be specified by setting **Maximum Number of Backup Archive Files** within the "Settings" Tab.

The archived data can be retrieved via the screen **Administration** > **Automatic Archiving** > **Action 'Load IP Device from Archive'**.

This area features the following components:

- General Data
- Possible Action Buttons
- "Settings" Tab
- "IP Devices to archive" Tab
- "Mobile Users to archive" Tab
- "Protocol" Tab

General Data



Archive Task:	
Archive File:	
Mobile User Archive File:	
Remark:	

Archive Task

Name of the archive task.

Archive File

Filename and directory path for the archive file on the DLS Server. If the file is not present, it will be created during the first archiving of data; if it is already present, the archive data will be added to the existing .zip-archive.

Mobile User Archive file

Filename and directory path for the archive file on the DLS Server. The file name will be derived from **Archive File** and cannot be changed.

Remark

Remark on archive task.

Browse...

Select excisting archive path. Path name and filename will be written to the archive file. Only directories can be searched, not particular files.

Test

Test if the file is accessible.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the Search view before new search criteria are entered.

Save

Starts a job for distributing the configuration changes. For more information, see Section 15.1,

"First Steps: Changing IP Device Parameters".

Discard

The modifications carried out in the mask are discarded.

Export File

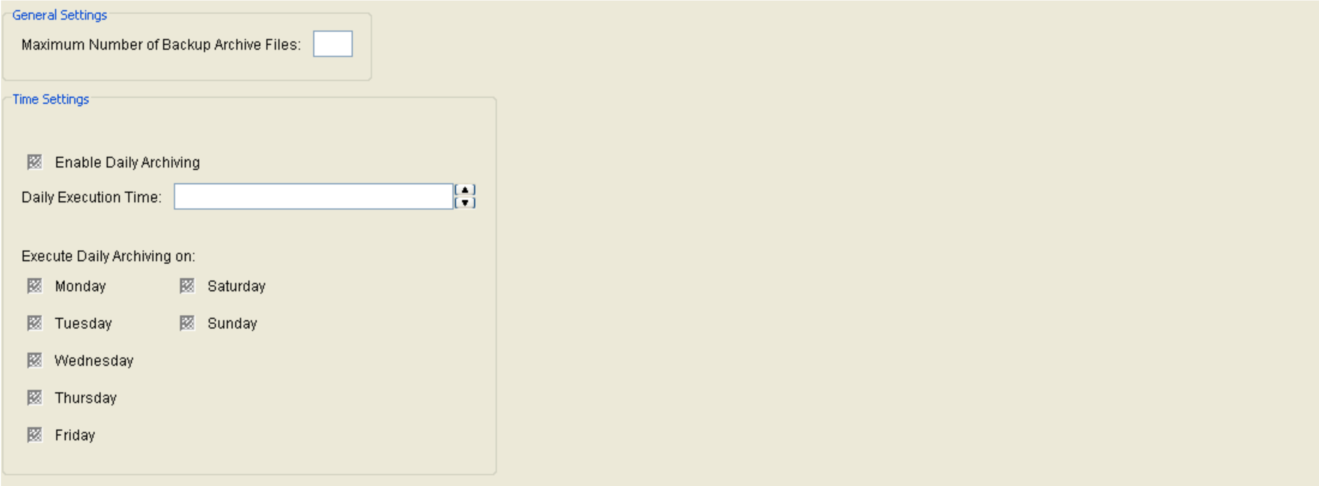
The inventory data are exported into a csv formatted file.

Refresh

Refreshes the window contents from the database.

6.11.1 "Settings" Tab

Call: Main Menu > Administration > Automatic Archiving > "Settings" Tab



General Settings

Maximum Number of Backup Archive Files:

Time Settings

☒ Enable Daily Archiving

Daily Execution Time:

Execute Daily Archiving on:

☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☒ Saturday
☒ Sunday

General Settings

Maximum Number of Backup Archive Files

Contains the number of backup files to be created for file history, if the original archive file is overwritten.

Time Settings

Enable daily Archiving

Activates daily archiving of IP Devices .

Daily Execution Time

Time of day at which the archiving is started.

> Switching from daylight saving time to regular time (one hour back) will not lead to a second execution of a job that has been started in the time interval hereby doubled. When switching from regular time to daylight saving time (one hour advance), a job which is scheduled for this skipped time will not be executed.

Execute Daily Archiving on:

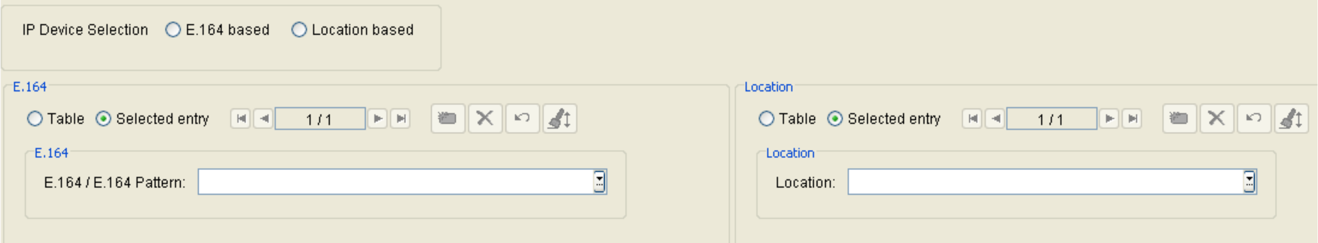
Restricts Archiving to specific days of the week.

Archive now

Starts archiving immediately without any regards to settings for automatic archive. The archive will be saved to the **Archive File** currently displayed.

6.11.2 "IP Devices to archive" Tab

Call: Main Menu > Administration > Automatic Archiving > "IP Devices to archive" Tab



IP Device Selection

E.164 based

Selection of IP Devices to be archived by E.164 number.

Location based

Selection of IP Devices to archive by location.

E.164

E.164 /E.164 Pattern

Entire E.164 number or a range of E.164 numbers partly qualified with '*', e.g. 31* (= all E.164 numbers, starting with 31...).

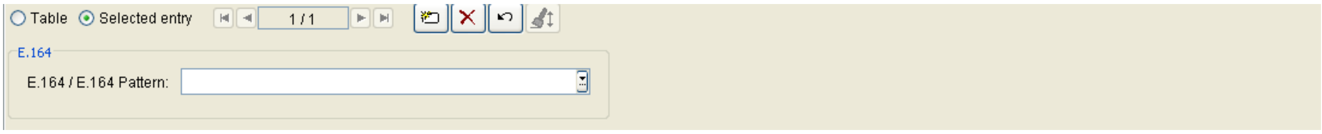
Location

Location

Select a defined location. ’Default Location’ cannot be selected.

6.11.3 "Mobile Users to archive" Tab

Call: Main Menu > Administration > Automatic Archiving > "Mobile Users to archive" Tab



E.164

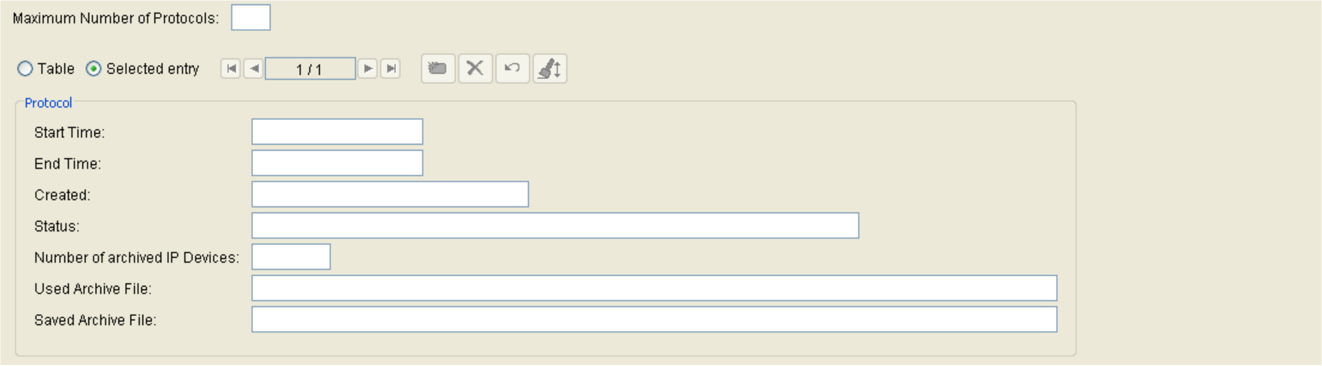
E.164 / E.164 Pattern:

A complete E.164 number or a range of numbers partly qualified with ’*’ can be entered here.

Example: **31*** = all E.164 numbers that begin with 31.

6.11.4 "Protocol" Tab

Call: Main Menu > Administration > Automatic Archiving > "Protocol" Tab



Maximum Number of Protocols:

○ Table ● Selected entry 1 / 1

Protocol

Start Time:

End Time:

Created:

Status:

Number of archived IP Devices:

Used Archive File:

Saved Archive File:

Protocol

Maximum Number of Protocols:

Each protocol entry can be deleted manually or will be deleted automatically according to the number entered here.

Start Time

Start Time of archiving.

End Time

End Time of archiving.

Created

Displays whether it is an automatic or a manual archive task.

- **Manual**
- **Timer triggered**

Status

Status of archiving.

Possible values:

- **Archive Task successful**
- **Archive Task failed**
- **Old Protocol entries automatically deleted**

Number of archived IP Devices

Number of archived IP Devices.

Used Archive File

Filename of the currently used archive file.

Saved Archive File

Filename of the latest saving of the archive file.

6.12 Automatic Upload Diagnosis- and Security Log Files

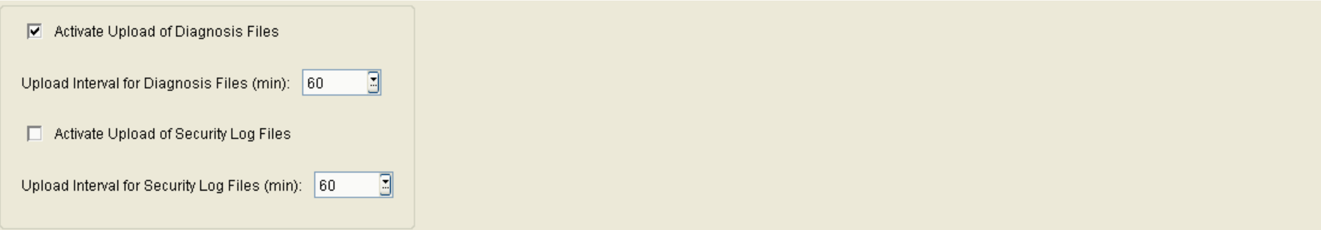
Call: Main Menu > Administration > Automatic Upload Diagnosis- and Security Log Files

This area enables the user to upload scheduled diagnosis- and security log files of selected IP Devices. The uploaded file will be stored on a network drive. The path is defined in **Main Menu** > **Administration** > **File Server** > **OpenStage Diagnosis Files** or **OpenStage Security Log Files**.

This area features the following components:

- General Data
- Possible Action Buttons
- "Protocol" Tab

General Data



☑ Activate Upload of Diagnosis Files

Upload Interval for Diagnosis Files (min): 60

☐ Activate Upload of Security Log Files

Upload Interval for Security Log Files (min): 60

Activate Upload of Diagnosis Files

When active, diagnosis files of selected IP Devices are uploaded.

Upload Interval for Diagnosis Files (min)

Determines the time between two upload jobs (in minutes).

Possible Options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**
- **240**

Default value: **60**

Activate Upload of Security Log Files

When active, security log files of selected IP Devices are uploaded.

Upload Interval for Security Log Files (min)

Determines the time interval between two upload jobs (in minutes).

Possible Options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**

- **120**
- **240**

Default value: **60**

Possible Action Buttons

Depending on the selected view and DLS state, various possible action buttons are available.

Save

Saves all settings made.

Discard

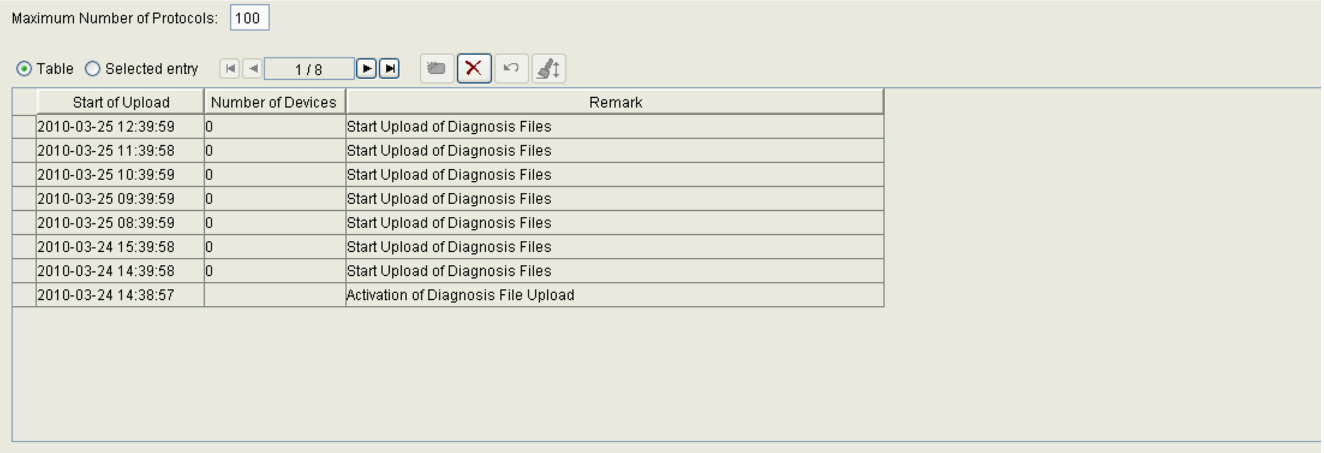
Discards any changes entered.

Refresh

Updates the window using the database.

6.12.1 "Protocol" Tab

Call: Main Menu > Administration > Automatic Upload Diagnosis- and Security Log Files > "Protocol" Tab



Maximum Number of Protocols: 100

Start of Upload	Number of Devices	Remark
2010-03-25 12:39:59	0	Start Upload of Diagnosis Files
2010-03-25 11:39:58	0	Start Upload of Diagnosis Files
2010-03-25 10:39:59	0	Start Upload of Diagnosis Files
2010-03-25 09:39:59	0	Start Upload of Diagnosis Files
2010-03-25 08:39:59	0	Start Upload of Diagnosis Files
2010-03-24 15:39:58	0	Start Upload of Diagnosis Files
2010-03-24 14:39:58	0	Start Upload of Diagnosis Files
2010-03-24 14:38:57		Activation of Diagnosis File Upload

Maximum Number of Protocols:

Each protocol entry can be deleted manually or will be deleted automatically according to the number entered here.

Start of Upload

Displays the upload's starting time.

Number of Devices

Displays the number of handled IP Devices.

Remark

Remark on the upload.

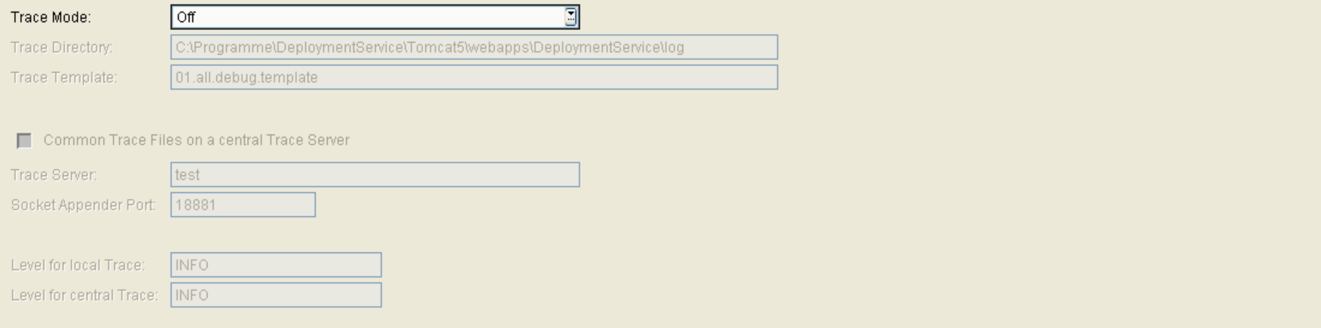
6.13 Trace Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "Additional Settings and Actions" Tab
- "Repeat filter" Tab
- "Message Filter" Tab
- "Filter test" Tab

General Data

Call: Main Menu > Administration > Trace Configuration



Trace Mode: Off

Trace Directory: C:\Programme\DeploymentService\Tomcat5\webapps\DeploymentService\log

Trace Template: 01.all.debug.template

☐ Common Trace Files on a central Trace Server

Trace Server: test

Socket Appender Port: 18881

Level for local Trace: INFO

Level for central Trace: INFO

You can use this menu item to configure trace operations. The settings are stored in the DLS database. A timer monitors if there are any new entries in the database. If so, the trace is modified accordingly; where applicable, changes are also transferred to the other servers in a cluster.

> The changes take effect after approximately two minutes.

> Individual settings can restrict the options available in the menu **Administration** > **Display Logging Data**.

For information on general interface operation, see Section 5.4.2, "Work Area".

Trace Mode

Option for selecting the trace mode.

Possible values:

- **Off**
  No special traces are performed. All error messages will be written to a default tracefile. This is the default setting after installation.
- **DLS Server**
  The trace is performed in the DLS server with the assigned **Level for local Trace**.
- **DLS Communication**
  Communication between IP devices and DLS server is traced with the assigned **Level for local Trace**. Additionally all error messages will be written to the default tracefile.
- **Log4j Template**
  The trace is performed with the predefined trace template selected under **Trace Template**.

Trace Directory

Directory in which the trace files are stored.

Trace Template

Option for selecting predefined trace settings. The trace templates are stored in the file directory `<drive>:\Program Files\DeploymentService\Tomcat5\webapps\DeploymentService\log\templates`. The settings in the templates are only effective if the **Trace Mode** "Log4j Template" is set.

Possible values:

- **01.all.debug.template**
  Log all DLS activities with DEBUG logging level.
- **02.all.info.template**
  Log all DLS activities with INFO logging level.
- **03.default.template**
  Default setting. Log all DLS activities with ERROR logging level.
- **04.gateway.template**
  Log all gateway activities with DEBUG logging level.
- **05.gateway.wpcomm.details.template**
  Log all gateway activities including communication between workpoint and DLS with DEBUG logging level.
- **06.gateway.wpcomm.info.template**
  Log all gateway activities including communication between workpoint and DLS with DEBUG logging level.
- **07.keyexchange.template**
  Log all gateway and key distribution activities with DEBUG logging level.
- **08.keyexchange.wpcomm.details.template**
  Log all gateway and key distribution activities including communication between workpoint and DLS with DEBUG logging level.
- **09.keyexchange.wpcomm.info.template**
  Log all gateway and key distribution activities including communication between workpoint with DEBUG logging level.
- **10.wpcomm.details.template**
  Log communication between workpoint and DLS with DEBUG logging level.
- **11.wpcomm.short.template**
  Log communication between workpoint and DLS with INFO logging level.
- **12.wpscan.wpcomm.details.template**
  Log all workpoint-based scan activities including communication between workpoint and DLS with DEBUG logging level.
- **13.wpscan.wpcomm.short.template**
  Log all workpoint-based scan activities including communication between workpoint and DLS with INFO logging level.

- **14.dlsapi.template**
  Log all DLS API methods with DEBUG logging level.
- **15.auth.debug.template**
  Log all authentication activities including communication between workpoint and DLS with DEBUG logging level.
- **16.nodb.debug.template**
  Log all DLS activities with the exception of database activities including communication between workpoint and DLS with DEBUG logging level.
- **17.pp.em.debug.template**
  Log all Plug&Play and element manager related activities with DEBUG logging level.

Common Trace Files on a central Trace Server

Traces of all nodes in a cluster are written to a file on a central server. The files `dlswpcommunication.*.txt`, `dlslog.*.txt`, and `dlserror.*.txt` are created.

Trace Server

Server where the common trace files are stored.

Socket Appender Port

Number of ports used for sending the common trace data to a node within the cluster.
Default value: **18881**.

Level for local Trace

Trace level setting for local traces in the DLS server. The hierarchy of trace levels is DEBUG < INFO < WARN < ERROR < FATAL, that is, if DEBUG is set, all other levels are also logged. If the diagnostic settings are controlled with a template, the value set there for this parameter has precedence.

Possible values:

- **DEBUG**
  Comprehensive trace of processes.
- **INFO**
  Selected process information.
- **WARN**
  Displays potential problems.
- **ERROR**
  Displays problems that do not cause the deployment service to fail.
- **FATAL**
  Displays problems that cause the deployment service to fail.

Level for central Trace

Trace level for common traces on a trace server within the cluster. If the diagnostic settings are controlled with a template, the value set there for this parameter has precedence.

Possible values:

- **INFO**
  Selected process information.
- **WARN**
  Displays potential problems.
- **ERROR**
  Displays problems that do not cause the deployment service to fail.
- **FATAL**
  Displays problems that cause the deployment service to fail.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Save

Saves any unsaved changes.

Discard

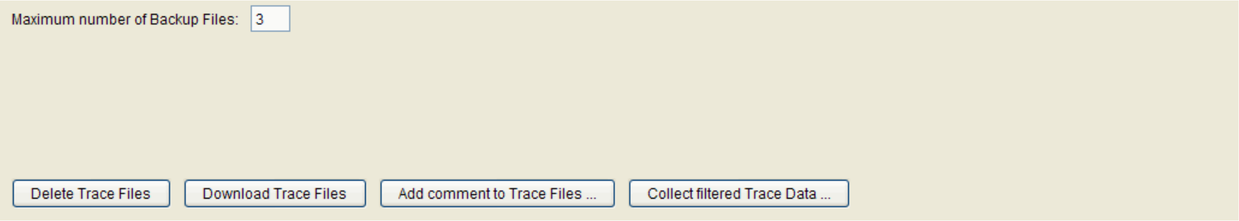
Discards any unsaved changes.

Refresh

Refreshes the content of the relevant page.

6.13.1 "Additional Settings and Actions" Tab

Call: Main Menu > Administration > Trace Configuration > "Additional Settings and Actions" Tab



Maximum number of Backup Files: 3

Delete Trace Files
Download Trace Files
Add comment to Trace Files ...
Collect filtered Trace Data ...

Maximum Number of Backup Files

Maximum number of backups per trace files.

Value range: **1** - **999**

Delete Trace Files

Delete all trace files.

Download Trace Files

Download all trace files in a .zip-file to a local path.

> If you use Microsoft Internet Explorer, **Automatic prompting for file downloads** has to be enabled. To achieve this, go to **Tools** > **Internet Options...** > **Tabsheet "Security"**. Here, select the web content zone the DLS server address belongs to and press **Custom Level**. In the **Security Settings** popup window, under **Downloads**, you can find the option mentioned above.

Add comment to Trace Files ...

Insert a comment in all trace files.

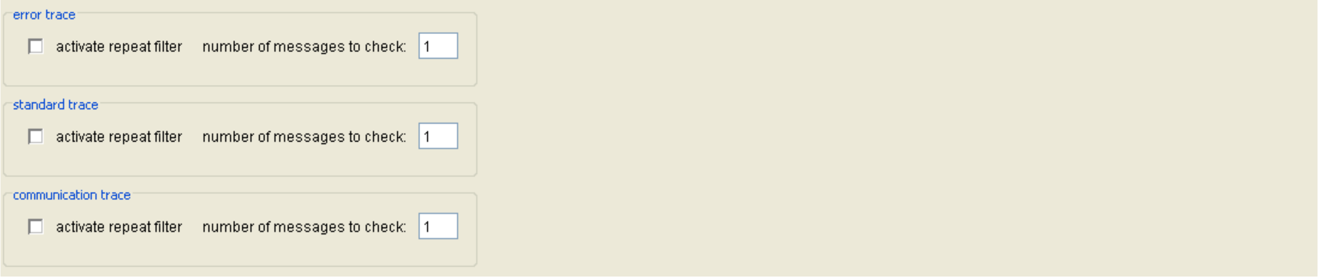
Collect filtered Trace Data ...

This function filters trace files already generated trace files (`dlslog.txt` and `dlsWpCommunication.txt`) according to certain filter criteria: E.164 numbers, IP addresses, or device IDs. A combination of criteria is not possible. These filter criteria are requested in a popup window. Data records which match a filter criterion are stored in an particular trace file. By clicking **Download Trace Files**, the files created are displayed. The generated files receive the following names: `<filter criterion>_FILTERED_dlslog.txt` and `<filter criterion>_FILTERED_dlsWpCommunication.txt`. With **Delete Trace Files**, these files can be deleted.

6.13.2 "Repeat filter" Tab

> By applying this function, messages which are required for analysis might possibly be lost. Therefore, it should be used with care, preferably only by request of the DLS support team.

Call: Main Menu > Administration > Trace Configuration > "Repeat filter" Tab



error trace

□ activate repeat filter number of messages to check: 1

standard trace

□ activate repeat filter number of messages to check: 1

communication trace

□ activate repeat filter number of messages to check: 1

Error trace

Activate repeat filter

When activated, repetitions of messages in the error trace are filtered out. The context range, within which repetitions are searched, is specified in the **Number of messages to check** parameter.

Number of messages to check

Size of a block of sequenced messages in the error trace, within which repetitions shall be filtered out.

Standard trace

Activate repeat filter

When activated, repetitions of messages in the standard trace are filtered out. The context range, within which repetitions are searched, is specified in the **Number of messages to check** parameter.

Number of messages to check

Size of a block of sequenced messages in the standard trace, within which repetitions shall be filtered out.

Communication trace

Activate repeat filter

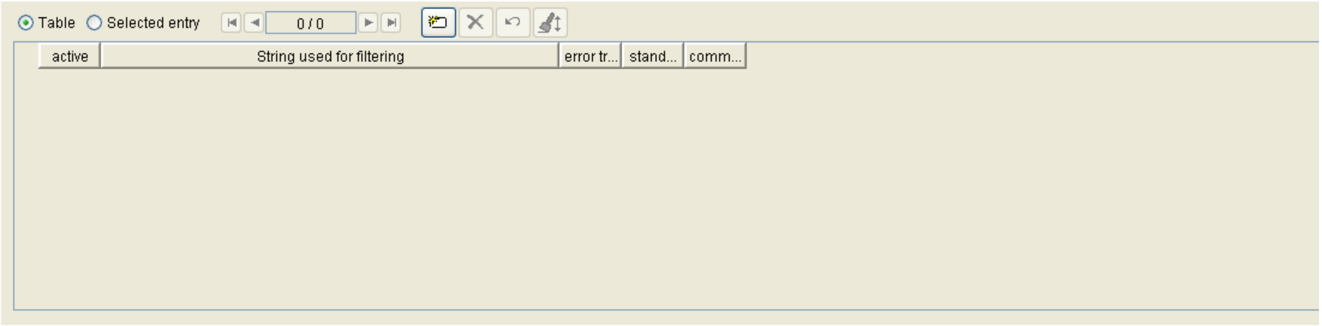
When activated, repetitions of messages in the communication trace are filtered out. The context range, within which repetitions are searched, is specified in the **Number of messages to check** parameter.

Number of messages to check

Size of a block of sequenced messages in the communication trace, within which repetitions shall be filtered out.

6.13.3 "Message Filter" Tab

Call: Main Menu > Administration > Trace Configuration > "Message Filter" Tab



active	String used for filtering	error tr...	stand...	comm...

active

Filter is switch off and on.

String used for filtering

Filter according to entered string.

Error trace

If active, this string is valid for error trace filtering.

Standard trace

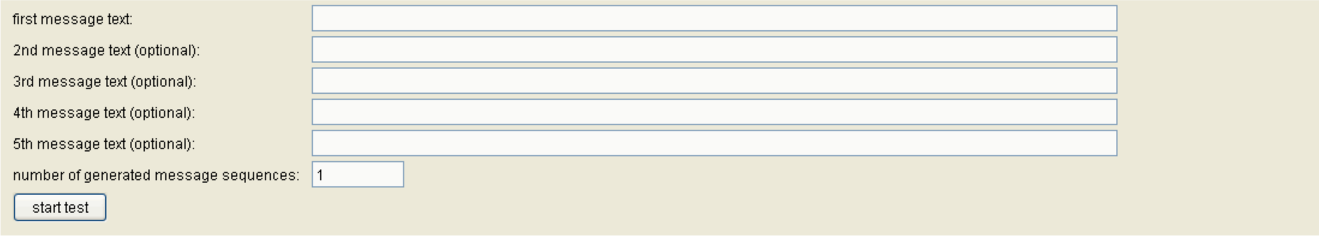
If active, this string is valid for standard trace filtering.

Communication trace

If active, this string is valid for communcation trace filtering.

6.13.4 "Filter test" Tab

Call: Main Menu > Administration > Trace Configuration > "Filter test" Tab



first message text:

2nd message text (optional):

3rd message text (optional):

4th message text (optional):

5th message text (optional):

number of generated message sequences: 1

1st message text

String as test message for testing the configured filters.

2nd message text (optional)

Additional string for testing the configured filters; appears as a separate message.

3rd message text (optional)

Additional string for testing the configured filters; appears as a separate message.

4th message text (optional)

Additional string for testing the configured filters; appears as a separate message.

5th message text (optional)

Additional string for testing the configured filters; appears as a separate message.

Number of generated message sequences

Defines how often the defined test messages shall be generated.

Start Test

The test messages are generated and filtered. The results appear in the traces.

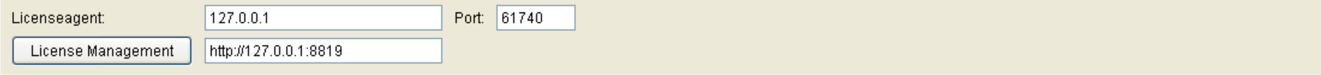
6.14 Server Licenses

This area features the following components:

- General Data
- Possible Action Buttons
- "License state" Tab
- "Multiple DLS Servers" Tab

General Data

Call: Main Menu > Administration > Server Licenses



Licenseagent: 127.0.0.1 Port: 61740

http://127.0.0.1:8819

Licenseagent

IP address or host name of license agent.

Port

Port number for access to the license server.

License Management

URL of the license server. Press the adjacent **License Management** action button to open the License Management Web interface in a separate window.

Possible Action Buttons

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

Updates the window using the database.

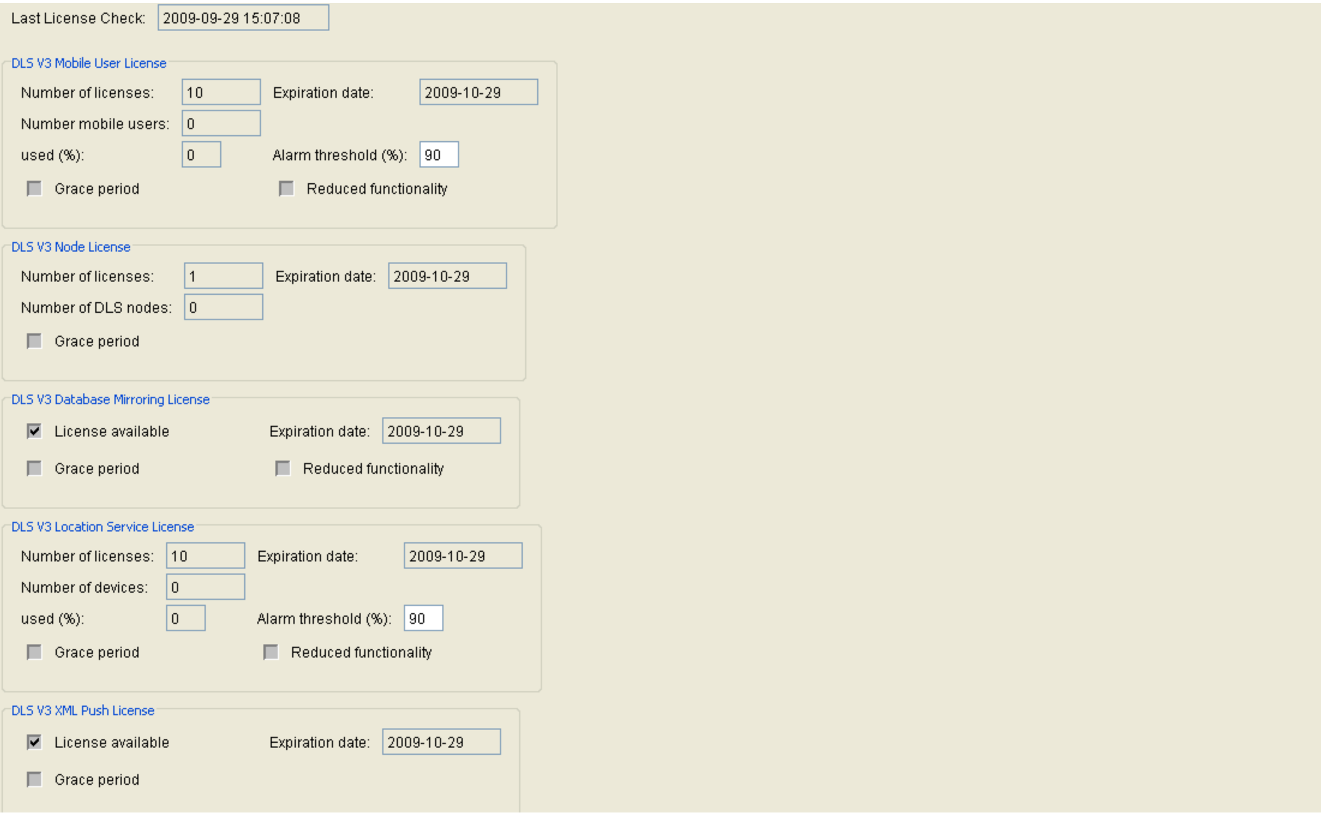
Export Licenses

Issue renewed request for available licenses from the license agent.

6.14.1 "License state" Tab

Call: Main Menu > Administration > Server Licenses > "License state" Tab

The current status of various licenses is displayed here.



Last License Check: 2009-09-29 15:07:08

DLS V3 Mobile User License

Number of licenses: 10 Expiration date: 2009-10-29
Number mobile users: 0
used (%): 0 Alarm threshold (%): 90
□ Grace period □ Reduced functionality

DLS V3 Node License

Number of licenses: 1 Expiration date: 2009-10-29
Number of DLS nodes: 0
□ Grace period

DLS V3 Database Mirroring License

☑ License available Expiration date: 2009-10-29
□ Grace period □ Reduced functionality

DLS V3 Location Service License

Number of licenses: 10 Expiration date: 2009-10-29
Number of devices: 0
used (%): 0 Alarm threshold (%): 90
□ Grace period □ Reduced functionality

DLS V3 XML Push License

☑ License available Expiration date: 2009-10-29
□ Grace period

Last License Check

Date and time of the last license scan at the license agent are displayed.

DLS V3 Mobile User License

Number of licenses

Indicates the number of mobile users that can be configured with the current license.

Expiration date

An expiration date is displayed when working with a demo license (grace period). This is the case, for example, when the CLA (license agent) is not or no longer available. A license awarded by the CLA is not limited in time.

No more DLS administration is possible after this date. Please contact your license administrator.

Number mobile users

Indicates the number of mobile user licenses already in use for mobile users.

used (%)

Indicates the number of licenses already in use as a percentage.

Alarm threshold (%)

Specify the used-license percentage that should generate a license alarm.

Grace period

This box is selected if you are unable to contact the CLA. The last license determined is then used. If the CLA has not yet been reached, 10 mobile user licenses are available. The DLS tries to contact the CLA every 45 minutes. No more administration of mobile users is possible when the term specified in the **Expiration date** field expires. Please contact your license administrator.

Reduced functionality

This check box is automatically selected if the number of licenses has been exceeded. In this case, the only option available is to delete mobile users.

Please contact your license administrator.

DLS V3 Node License

Number of licenses

Indicates the number of DLS V2 Node Licenses.

Number of DLS nodes

Indicates the number of additional active DLS Nodes in a cluster. With Single-Node mode, 0 is displayed here.

Expiration date

An expiration date is displayed when working with a demo license (grace period). This is the case, for example, when the CLA (license agent) is not or no longer available. A license awarded by the CLA is not limited in time.

After this date, DLS operation in cluster mode will no longer be possible. Please contact your license administrator.

Grace period

Checked if license is granted although CLA is not available. The license which was determined last is then used. If the CLA has not yet been reached, 1 DLS node license is available for the grace period. The DLS tries to contact the CLA every 45 minutes. Only Single-Node mode is possible when the term specified in the **Expiration date** field expires. Please contact your license administrator.

DLS V3 Database Mirroring License

License available

License for Database Mirroring available

Expiration date

An expiration date is displayed when working with a demo license (grace period). This is the case, for example, when the CLA (license agent) is not or no longer available. A license awarded by the CLA is not limited in time.

After this date, database mirroring will no longer take place. Please contact your license administrator.

Grace period

If checked, license is granted although licenseagent is not available. The last license determined is then used. If the CLA has not yet been reached, no database mirroring is available. The DLS tries to contact the CLA every 45 minutes.

No database mirroring will take place when the date in the **Expiration date** field expires. Please contact your license administrator.

Reduced functionality

This check box is automatically selected if the number of licenses has been exceeded. In this case, no database mirroring will be performed.

Please contact your license administrator

DLS V3 Location Service License

> This license is necessary to use the function 'Open Communications Solution for Location and Identity Assurance' (OCS LIA).

Number of Licenses

Indicates number of licenses for the Location Service (IP Infrastructure).

Number of devices

Number of IP Devices, supplied with IP Infrastructure data by means of Location Service.

used (%)

Percentage of used Location Service Licenses.

Alarm threshold (%)

Specifies at which percentage of used licenses an alarm shall be generated.

Expiration date

An expiration date is displayed when working with a demo license (grace period). This is the case, for example, when the CLA (license agent) is not or no longer available. A license awarded by the CLA is not limited in time.

After this date IP Devices will not be supplied with IP Infrastructure data, except emergency Call, by means of Location Service. Please contact you license administrator.

Grace period

Checked if the CLA is unreachable. The licenses determined last are then used. If the CLA has not yet been reached, 1 DLS node license will be available for the grace period. The DLS tries to contact the CLA every 45 minutes. When the term specified in the Expiration date field expires, the IP Devices will not be supplied with IP Infrastructure data, except Emergency Call, by means of Location Service. Please contact your license administrator.

Reduced functionality

This check box is automatically selected if the number of licenses has exceeded. In this case, the only option available is to delete IP Devices.

Please contact your license administrator

DLS V3 XML Push License

License available

XML Push can only be used with a valid license.

Expiration date

An expiration date is displayed when working with a demo license (grace period). This is the case, for example, when the CLA (license agent) is not or no longer available. A license awarded by the CLA is not limited in time.

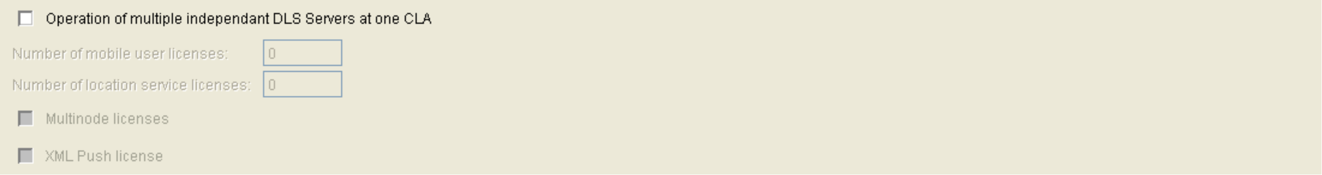
After this date, XML Push will no longer be available. Please contact you license administrator.

Grace period

Checked if the CLA is unreachable. The licenses determined last are then used. If the CLA has not yet been reached, XML Push is not available. The DLS tries to contact the CLA every 45 minutes. XML Push will not be available when the date in **Expiration date** expires. Please contact your license administrator.

6.14.2 "Multiple DLS Servers" Tab

Call: Main Menu > Administration > Server Licenses > "Multiple DLS Servers" Tab



☐ Operation of multiple independant DLS Servers at one CLA

Number of mobile user licenses: 0

Number of location service licenses: 0

☐ Multinode licenses

☐ XML Push license

Operation of multiple independent DLS Servers at one CLA

If activated, the basic device and mobile user licenses associated with multiple independent DLS servers can be managed at a central license agent (CLA).

Number of mobile user licenses

Maximum number of mobile user licenses to be requested by this DLS at the central license agent (CLA).

Number of location service licenses

Maximum number of location service licenses to be requested by this DLS at the central license agent (CLA).

Multinode licenses

If activated, DLS requests licenses for DLS Nodes and DB Mirroring from the CLA.

XML Push licenses

If activated, the DLS requests licenses for XML Push from the CLA.

7 IP Devices

Call: Main Menu > IP Devices

This menu item consists of the following areas:

- IP Phone Configuration
- IP Client Configuration
- IP Gateway Configuration
- IP Device Interaction
- IP Device XML Applications
- IP Device Management

Use this area to display and change the configuration data of IP devices.

> If changes are made in data records that have been generated using templates, these changes are not automatically applied to the templates.
> These changes must be manually saved to the template (Section 15.4, "Editing Templates").

> You can enter parameters for both SIP and HFA for every IP client in the **IP Client Configuration** area.

> An IP device can only be configured at the DLS after its successful registration. For registration, the IP device must be familiar with the relevant DLS address. Registration at the DLS is achieved by:
>
> - reading out IP device data via the DLS, see Section 7.4.4, "Scan IP Devices" and by
> - plugging the LAN connector or power supply into the IP device.

7.1 IP Phone Configuration

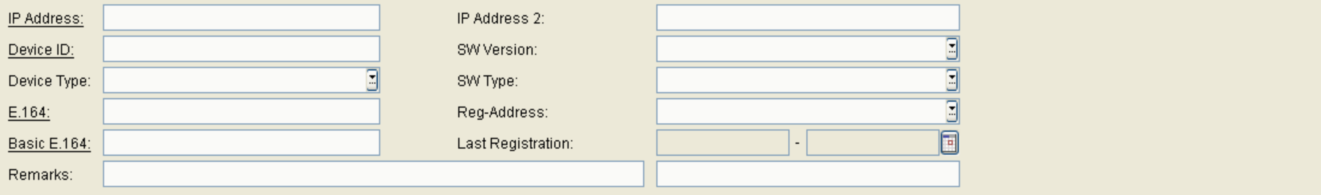
Call: Main Menu > IP Devices > IP Phone Configuration

This menu consists of the following submenus:

- Gateway/Server
- IP Routing
- Ports
- Features
- Quality of Service
- QoS Data Collection
- Security Settings
- Telephony
- Small Remote Site Redundancy
- Dialing Properties
- Time Parameters
- Audio Settings
- SNMP Settings
- Applications
- LDAP
- User Settings
- SIP Mobility
- HFA Mobility
- Keysets/Keylayout
- WLAN Settings
- Signaling and Payload Encryption (SPE)
- VoIP Security V1
- IEEE 802.1x
- Diagnosis
- Miscellaneous
- File Deployment

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP phones. The base data associated with the IP phones found is displayed in **Object** view (no changes possible except under **Remarks**).



IP Address:		IP Address 2:	
Device ID:		SW Version:	
Device Type:		SW Type:	
E.164:		Reg-Address:	
Basic E.164:		Last Registration:	-
Remarks:			

You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.

All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only **those** IP phones that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of the IP phone. For OpenStage, an IPv4 or IPv6 address is displayed here. See also the description of the **IP Protokoll Modus** parameter.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

IP phone device type. The icon indicates whether this is a virtual device.

All IP phone types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **optiPoint 410 standard**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

SW Type:

IP phone software type.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**

Reg-Address

IP address or DNS name of the HFA or SIP server at which the device is registered.

Last Registration:

Time of last IP phone registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Remarks:

Fields for general information.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, **IP address** contains the IPv4 address, and **IP address 2** contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP phones that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Get

Loads a template that has already been saved. For more information, see Section 15.4, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.4, "Editing Templates".

Discard

Discards any changes made and new entries.

Read

The parameters displayed on the new mask are read in again by the IP device.

Rename

Changes the name of a saved template. For more information, see Section 15.4, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.4, "Editing Templates".

Import Certificate

Imports a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.12, "Security: Administering Certificates".

Remove Certificate

Deletes a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.12, "Security: Administering Certificates".

7.1.1 Gateway/Server

Call: Main Menu > IP Devices > IP Phone Configuration > Gateway/Server

This area features the following components:

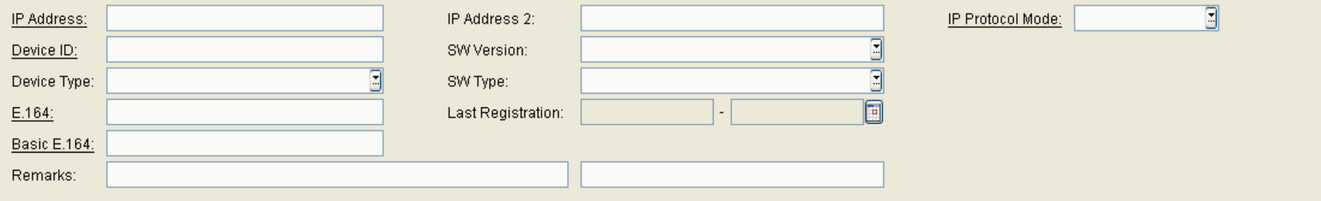
- General Data
- Possible Action Buttons
- "Gateway (HFA) / SIP Server" Tab
- "Gateway (Standby)" Tab
- "SIP Terminal Settings" Tab
- "SIP Registering 1" Tab
- "SIP Registering 2" Tab
- "SIP Survivability" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP phones. The base data associated with the IP phones found is displayed in **Object** view (no changes possible except under **Remarks**).



You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.

All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only **those** IP phones that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of the IP phone. For OpenStage, an IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

IP phone device type.

All IP phone types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **optiPoint 410 standard**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

SW Type:

IP phone software type.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**

Last Registration:

Time of last IP phone registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Remarks:

Fields for general information.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

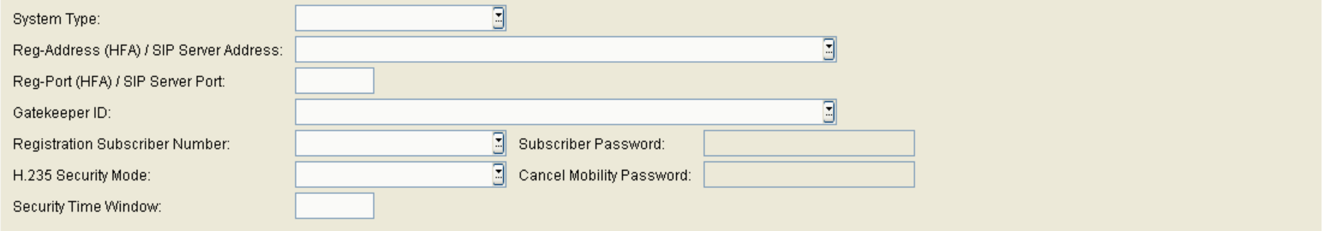
Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

7.1.1.1 "Gateway (HFA) / SIP Server" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Gateway/Server > "Gateway (HFA) / SIP Server" Tab


System Type:
Reg-Address (HFA) / SIP Server Address:
Reg-Port (HFA) / SIP Server Port:
Gatekeeper ID:
Registration Subscriber Number:
Subscriber Password:
H.235 Security Mode:
Cancel Mobility Password:
Security Time Window:

System Type:

Type and version of the communication platform at which the workpoint is operated.

Possible options:

- **Unknown**
- **HiPath 3000 generic**
- **HiPath 3000 V4.0**
- **HiPath 3000 V5.0**
- **HiPath 3000 V6.0**
- **HiPath 3000 V7.0**
- **HiPath 3000 V8.0**
- **HiPath 3000 V9.0**
- **HiPath 4000 generic**
- **HiPath 4000 V1.0**
- **HiPath 4000 V2.0**
- **HiPath 4000 V3.0**
- **HiPath 4000 V4.0**
- **HiPath 4000 V5.0**
- **HiPath 4000 V6.0**
- **HiPath 4000 V7.0**

Only available in HFA workpoints.

Reg-Address (HFA) / SIP Server Address:

IP address or host name of the PBX or gateway used for operating the workpoint.

Reg-Port (HFA) / SIP Server Port:

Port number of the PBX, gateway or SIP server used for operating the workpoint.

Gatekeeper ID:

ID of the PBX, gateway or gatekeeper used for operating the workpoint.

> This ID corresponds to the "Globid" parameter in AMO HFAB for the HiPath 4000 resp. the H.323 ID with the HiPath 3000.

Registration Subscriber Number:

Phone number of the subscriber at the PBX.

Example: **12345**

Only available in HFA workpoints.

H.235 Security Mode:

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Only available in HFA workpoints.

Security Time Window:

Indicates the maximum time difference permitted between the individual devices that should all run synchronously in H.235.

Only available in HFA workpoints.

Subscriber Password:

Password of the workpoint at the PBX.

Only available in HFA workpoints.

Cancel Mobility Password:

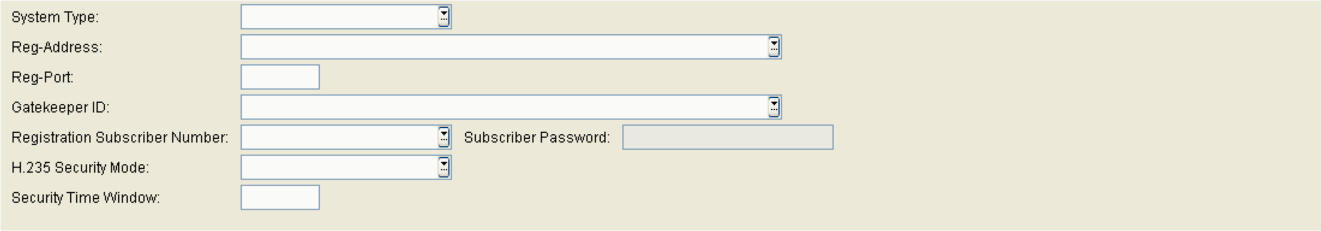
Password to disable the mobility function at the home workpoint.

Only available in HFA workpoints.

7.1.1.2 "Gateway (Standby)" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Gateway/Server > "Gateway (Standby)" Tab

> This "standby" data is used when the "home" data for the "Gateway (HFA) / SIP Server" Tab is not available. The SRSR functionality must be configured for this, see Section 7.1.9, "Small Remote Site Redundancy".



System Type:
Reg-Address:
Reg-Port:
Gatekeeper ID:
Registration Subscriber Number: Subscriber Password:
H.235 Security Mode:
Security Time Window:

System Type:

Type and version of the communication platform at which the workpoint is operated.

Possible options:

- **Unknown**
- **HiPath 3000 generic**
- **HiPath 3000 V4.0**
- **HiPath 3000 V5.0**
- **HiPath 3000 V6.0**
- **HiPath 3000 V7.0**
- **HiPath 3000 V8.0**
- **HiPath 3000 V9.0**
- **HiPath 4000 generic**
- **HiPath 4000 V1.0**
- **HiPath 4000 V2.0**
- **HiPath 4000 V3.0**
- **HiPath 4000 V4.0**
- **HiPath 4000 V5.0**
- **HiPath 4000 V6.0**
- **HiPath 4000 V7.0**

Only available in HFA workpoints.

Reg-Address:

IP address or host name of the PBX or gateway provided as standby for the workpoint.

Reg-Port:

Port number of the PBX or gateway provided as standby for the workpoint.

Gatekeeper ID:

ID of the PBX, gateway or gatekeeper provided as standby for the workpoint.

> This ID corresponds to the "Globid" parameter in AMO HFAB for the HiPath 4000 resp. the H.323 ID with the HiPath 3000.

Registration Subscriber Number:

Phone number of the subscriber at the PBX.

Example: **12345**

Only available in HFA workpoints.

H.235 Security Mode:

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Only available in HFA workpoints.

Security Time Window:

Indicates the maximum time difference permitted between the individual devices that should all run synchronously in H.235.

Only available in HFA workpoints.

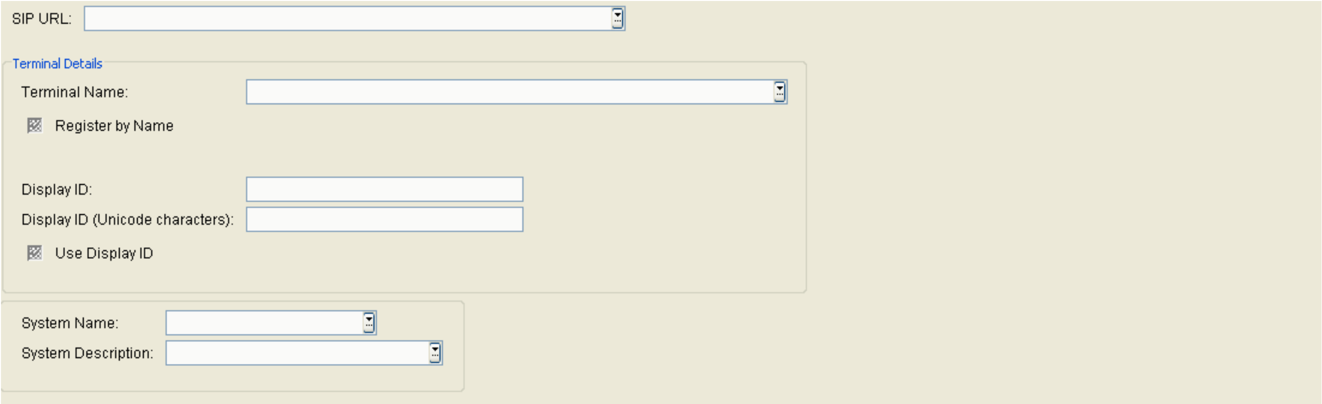
Subscriber Password:

Password of the workpoint at the standby PBX.

Only available in HFA workpoints.

7.1.1.3 "SIP Terminal Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Gateway/Server > "SIP Terminal Settings" Tab



SIP URL:

SIP address of the IP phone.

Format: **<SIP user ID>@<Domain>**.

Terminal Details

Terminal Name:

Name of the IP phone used as a synonym for the phone number during registration.

Only necessary if the **Register by Name** checkbox is selected and the registrar server is appropriately configured.

Register by Name

If this checkbox is activated, the phone logs on using the **Terminal Name**.

Display ID:

Name of the IP phone, as displayed on the telephone.

Value range: max. 24 alphanumeric characters.

Display ID (Unicode characters):

Name of the IP phone, as displayed on the telephone, in unicode characters.

> Unicode is only available in the OpenStage family of telephones.

Value range: max. 24 alphanumeric characters.

Use Display ID

If this checkbox is activated, the display ID is displayed on the device’s status bar.

System Name:

Random name that appears in the lower right-hand corner of the IP phone’s display (in two-line display).

Example: **HiPath**

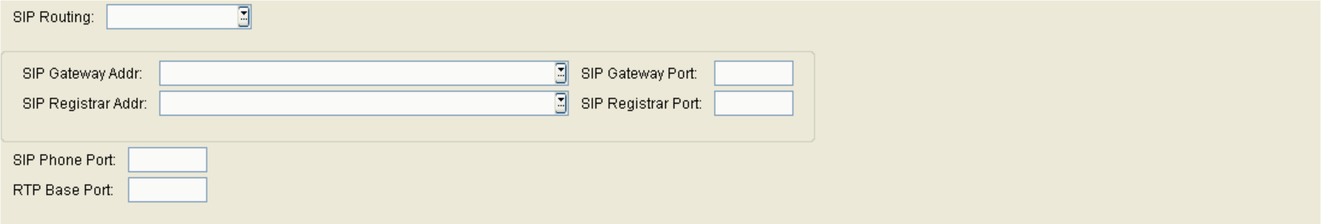
Value range: max. 10 alphanumeric characters.

System Description:

Used to display a system description at the workpoint (for three- or four-line display).

7.1.1.4 "SIP Registering 1" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Gateway/Server > "SIP Registering 1" Tab



SIP Routing:

Possible options:

- **Direct**
  For test purposes only.
- **Gateway**
  If a gateway is used.
- **Server**
  If an SIP proxy is used.

If Direct or Gateway is selected, no registration messages are sent during registration. Registration messages are sent to the registrar server for the **Server** routing mode.

SIP Gateway Addr:

IP address of the SIP gateway if the routing mode **Gateway** is used.

SIP Gateway Port:

Port number of the SIP gateway if the routing mode **Gateway** is used.

SIP Registrar Addr:

IP address of the SIP registrar.

SIP Registrar Port:

Port number of the SIP registrar.

SIP Phone Port:

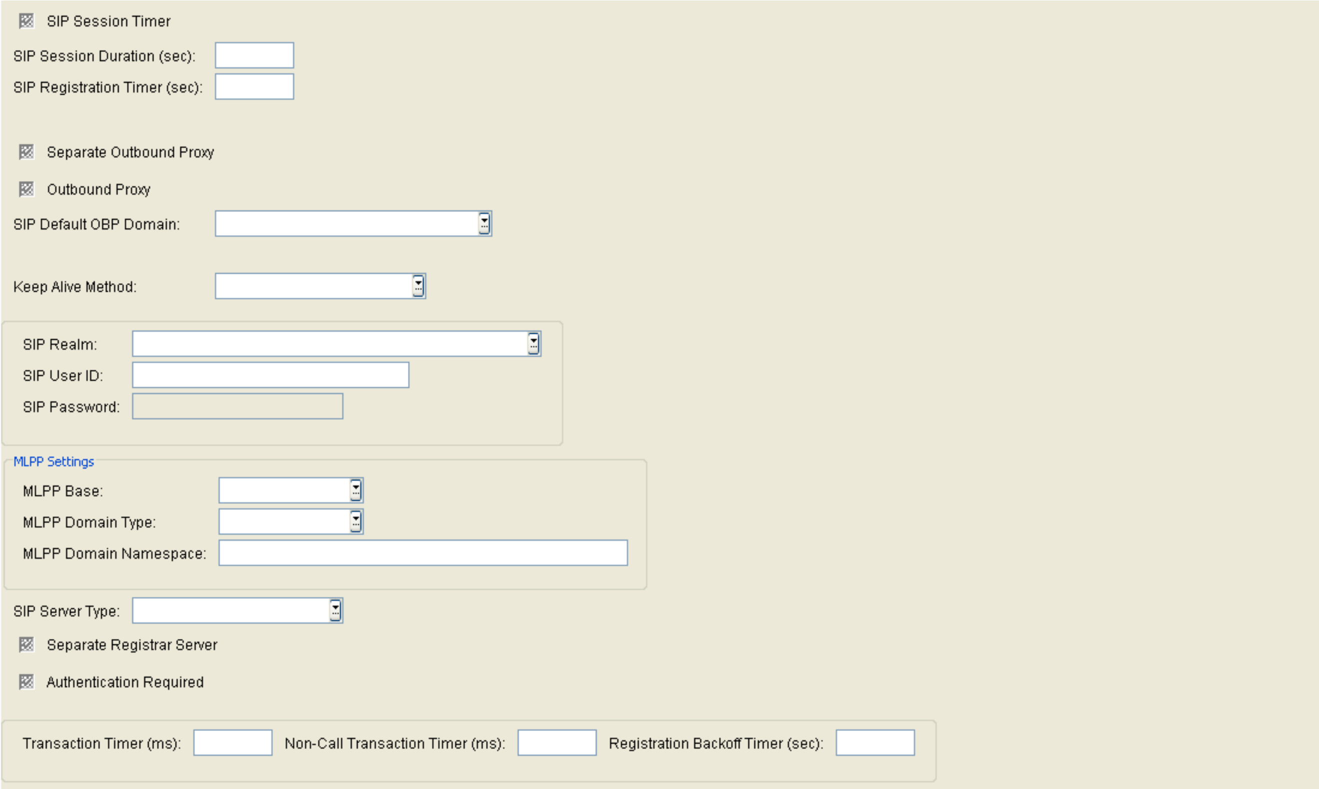
Port number of the IP phone.

RTP Base Port:

Base port number for RTP transport.

7.1.1.5 "SIP Registering 2" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Gateway/Server > "SIP Registering 2" Tab



SIP Session Timer

Checkbox for activating the SIP session timer. The timer is used to monitor the duration of an SIP session.

SIP Session Duration:

Highest duration in seconds for an SIP session.

Value range: **0** ... **3600** seconds.

SIP Registration Timer (sec.):

Time until re-registration at the SIP server. Re-registration ensures that the SIP telephone remains logged on to the SIP server. It can also detect server connectivity problems.

Value range: **0** ... **4320** seconds.

Default: **0**

Separate Outbound Proxy

If this option is activated, a separate outbound proxy is used. This parameter is used with optiPoint WL2 phones to indicate an outbound proxy which is not identical with the SIP proxy.

Outbound Proxy

Checkbox for activating an SIP proxy for outbound calls.

Together with **SIP Default OBP Domain**, this checkbox controls outbound call routing on the basis of the number dialed or the user ID.

For more information, see Chapter 17, "Outbound Proxy".

SIP Default OBP Domain:

Together with **Outbound Proxy** this entry controls outbound call routing on the basis of the number dialed or the user ID.

For more information, see Chapter 17, "Outbound Proxy".

Keep Alive Method:

Selects the keep alive method used between comms and the switch.

Possible options:

- **Sequence**
- **CRLF**

SIP Realm:

Naming range where the user ID and password are valid. This SIP realm must be entered in the system and on the SIP server.

SIP User ID:

The user ID is the first part of the SIP URL. Required, together with the password, to access the SIP server.

SIP Password:

Password associated with the user ID, required to access the SIP server.

MLPP Settings

MLPP Base

Possible options:

- **Local**
- **Server**

MLPP Domain Type

Specifies which resource priority namespace will be accepted from a fixed list.

Possible options:

- **dsn**
  dsn-000000
- **uc**
  uc-000000
- **dsn+uc**
- **Other domain**

MLPP Domain Namespace

Specifies an ASCII string for a single resource priority namespace which will be accepted.

Alphanumerical characters and the following special charakters are allowed: -!%*_+` "~

A "." is not allowed.

SIP Server Type:

Selects the appropriate SIP server type for the IP phone.

Possible options:

- **Broadsoft**
- **OpenScape Voice**
- **Sylantro**
- **Other**
- **HiQ 8000**
- **Genesys**

Separate Registrar Server

If you log on to a WLAN, you can be contacted at your personal number. A registrar assigns the SIP URI or IP address you are currently logged on under to your personal number. Your SIP provider may offer a separate registrar server.

Activate this checkbox to log on to a separate registrar proxy server. You can enter the server address and port number of the registrar proxy server in the entry fields that then appear.

Only applies to WLAN phones.

Authentication Required

Activate this checkbox if you have to enter your **SIP user ID** in addition to the standard access data to log on to the SIP provider.

Only applies to WLAN phones.

Transaction Timer (ms)

Time in milliseconds that a device will wait for a requested SIP message before the server is categorized as unavailable.

Non-Call Transaction Timer (ms)

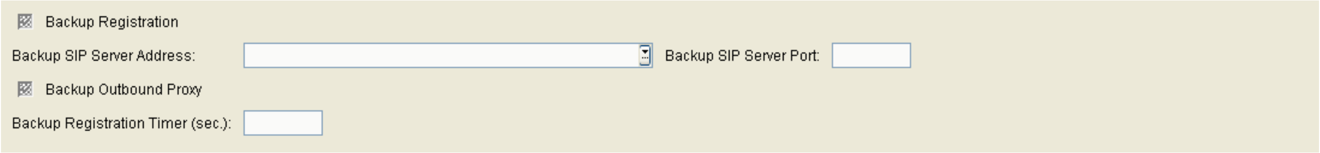
Time in milliseconds allowed for non-INVITE (nonCall) based transaction (F timer).

Registration Backoff Timer (sec)

Time in seconds allowed between attempts to reREGISTER after a registration failure.

7.1.1.6 "SIP Survivability" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Gateway/Server > "SIP Survivability" Tab



Backup Registration

Checkbox for activating the backup registration.

Backup SIP Server Address:

IP address or host name of the backup SIP server.

Backup SIP Server Port:

Port number for communication with the backup SIP server.

Backup Outbound Proxy

Checkbox for activating the SIP Proxy backup for outgoing calls.

For more information, see Chapter 17, "Outbound Proxy".

Backup Registration Time:

Time period before re-registration at the backup SIP server. Re-registration ensures that the SIP telephone remains logged on to the backup SIP server. It can also detect server connectivity problems.

Requirement: An SIP server backup must be used.

Value range: **0** ... **4320** seconds.

Default: **0**.

7.1.2 IP Routing

Call: Main Menu > IP Devices > IP Phone Configuration > IP Routing

This area features the following components:

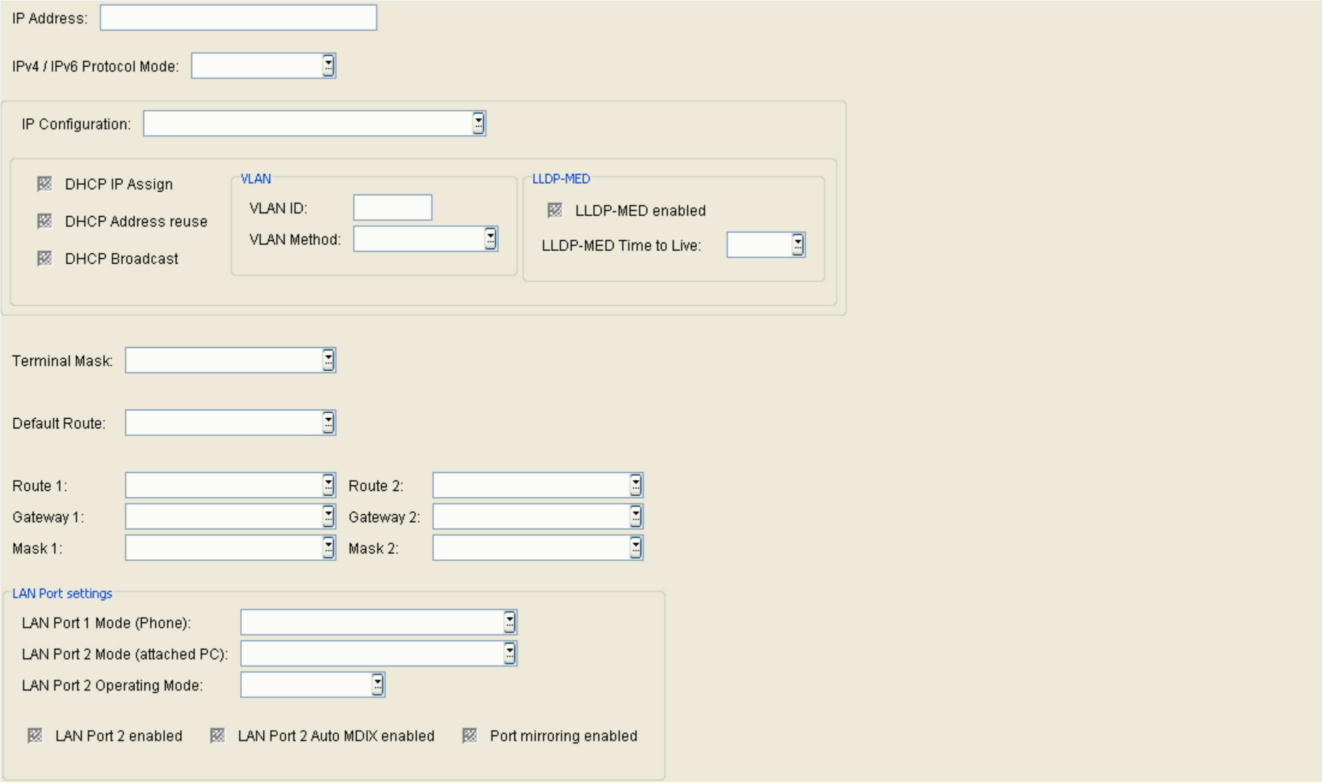
- General Data
- Possible Action Buttons
- "IP Routing" Tab
- "IPv6 Settings" Tab
- "DNS Server" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.2.1 "IP Routing" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > IP Routing > "IP Routing" Tab



IP Address

IP address of the IP phone.

IPv4 / IPv6 Protocol Mode

Selects the internet protocol to be used by the IP phone.

Possible Options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

IP Configuration

Determines how the IP settings are to be configured; valid from OpenStage version 1.5. With versions < 1.5, this field is greyed out, like the remaining LLDP-MED parameters.

> Please note that the writing and reading procedures for this parameter differ from one another. When the DLS user select a particular option (e.g. "LLDP-MED with DHCP Configuration"), the IP configuration parameters are set and sent to the end device. When reading from the device, however, "Please select an option for IP Configuration" is displayed in any case. This is due to the possibility that the parameter may not have been detected unambigously; for instance, the value of the **VLAN method** parameter can depend on whether the VLAN ID has been determined over DHCP or over LLDP-MED.

The field is predefined with 'Please select an option for IP Configuration'.

Possible Values:

- **LLDP-MED with DHCP Configuration**
- **Use DHCP**
- **Manual VLAN with DHCP Configuration**
- **Manual Settings**

DHCP IP Assign

This checkbox can be activated if a DHCP server is present. The workpoint then obtains the IP address data dynamically from the DHCP server.

This checkbox must not be activated if there is no DHCP server available. Instead, the IP address data (**IP Address**, **Terminal Mask** and **Default Route**) must be manually set for this workpoint.

DHCP lease reuse

This checkbox can be activated if a DHCP server is present. If the switch is activated, the DHCP lease will be reused.

DHCP Broadcast

This checkbox can be activated if a DHCP server is present. With this entry the user can change the DHCP protocol element "flags". If the broadcast flag is enabled, the DHCP server will broadcast its responses to the phone's requests; otherwise unicast responses will be used.

VLAN

VLAN ID:

VLAN ID when using virtual LANs. Can only be changed if QoS layer 2 is active. The value is read-only if it has been dynamically assigned with DHCP.

Value range: **0** ... **4095**.

VLAN Method:

Determines how the VLAN ID is assigned to the end device. Can only be changed when QoS layer 2 has been activated.

Possible options:

- **Manually**
  The VLAN ID is entered manually.
- **DHCP**
  The VLAN ID supplied by the DHCP server is used.
- **None**
  (For WLAN only)
- **LLDP-MED**
  The VLAN ID supplied by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) is used. Available for OpenStage from V1R5 onwards.

LLDP-MED

LLDP-MED enabled:

Enables sending and receiving LLDP data.

LLDP-MED Time-to-Live

Possible Values:

- **40**
- **60**
- **80**
- **100**
- **110**
- **120**
- **140**
- **180**
- **240**
- **320**
- **400**

Terminal Mask:

Subnet mask for the IP address.

The value is read-only if it was dynamically assigned with DHCP.

Default Route:

IP address or host name of the default router/gateway.

The value is read-only if it was assigned with DHCP.

Route 1:

IP address or host name of the first static route (optional).

Gateway 1:

IP address or host name of the router/gateway of the first static route (optional).

Mask 1:

Subnet mask of the first static route (optional).

Route 2:

IP address or host name of the second static route (optional).

Gateway 2:

IP address or host name of the router/gateway of the second static route (optional).

Mask 2:

Subnet mask of the second static route (optional).

LAN Port settings

LAN Port 1 Mode (Phone):

Data rate mode for the first Ethernet port on the IP phone. The first port is connected to the LAN. The data rate value depends on the switch or router bandwidth that is supported in the network.

Possible options:

- **10 Mbps half-duplex**
- **10 Mbps full-duplex**
- **100 Mbps half-duplex**
- **100 Mbps full-duplex**
- **Auto**

Default: **Auto**

LAN Port 2 Mode (attached PC):

Data rate mode for the second LAN port on the IP phone. The value depends on the switch or router bandwidth that is supported in the network.

Possible options:

- **10 Mbps half-duplex**

- **10 Mbps full-duplex**
- **100 Mbps half-duplex**
- **100 Mbps full-duplex**
- **Auto**

Default: **Auto**

LAN Port 2 Operating Mode

Choice between three modes of operation for the PC port.

Possible options:

- **Disabled**
  The LAN port is inactive.
- **Enabled**
  The LAN port is active.
- **Mirror**
  All data traffic on LAN port 1 is mirrored to port 2.

LAN Port 2 enabled

Checkbox for enabling LAN port 2.

LAN Port 2 Auto MDIX enabled

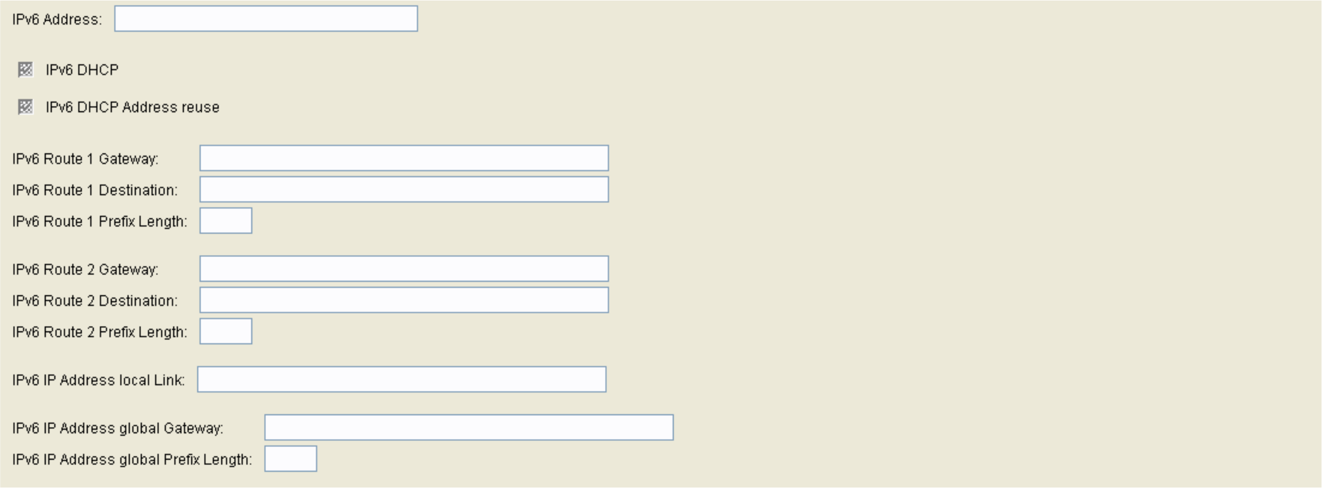
Checkbox for enabling LAN Port 2 Auto MDIX. If Auto MDIX is enabled, the LAN port automatically switches between normal MDI and MDI-X (crossover circuit).

Port mirroring enabled

When this checkbox is activated, all data traffic on LAN port 1 can be mirrored to port 2: The operation type for **LAN Port 2 Operating Mode** must be set to **Mirror**.

7.1.2.2 "IPv6 Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > IP Routing > "IPv6 Settings" Tab



IPv6 Address:

☑ IPv6 DHCP

☑ IPv6 DHCP Address reuse

IPv6 Route 1 Gateway:
IPv6 Route 1 Destination:
IPv6 Route 1 Prefix Length:

IPv6 Route 2 Gateway:
IPv6 Route 2 Destination:
IPv6 Route 2 Prefix Length:

IPv6 IP Address local Link:

IPv6 IP Address global Gateway:
IPv6 IP Address global Prefix Length:

IPv6 Address

IPv6 address of the IP phone.

IPv6 DHCP

IPv6 DHCP

IPv6 DHCP Address reuse

When activated, the address provided by the IPv6 DHCP server is reused.

IPv6 Route 1 Gateway

IPv6 address of the router/gateway for the first static route.

IPv6 Route 1 Destination

Destination address for the first static route.

IPv6 Route 1 Prefix Length

Prefix length for the first static route.

IPv6 Route 2 Gateway

IPv6 address of the router/gateway for the second static route.

IPv6 Route 2 Destination

Destination for the second static route.

IPv6 Route 2 Prefix Length

Prefix length for the second static route.

IPv6 IP Address local Link

Local link address of the IP phone.

IPv6 IP Address global Gateway

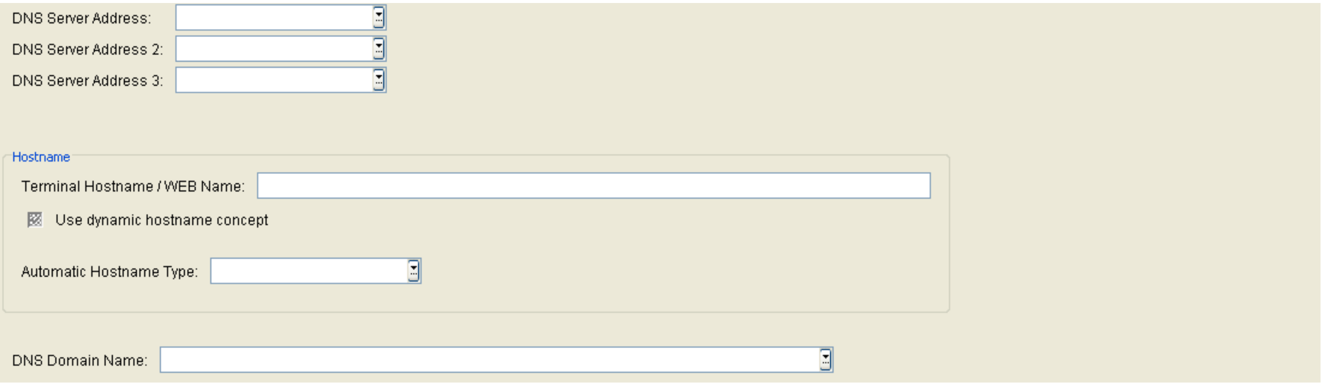
IPv6 address of the global router/gateway .

IPv6 IP Address global Prefix Length

Length of the global prefix.

7.1.2.3 "DNS Server" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > IP Routing > "DNS Server" Tab



DNS Server Address:

IP address or host name of the DNS server.

The value is read-only if it was dynamically assigned with DHCP.

DNS Server Address 2:

IP address or host name of the second DNS server (optional).

The value is read-only if it was dynamically assigned with DHCP.

Not available in optiPoint 400.

DNS Server Address 3:

IP address or host name of the third DNS server (optional).

The value is read-only if it was dynamically assigned with DHCP.

Not available in optiPoint 400.

Hostname

Terminal Hostname / WEB Name:

Host name of the terminal.

Permitted characters: letters, digits, hyphens, underscores, and periods; case-sensitive; maximum length: 63 characters.

The value is read-only if it was dynamically assigned with DHCP.

Use dynamic hostname concept

If this checkbox is activated, the E.164 number is used as the DNS host name for IP phones.

Automatic Hostname Type:

Type of automatically generated hostname.

Possible Values:

- **No DDNS Hostname**
- **Only WEB Name**
- **Only Number**
- **Prefix Number**
- **MAC based**

DNS Domain Name:

Domain name of the DNS server.

The value is read-only if it was dynamically assigned with DHCP.

7.1.3 Ports

Call: Main Menu > IP Devices > IP Phone Configuration > Ports

This area features the following components:

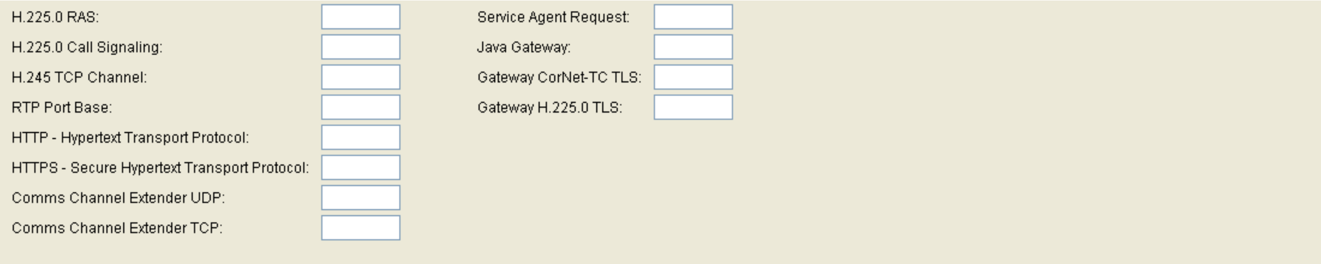
- General Data
- Possible Action Buttons
- "Ports" Tab
- "Ports (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.3.1 "Ports" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Ports > "Ports" Tab



H.225.0 RAS:		Service Agent Request:	
H.225.0 Call Signaling:		Java Gateway:	
H.245 TCP Channel:		Gateway CorNet-TC TLS:	
RTP Port Base:		Gateway H.225.0 TLS:	
HTTP - Hypertext Transport Protocol:			
HTTPS - Secure Hypertext Transport Protocol:			
Comms Channel Extender UDP:			
Comms Channel Extender TCP:			

H.225.0 RAS:

Port number for H.225 RAS.

Purpose: Registration and approval in the case of VoIP.

For communication with the following clients: Netmeeting, AP1120.

Port used: **1719**

H.225.0 Call Signaling:

Port number for H.225 call signaling.

Purpose: Connection control in the case of VoIP.

For communication with the following clients: HG1500, IP phones, Netmeeting, AP1120.

Port used: **1720**

H.245 TCP Channel

Port number for the H.245 TCP channel.

RTP Port Base:

Port number for RTP.

Purpose: Transporting voice packets in the case of VoIP.

For communication with the following clients: HG1500, IP phones, Netmeeting, AP11xx.

Port range used: **29100** ... **29131**

HTTP - Hypertext Transport Protocol:

Port number for HTTP.

Purpose: Web-based Management.

For communication with the following clients: the workpoint’s WBM.

Port used: **8085**

HTTPS - Secure Hypertext Transport Protocol:

Port number for HTTPS.

Purpose: Web-Based Management.

For communication with the following clients: the workpoint's WBM.

Only available in SIP workpoints.

Port used: **443**

Comms Channel Extender UDP Port:

Comms Channel Extender TCP Port:

Service Agent Request:

JAVA Gateway:

Port number for gateways used by Java applications.

Gateway CorNet-TC TLS

Port used by the HFA gateway for secure communication with the workpoint.

Only available in HFA workpoints.

Gateway H.225.0 TLS

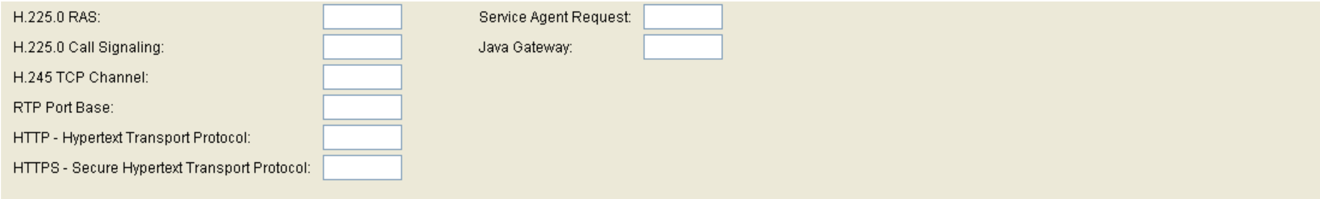
Port used for secure signalling with H.255.

Only available in HFA workpoints.

7.1.3.2 "Ports (Standby)" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Ports > "Ports (Standby)" Tab

> This "standby" data is used when the "home" data for the "Ports" Tab is not available. The SRSR functionality must be configured for this, see Section 7.1.9, "Small Remote Site Redundancy".



H.225.0 RAS:		Service Agent Request:	
H.225.0 Call Signaling:		Java Gateway:	
H.245 TCP Channel:			
RTP Port Base:			
HTTP - Hypertext Transport Protocol:			
HTTPS - Secure Hypertext Transport Protocol:			

H.225.0 RAS:

Port number for H.225 RAS.

Purpose: Registration and approval in the case of VoIP.

For communication with the following clients: Netmeeting, AP1120.

Port used: **1719**

H.225.0 Call Signaling:

Port number for H.225 call signaling.

Purpose: Connection control in the case of VoIP.

For communication with the following clients: HG1500, IP phones, Netmeeting, AP1120.

Port used: **1720**

H.245 TCP Channel

Port number for the H.245 TCP channel.

For communication with the following clients:

Port used:

RTP Port Base:

Port number for RTP.

Purpose: Transporting voice packets in the case of VoIP.

For communication with the following clients: HG1500, IP phones, Netmeeting, AP11xx, MEB.

Port range used: **29100** ... **29131**

HTTP - Hypertext Transport Protocol:

Port number for HTTP.

Purpose: Web-based Management.

For communication with the following clients: the workpoint’s WBM.

Port used: **8085**

HTTPS - Secure Hypertext Transport Protocol:

Port number for HTTPS (HTTP with SSL encryption).

Purpose: Web-based Management.

For communication with the following clients: the workpoint’s WBM.

Only available in SIP workpoints.

Port used: **443**

Service Agent Request:

Port number for service agent request.

JAVA Gateway:

Port number for the Java gatekeeper.

Gateway CorNet-TC TLS

Port used by the standby HFA gateway for secure communication with the workpoint.

Only available in HFA workpoints.

Gateway H.225.0 TLS

Port used for secure signalling with H.225 when the workpoint has switched to the standby gateway.

Only available in HFA workpoints.

7.1.4 Features

Call: Main Menu > IP Devices > IP Phone Configuration > Features

This area features the following components:

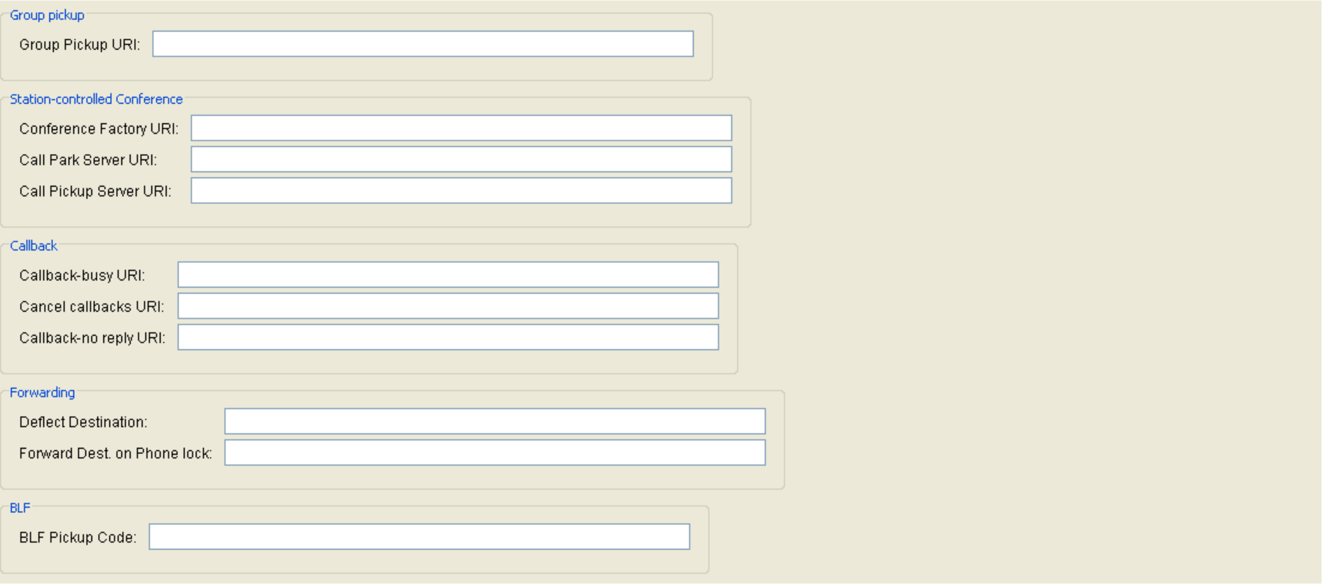
- General Data
- Possible Action Buttons
- "Feature Settings 1" Tab
- "Feature Settings 2" Tab
- "Call related User Settings" Tab
- "Availability" Tab
- "Server based features" Tab
- "Dialplan" Tab
- "Ringer Melody / Tone" Tab
- "Call Forwarding" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.4.1 "Feature Settings 1" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Features > "Feature Settings 1" Tab



Group pickup

Group Pickup URI:

Station-controlled Conference

Conference Factory URI:

Call Park Server URI:

Call Pickup Server URI:

Callback

Callback-busy URI:

Cancel callbacks URI:

Callback-no reply URI:

Forwarding

Deflect Destination:

Forward Dest. on Phone lock:

BLF

BLF Pickup Code:

Group pickup

Group Pickup URI:

URI of the group pickup.

Only available in SIP workpoints.

Station-controlled Conference

Conference Factory URI:

URI for setting up conference calls.

Only available in SIP workpoints.

Call Park Server URI:

URI of the server for parking calls.

Only available in SIP workpoints.

Call Pickup Server URI:

URI of the server for group pickup.

Only available in SIP workpoints.

Callback

Callback-busy URI:

URI of the server that controls the "Callback-busy" feature.

Cancel callbacks URI:

URI that prompts the server to delete callback requests.

Callback-no reply URI

URI of the server that controls the "Callback-no reply" feature.

Deflection

Deflect Destination

Destination number for call forwarding.

Forward Dest. on Phone lock:

Destination number for forwarding in the case of a call to a locked workpoint.

BLF

BLF Pickup Code:

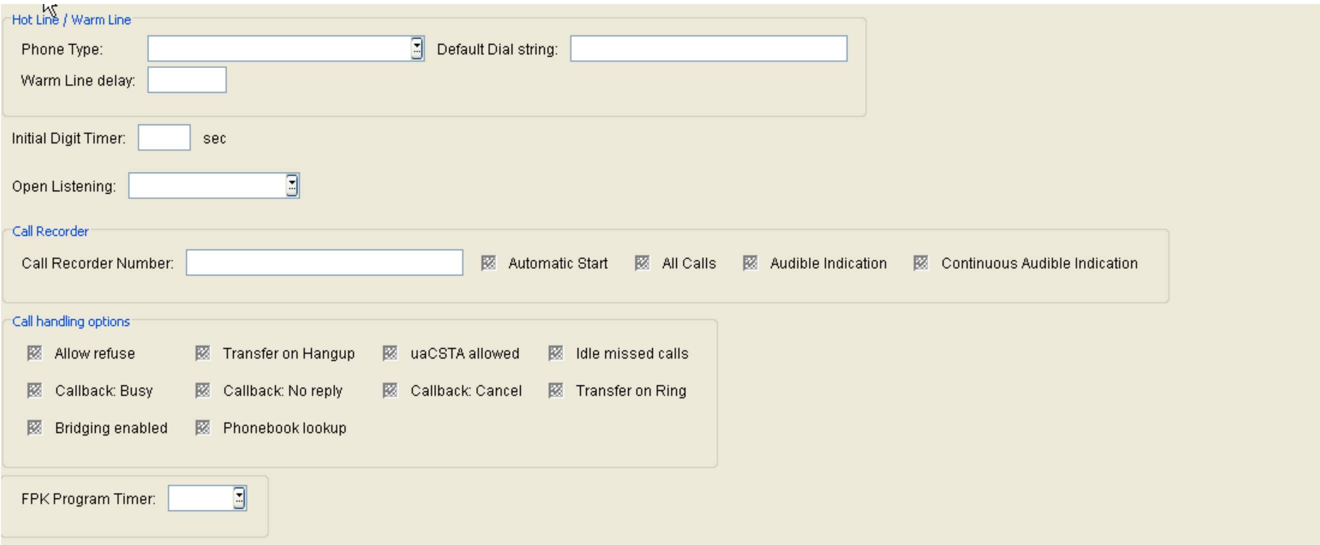
Feature code for BLF Pickup Code with Asterisk.

Only available in SIP workpoints.

7.1.4.2 "Feature Settings 2" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Features > "Feature Settings 2" Tab

> When operating SIP IP phones on HiPath 3000 and HiPath 4000 platforms, the following features are not available and should be deactivated so that users cannot see or select them:
>
> - Auto answer
> - Callback-busy
> - Auto reconnect
> - Callback-no reply
>
> See also "Availability" Tab.



Hot Line / Warm Line

Phone Type: [ ]   Default Dial string: [ ]

Warm Line delay: [ ]

Initial Digit Timer: [ ] sec

Open Listening: [ ]

Call Recorder

Call Recorder Number: [ ]   ☒ Automatic Start   ☒ All Calls   ☒ Audible Indication   ☒ Continuous Audible Indication

Call handling options

☒ Allow refuse   ☒ Transfer on Hangup   ☒ uaCSTA allowed   ☒ Idle missed calls

☒ Callback: Busy   ☒ Callback: No reply   ☒ Callback: Cancel   ☒ Transfer on Ring

☒ Bridging enabled   ☒ Phonebook lookup

FPK Program Timer: [ ]

Hot Line/Warm Line

Phone Type:

Set device property.

Possible options:

- **Ordinary**
- **Hotline**
- **Warmline**

Only available in SIP workpoints.

Default Dial String:

Destination number for the functions "Hotline" and "Warmline".

Only available in SIP workpoints.

Warm Line delay:

Dialing delay in seconds for the warm line function.

For "Hotline" (emergency call) the value 0 should be entered as the time.

Only available in SIP workpoints.

Initial Digit Timer:

Waiting time in seconds for a dialed digit after the dial tone starts.

Only available in SIP workpoints.

Open Listening

Configures switching to Open Listening mode.

Possible options:

- **Standard Mode**
  To switch to Open Listening mode, the user must press and hold the Open Listening key while returning the handset to the cradle.
- **US Mode**
  To switch to Open Listening mode, the user must press the Open Listening key and then return the handset to the cradle.

Call Recorder

Recording Mode

Determines the behaviour of the call recording.

Possible options:

- **Manual**
- **Auto Start**
- **All Calls**

Audible Notification

Select the tone for audible notification.

Possible options:

- **Off**
- **On / Single Shot**
- **Continuous**

Call Recorder Number:

Phone number of the call recorder.

Automatic Start

When activated, call recording is started automatically, with incoming calls and with outgoing calls. The user can switch the recording on or off during a conversation. The checkbox is effective only if voice recording is activated on the phone.

All Calls

When activated, call recording is started automatically, with incoming calls and with outgoing calls. The user can not control the recording. The checkbox is effective only when voice recording is activated on the phone.

Audible Indication

A beep signals to the called party that the phone call is being recorded.

Continuous Audible Indication

A continuous audible indication signals to the called party that the phone call is being recorded. The checkbox is effective only when **Audible Indication** is activated.

Call handling options

Allow refuse

Checkbox for activating the function for rejecting calls.

Only available in SIP workpoints.

Transfer on Hangup

Checkbox for activating the "Transfer on Hangup" feature.

Only available in SIP workpoints.

uaCSTA allowed

Checkbox to activate the "uaCSTA" feature.

Only available in SIP workpoints.

Idle missed calls

If set, an indication for missed calls will be shown on the display.

Callback: Busy

Checkbox for activating the "Callback-busy" feature.

Only available in SIP workpoints.

Callback: No reply

Checkbox for activating the "Callback-no reply" feature.

Only available in SIP workpoints.

Callback: Cancel

When active, the user can cancel callback requests.

Transfer on Ring

Checkbox for activating the "Transfer on Ring" feature

Only available in SIP workpoints.

Bridging enabled

When active, call bridging is enabled.

Only available in SIP workpoints.

Phonebook lookup

Checkbox for activating the "Phonebook lookup" feature.

FPK Program Timer

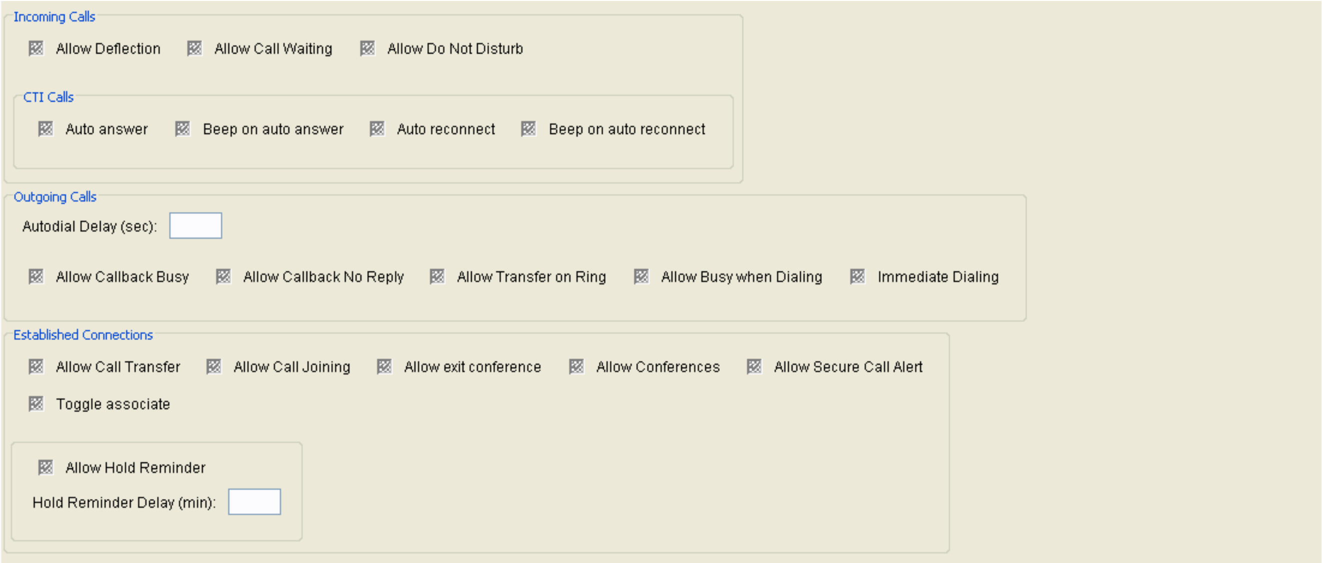
When "Off" is selected, the free programmable keys (FPKs) will not change to programming mode on long press.

Possible options:

- **On**
- **Off**

7.1.4.3 "Call related User Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Features > "Call related User Settings" Tab



Incoming Calls

☒ Allow Deflection ☒ Allow Call Waiting ☒ Allow Do Not Disturb

CTI Calls

☒ Auto answer ☒ Beep on auto answer ☒ Auto reconnect ☒ Beep on auto reconnect

Outgoing Calls

Autodial Delay (sec):

☒ Allow Callback Busy ☒ Allow Callback No Reply ☒ Allow Transfer on Ring ☒ Allow Busy when Dialing ☒ Immediate Dialing

Established Connections

☒ Allow Call Transfer ☒ Allow Call Joining ☒ Allow exit conference ☒ Allow Conferences ☒ Allow Secure Call Alert

☒ Toggle associate

☒ Allow Hold Reminder

Hold Reminder Delay (min):

Incoming calls

Allow Deflection

Checkbox for activating Call Deflection.

Allow Call Waiting

Checkbox for activating Call Waiting.

Allow Do Not Disturb

Checkbox for activating Do Not Disturb.

CTI Calls

Auto answer

Checkbox for activating Auto Answer.

Only available in SIP workpoints.

Beep on auto answer

Checkbox for activating a confirmation beep on Auto Answer.

Only available in SIP workpoints.

Auto reconnect

Checkbox for activating automatic reconnection of a parked call.

Only available in SIP workpoints.

Beep on auto reconnect

Checkbox for activating a confirmation beep on reconnection of a parked call.

Only available in SIP workpoints.

Outgoing calls

Autodial delay (sec):

Delay for Automatic Dialing in seconds.

Allow Callback Busy

Checkbox for activating Callback on Busy.

Allow Callback No Reply

Checkbox for activating Callback on No Reply.

Allow Transfer on Ring

Checkbox for activating Transfer on Ring.

Allow Busy when Dialing

Checkbox for activating Busy when Dialing.

Immediate Dialing

If this check box is active, immediate dialing is executed as soon as the entered string matches a dial plan entry.

Only available in SIP workpoints.

Established Connections

Allow Call Transfer

Checkbox for activating Call Transfer.

Allow Call Joining

Checkbox for activating Call Joining.

Allow exit conference

Checkbox for activating Exit Conference.

Allow Conferences

Checkbox for activating Conferences.

Allow Secure Call Alert

If the handling of secure calls is enabled on the phone and this check box is activated, a popup window and an alert tone will notify the user when an insecure (unencrypted) call comes in.

Toggle associate

When this feature is activated, the following procedure will ensue: The user has accepted a second call, whereby the first call is put to hold. As soon as the user has alternated back to the first call, and then again to the second call, he/she can connect both calling parties by going on-hook.

Allow Hold Reminder

Checkbox for activating the Hold Reminder.

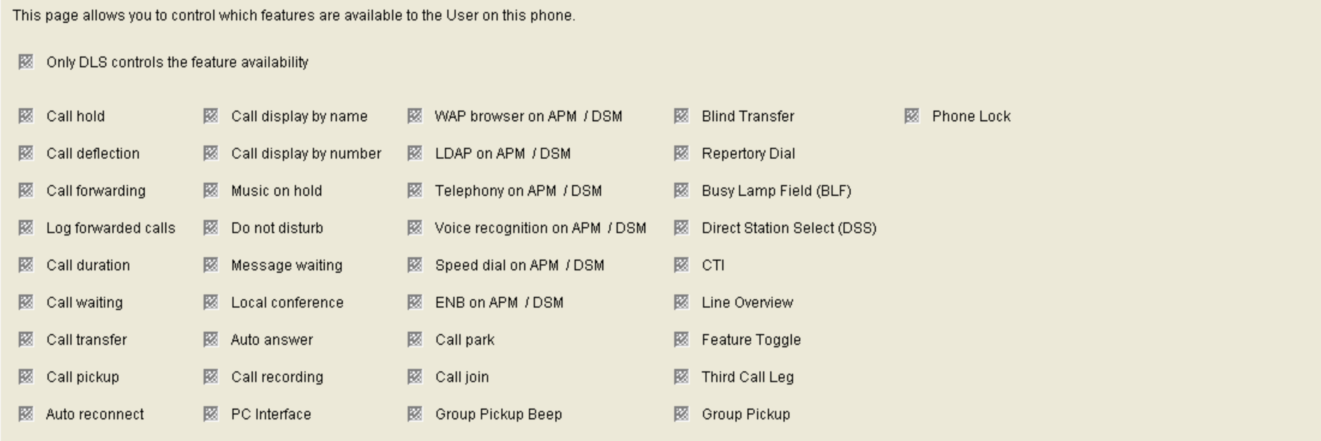
Hold Reminder Delay (min):

Delay for the Hold Reminder in minutes.

7.1.4.4 "Availability" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Features > "Availability" Tab

> When operating SIP IP phones on HiPath 3000 and HiPath 4000 platforms, the following features are not available and should be deactivated so that users cannot see or select them:
>
> - Auto answer
> - Call deflection
> - Call forwarding
> - Auto answer
> - Call waiting
> - Log forwarded calls
> - Music on hold
> - Call park
> - Call transfer
> - Local conference
> - Message waiting
>
> See also "Feature Settings 2" Tab.



This page allows you to control which features are available to the User on this phone.

☑ Only DLS controls the feature availability

☑ Call hold
☑ Call deflection
☑ Call forwarding
☑ Log forwarded calls
☑ Call duration
☑ Call waiting
☑ Call transfer
☑ Call pickup
☑ Auto reconnect

☑ Call display by name
☑ Call display by number
☑ Music on hold
☑ Do not disturb
☑ Message waiting
☑ Local conference
☑ Auto answer
☑ Call recording
☑ PC Interface

☑ WAP browser on APM / DSM
☑ LDAP on APM / DSM
☑ Telephony on APM / DSM
☑ Voice recognition on APM / DSM
☑ Speed dial on APM / DSM
☑ ENB on APM / DSM
☑ Call park
☑ Call join
☑ Group Pickup Beep

☑ Blind Transfer
☑ Repertory Dial
☑ Busy Lamp Field (BLF)
☑ Direct Station Select (DSS)
☑ CTI
☑ Line Overview
☑ Feature Toggle
☑ Third Call Leg
☑ Group Pickup

☑ Phone Lock

Only DLS controls feature availability

If this checkbox is activated, the availability of features is controlled exclusively by the DLS. The data entered in the "Feature Availability" tab is used. If this checkbox is not activated, the availability can also be controlled on the IP Device.

Only available in SIP workpoints.

Call hold

Checkbox for activating the function for placing calls on hold.

Only available in SIP workpoints.

Call deflection

Checkbox for activating manual forwarding for incoming calls (CD).

Only available in SIP workpoints.

Call forwarding

Checkbox for activating automatic call forwarding (CF).

Only available in SIP workpoints.

Log forwarded calls

Checkbox for activating logging for forwarded calls.

Only available in SIP workpoints.

Call duration

Checkbox for activating the function for displaying the call duration.

Only available in SIP workpoints.

Call waiting

Checkbox for activating visual and/or acoustic alerting for waiting calls (CW).

Only available in SIP workpoints.

Call transfer

Checkbox for activating the function for transferring calls (ECT).

Only available in SIP workpoints.

Call pickup

Checkbox for activating the function for picking up parked calls.

Only available in SIP workpoints.

Auto reconnect

Checkbox for activating the auto reconnect feature.

Only available in SIP workpoints.

Call display by number

Switch for activating call number display at the workpoint.

Only available in SIP workpoints.

Call display by name

Switch for activating caller name display at the workpoint.

Only available in SIP workpoints.

Music on hold

Checkbox for activating music on hold for held and parked calls.

Only available in SIP workpoints.

Do not disturb

Checkbox for activating the do-not-disturb function (optical alerting and ring only).

Only available in SIP workpoints.

Message waiting

Checkbox for activating alerting for waiting messages (MWI).

Only available in SIP workpoints.

Local conference

Checkbox for activating the function for setting up a local conference.

Only available in SIP workpoints.

Auto answer

Checkbox for activating auto answer.

Only available in SIP workpoints.

Call Recording

Checkbox for enabling call recording.

PC Interface

Checkbox for enabling the interface between the PC and the device.

WAP browser on APM/DSM

Checkbox for activating the WAP browser on the optiPoint application module/display module.

Only available in SIP workpoints.

LDAP on APM/DSM

Checkbox for activating the LDAP function on the optiPoint application module/display module.

Only available in SIP workpoints.

Telephony on APM/DSM

Checkbox for activating the telephony function on the optiPoint application module/display module.

Only available in SIP workpoints.

Voice recognition on APM/DSM

Checkbox for activating the voice recognition function (voice dialing) on the optiPoint application module/display module.

Only available in SIP workpoints.

Speed dial on APM/DSM

Checkbox for activating the speed-dialing function on the optiPoint application module/display module with a Java midlet.

Only available in SIP workpoints.

ENB on APM/DSM

Checkbox for activating the electronic notebook on the optiPoint application module/display module.

Only available in SIP workpoints.

Call park

Checkbox for activating the function for parking calls.

Only available in SIP workpoints.

Call join

Checkbox for activating the function for joining calls.

Only available in SIP workpoints.

Group Pickup Beep

If this checkbox is activated, you will hear a beep when a call is waiting for a pickup group.

Blind Transfer

Checkbox for activating the feature "Blind Transfer".

Repertory Dial

Checkbox for activating the feature "Repertory Dial".

Busy Lamp Flag (BLF)

Checkbox for activating the Busy Lamp Field (BLF).

Direct Station Select (DSS)

Checkbox for activating Direct Station Select (DSS).

CTI

Checkbox for activating the CTI interface.

Line Overview

Checkbox for activating the line Ooverview.

Feature Toggle

Checkbox for activating the feature "Feature Toggle".

Third Call Leg

Checkbox for activating the feature "Third Call Leg".

Group Pickup

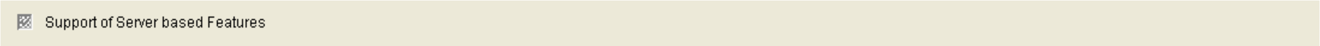
Checkbox for activating the feature "Group Pickup".

Phone Lock

Checkbox for activating the feature "Phone Lock".

7.1.4.5 "Server based features" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Features > "Server based features" Tab



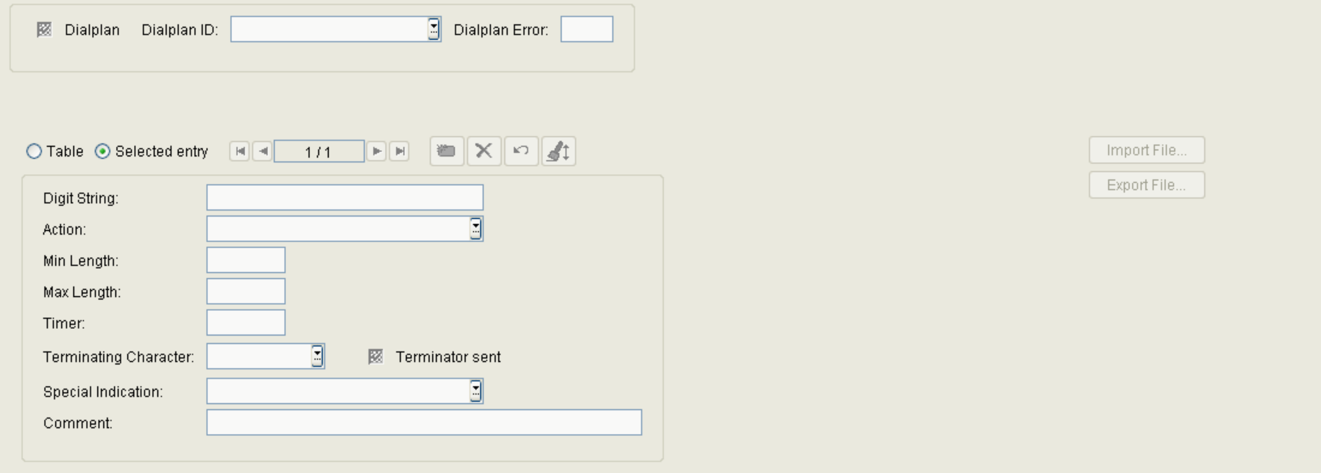
☑ Support of Server based Features

Support of Server based Features

If this checkbox is activated, server-based features on the device are enabled for the user.

7.1.4.6 "Dialplan" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Features > "Dialplan" Tab



Dialplan

Checkbox for activating the dial plan. The entries in this tab are interpreted if this checkbox is active.

Only available in SIP workpoints.

Dialplan ID

Name of the dial plan - must begin with a "!".

Value range: max. 14 alphanumeric characters.

Only available in SIP workpoints.

Dialplan Error

Specifies the dial plan entry that is faulty in the event of an error.

Value range: **1** ... **48**

Only available in SIP workpoints.

Digit String

Digit String Digit string for executing this action.

Only available in SIP workpoints.

Action

Action executed for this digit string.

Possible options:

- **-C- Action for digits**
- **-S- Send digits**

Only available in SIP workpoints.

Min Length

Minimum digit string length for digit string interpretation.

Only available in SIP workpoints.

Max Length

Maximum digit string length for digit string interpretation.

Only available in SIP workpoints.

Timer

Delay before the action is performed.

Value range: **1** ... **9** seconds.

Only available in SIP workpoints.

Terminating Character

Character that ends the digit string entered.

Possible options:

- **#**
- *****

Only available in SIP workpoints.

Special Indication

Possible options:

- **-E- emergency call**
- **-b- bypass**

Only available in SIP workpoints.

Comment

Field for general information.

Only available in SIP workpoints.

Terminator sent

Displays whether the terminating character is included in the digit string.

Import File

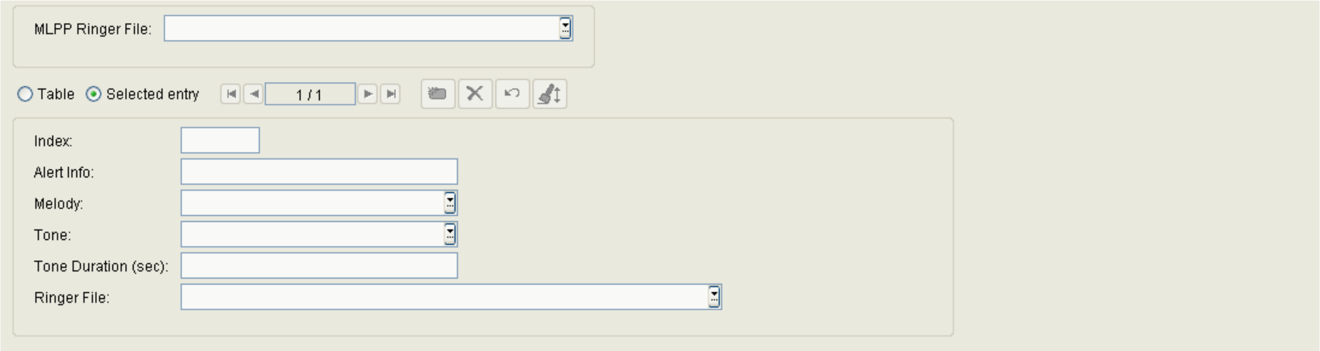
Imports a dialplan from a file in CSV format.

Export File

Exports a dialplan from a file in CSV format.

7.1.4.7 "Ringer Melody / Tone" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Features > "Ringer Melody / Tone" Tab



A template for **Ringer Melody / Tone** can be created by searching for an IP Device with entries in **Ringer Melody / Tone** (empty entries are allowed as well). Use the action **Copy to Template** to create a template. There must be 15 entries, which may be empty.
This template can be modified, saved, and applied.

MLPP Ringer File

Ringtone file to be used for priority calls.

Index

Automatically generated index for the particular distinctive ringtones.

Alert Info

If the string specified here is identical with a special string which is sent to the phone in the SIP alert info header, the corresponding ringtone is used.

Only available in SIP workpoints.

Melody

Type of ring melody.

Possible options: **Melody 1** ... **Melody 8, Melody off**

Only available in SIP workpoints.

Tone

Ringtone sequence.

Possible options:

- **1**
  = 1 sec ON, 4 sec OFF
- **2**
  = 1 sec ON , 2 sec OFF
- **3**
  = 0,7 sec ON, 0,7 sec OFF , 0,7 sec ON, 3 sec OFF

Only available in SIP workpoints.

Tone Duration

Duration of the ringtone.

Value range: **1** ... **300** seconds.

Default: **60** seconds.

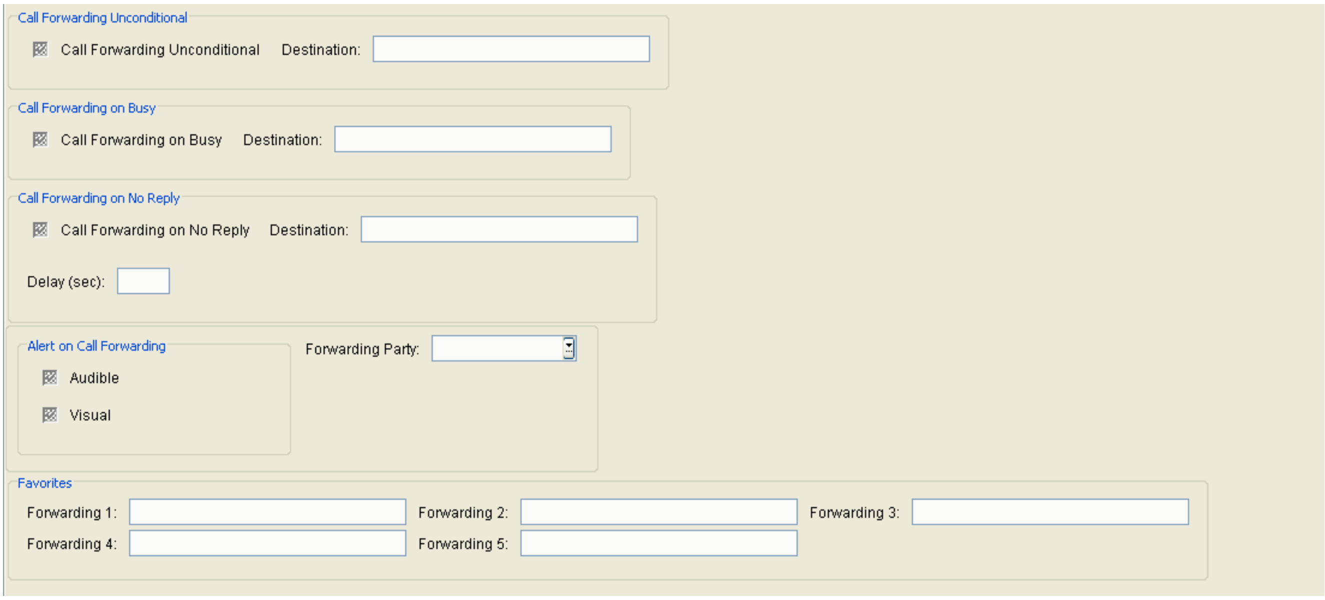
Only available in SIP workpoints.

Ringer File

Name of the audio file containing the ringtone.

7.1.4.8 "Call Forwarding" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Features > "Call Forwarding" Tab



Call Forwarding Unconditional

▨ Call Forwarding Unconditional Destination:

Call Forwarding on Busy

▨ Call Forwarding on Busy Destination:

Call Forwarding on No Reply

▨ Call Forwarding on No Reply Destination:

Delay (sec):

Alert on Call Forwarding

▨ Audible

▨ Visual

Forwarding Party:

Favorites

Forwarding 1: Forwarding 2: Forwarding 3:

Forwarding 4: Forwarding 5:

Call Forwarding Unconditional

Call Forwarding Unconditional

Schalter zum Aktivieren der "Anrufumleitung ohne weitere Bedingungen".

Checkbox for activating Unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Call Forwarding on Busy

Call Forwarding on Busy

Checkbox for activating Call Forwarding n Busy.

Destination:

Call number of the Call Forwarding destination.

Call Forwarding on No Reply

Call Forwarding on No Reply:

Checkbox for activating Call Forwarding on No Reply.

Destination:

Call number of the Call Forwarding destination.

Delay (sec):

As soon as this time span has expired without the call being accepted, the call is forwarded.

Alert on Call Forwarding

Audible

Checkbox for activating an audible alert on the forwarding phone.

Visual

Checkbox for activating a visible alert on the forwarding phone.

Forwarding Party:

Select which forwarding party will be displayed when multiple forwarding is active.

Possible options:

- **Display first**
- **Display last**

Favorites

Forwarding 1:

Forwarding 2:

Forwarding 3:

Forwarding 4:

Forwarding 5:

7.1.5 Quality of Service

Call: Main Menu > IP Devices > IP Phone Configuration > Quality of Service

This area features the following components:

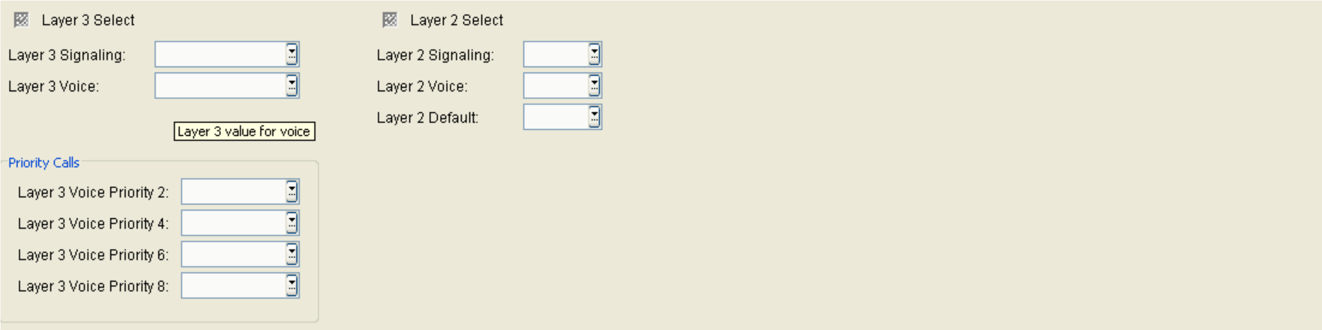
- General Data
- Possible Action Buttons
- "QoS Parameter" Tab
- "QoS Parameter (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.5.1 "QoS Parameter" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Quality of Service > "QoS Parameter" Tab



Layer 3 Select

Checkbox for activating the QoS layer 3 configuration.

Layer 3 Signaling:

Layer 3 value for call signaling.

Value range fo optiPoint HFA workpoints (lower than optiPoint HFA V5R5) and optiPoint SIP workpoints in SIP5 or lower: **0** **63**

Possible values for optiPoint SIP6 or higher and optiPoint HFA V5R5 or higher:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Possible values for OpenStage SIP/HFA:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**

- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**
- **0 - BE**
- **56 - CS7**

Possible values for WLAN HFA/SIP:

- **0 - BE**
- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Layer 3 Voice:

Layer 3 value for language.

Value range for optiPoint HFA workpoints (except optiPoint HFA V5R5 and higher) and optiPoint SIP workpoints with SIP5 or lower: **0** **63**

Possible values for optiPoint HFA from V5R5 and optiPoint SIP6 or higher:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**

- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Possible values for OpenStage SIP/HFA:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**
- **0 - BE**
- **56 - CS7**

Values for WLAN HFA/SIP:

- **0 - BE**
- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 -AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Layer 2 Select

Checkbox for activating the QoS layer 2 configuration.

Layer 2 Signaling:

Layer 2 value for call signaling.

Value range: **0** ... **7**

Layer 2 Voice:

Layer 2 value for voice.

Value range: **0** ... **7**

Layer 2 Default:

Default for the layer 2 value.

Value range: **0** ... **7**

Priority Calls

Layer 3 Voice Priority 2

Layer 3 value for voice at priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 4

Layer 3 value for voice at priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 6

Layer 3 value for voice at priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 8

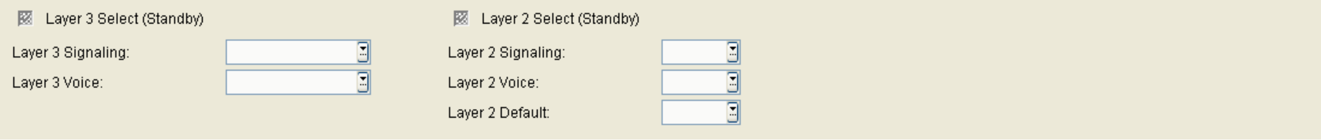
Layer 3 value for voice at priority calls.

Value range: **DSCP00** ... **DSCP63**

7.1.5.2 "QoS Parameter (Standby)" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Quality of Service > "QoS Parameter (Standby)" Tab

> This "standby" data is used when the "home" data for the "QoS Parameter" Tab is not available. The SRSR functionality must be configured for this, see Section 7.1.9, "Small Remote Site Redundancy".



☒ Layer 3 Select (Standby)

Layer 3 Signaling:

Layer 3 Voice:

☒ Layer 2 Select (Standby)

Layer 2 Signaling:

Layer 2 Voice:

Layer 2 Default:

Layer 3 Select (Standby)

Checkbox for activating the QoS layer 3 configuration.

Layer 3 Signaling:

Layer 3 value for call signaling.

Value range for optiPoint HFA workpoints (lower than optiPoint HFA V5R5) and optiPoint SIP workpoints in SIP5 or lower: **0** **63**

Possible values for optiPoint SIP6 or higher and optiPoint HFA V5R5 or higher:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Layer 3 Voice:

Layer 3 value for language.

Value range for HFA workpoints and SIP workpoints in SIP5 or lower: **0** **63**

Possible values for optiPoint SIP6 or higher and optiPoint HFA V5R5 or higher:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Possible values for WLAN HFA/SIP:

- **0 - BE**
- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 -AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Layer 2 Select (Standby)

Checkbox for activating the QoS layer 2 configuration.

Layer 2 Signaling:

Layer 2 value for call signaling.

Value range: **0** ... **7**

Layer 2 Voice:

Layer 2 value for voice.

Value range: **0** ... **7**

Layer 2 Default:

Default for the layer 2 value.

Value range: **0** ... **7**

7.1.6 QoS Data Collection

Call: Main Menu > IP Devices > IP Phone Configuration > QoS Data Collection

> This function is not available in the onboard variants of DLS on OpenScape Voice systems.

This area features the following components:

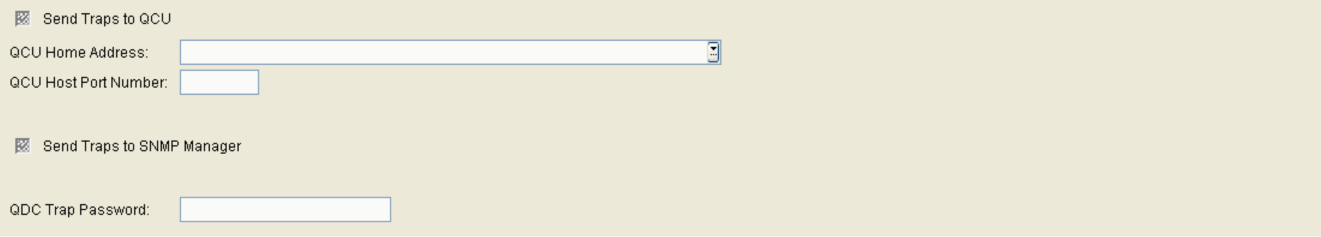
- General Data
- Possible Action Buttons
- "Server Data" Tab
- "Report Settings" Tab
- "Threshold Values" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.6.1 "Server Data" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > QoS Data Collection > "Server Data" Tab



☒ Send Traps to QCU

QCU Home Address:

QCU Host Port Number:

☒ Send Traps to SNMP Manager

QDC Trap Password:

Send Traps to QCU

Checkbox for activating the function that sends errors to the QCU.

QCU Home Address:

IP address or host name of the server that collects the QDC data.

QCU Host Port Number:

Port number for the server that collects the QDC data.

Send Traps to SNMP Manager

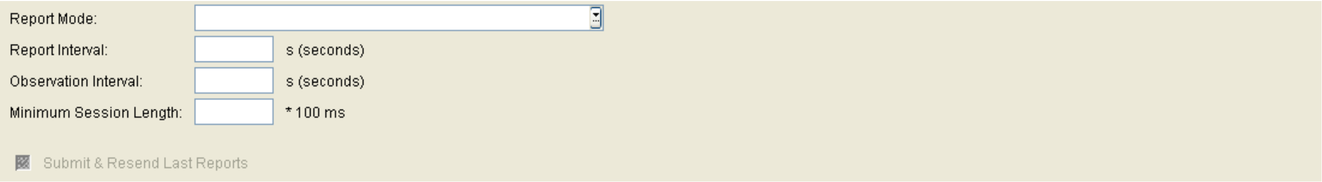
Checkbox for activating the function that sends errors to the SNMP Manager.

QDC Trap Password

Password of the server collecting the QDC traps.

7.1.6.2 "Report Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > QoS Data Collection > "Report Settings" Tab



Report Mode:		
Report Interval:		s (seconds)
Observation Interval:		s (seconds)
Minimum Session Length:		* 100 ms

☒ Submit & Resend Last Reports

Report Mode:

Specifies when a report should be generated.

Possible options:

- **EOS Threshold exceeded**
  At the end of the connection that exceeded the threshold.
- **EOR Threshold exceeded**
  At the end of the reporting interval that exceeded the threshold.
- **EOS (End of Session)**
  At the end of the connection.
- **EOR (End or Report Interval)**
  At the end of the reporting interval.

Report Interval:

Time interval in which a QoS report is sent.

Value range: **0** ... **3600** seconds.

Observation Interval:

Time interval in which threshold violation is checked.

Value range: **0** ... **5000** seconds.

Minimum Session Length:

A QoS report is sent if a session (for example, a call) undershoots this minimum.

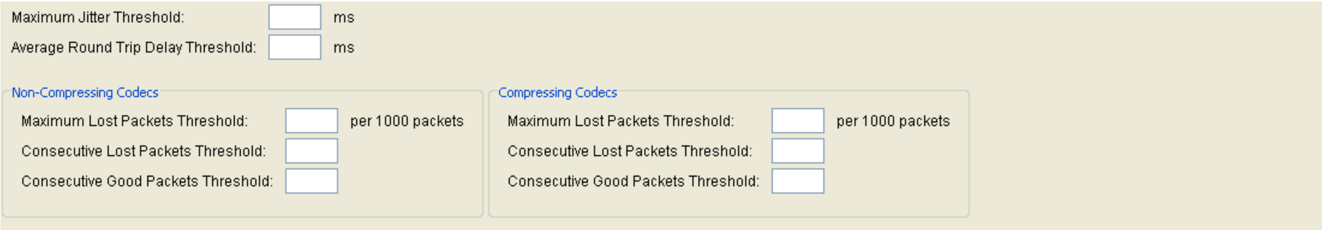
Value range: **0** ... **5000** (x 100 ms).

Submit & Resend Last Reports

When this checkbox is enabled, the workpoint resends the last QoS reports.

7.1.6.3 "Threshold Values" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > QoS Data Collection > "Threshold Values" Tab



Maximum Jitter Threshold: ms

Average Round Trip Delay Threshold: ms

Non-Compressing Codecs

Maximum Lost Packets Threshold: per 1000 packets

Consecutive Lost Packets Threshold:

Consecutive Good Packets Threshold:

Compressing Codecs

Maximum Lost Packets Threshold: per 1000 packets

Consecutive Lost Packets Threshold:

Consecutive Good Packets Threshold:

Maximum Jitter Threshold:

Maximum threshold in milliseconds for runtime fluctuations during data transmission to trigger a report.

Value range: **0** ... **255** ms.

Default: **15**

Average Round Trip Delay Threshold:

Average response time (in milliseconds) for signal transmission.

Default: **100**

Non-Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during uncompressed transmission.

Value range: **0** ... **255**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during uncompressed transmission.

Value range: **0** ... **255**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during uncompressed transmission.

Value range: **0** ... **255**

Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during compressed transmission.

Value range: **0** ... **255**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during compressed transmission.

Value range: **0** ... **255**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during compressed transmission.

Value range: **0** ... **255**

7.1.7 Security Settings

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings

This area features the following components:

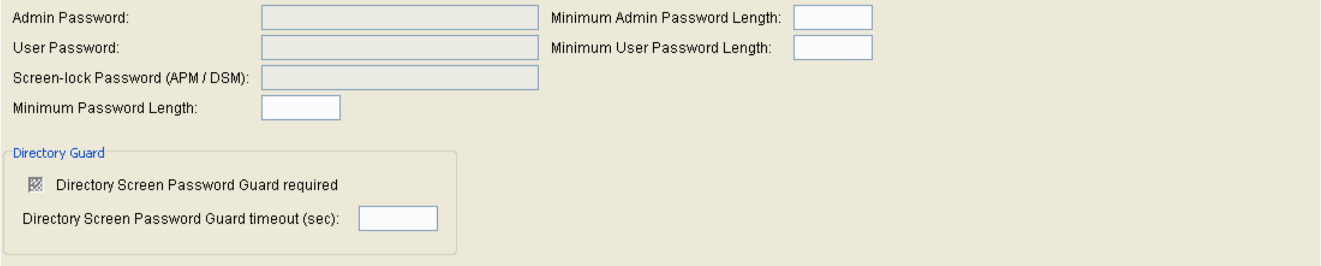
- General Data
- Possible Action Buttons
- "Passwords" Tab
- "Additional Password Policy Settings" Tab
- "Enabled Services (NW Stack)" Tab
- "WBM Server Certificate" Tab
- "HTTPS Server CA Certificates" Tab
- "OCSR 1 Server CA Certificate" Tab
- "OCSR 2 Server CA Certificate" Tab
- "OCSR 1 Signature CA Certificate" Tab
- "OCSR 2 Signature CA Certificate" Tab
- "Certificate Policy" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.7.1 "Passwords" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "Passwords" Tab



Admin Password:
User Password:
Screen-lock Password (APM / DSM):
Minimum Password Length:
Minimum Admin Password Length:
Minimum User Password Length:

Directory Guard

▨ Directory Screen Password Guard required
Directory Screen Password Guard timeout (sec):

Admin Password:

Password for access to the workpoint’s administration area.

User Password:

Password for access to the workpoint’s user area.

Screen-lock Password (DSM/APM):

Password for canceling the display lock on the optiPoint 410 Application Module/Display Module.

Only applicable if an Application Module/Display Module is used.

Minimum Password Length:

Minimum number of characters that an administration or user password must contain. Only available if the current object is a HFA telephone (old version) because in this case both passwords are the same length.

Minimum Admin Password Length:

Minimum number of characters that an administration password must contain. Only available if the current object is an SIP telephone.

Minimum User Password Length:

Minimum number of characters that a user password must contain. Only available if the current object is an SIP telephone.

Directory Guard

Directory Screen Password Guard required

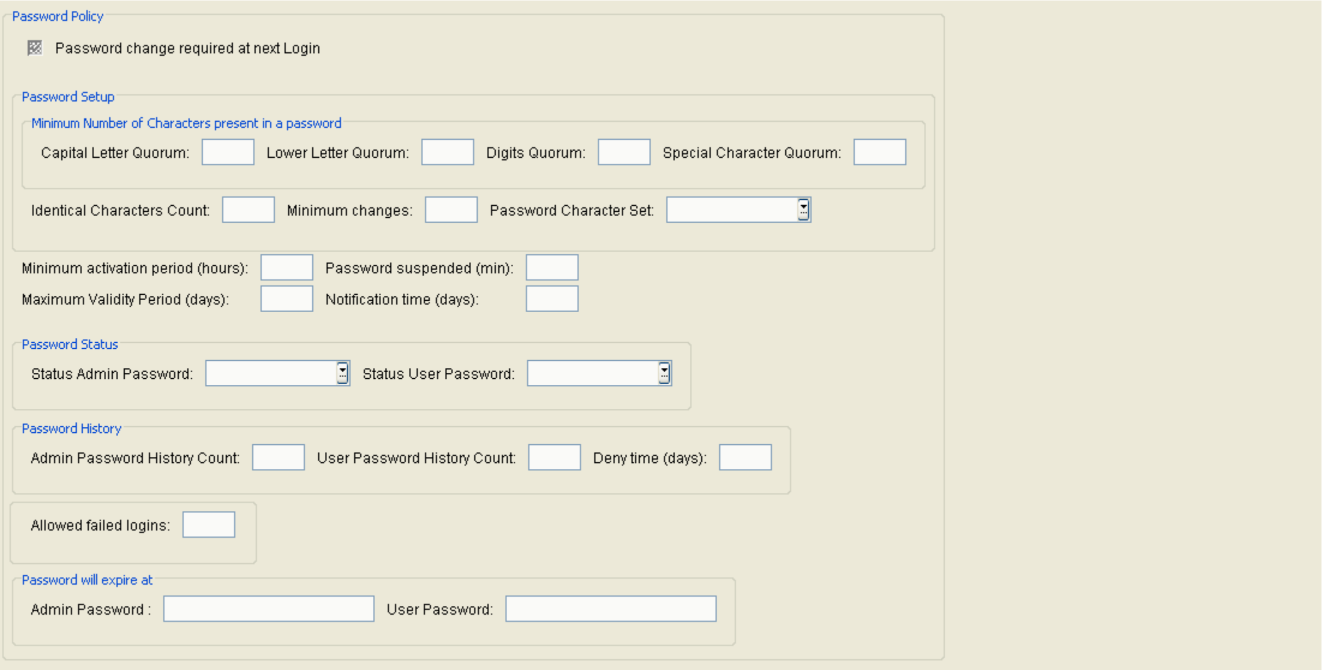
This checkbox activates password protection for the directory screen. To use the screen, you must enter the standard user password.

Directory Screen Password Guard timeout (sec)

Password protection is activated when the length of time specified here expires. After this time, you must enter the password to continue using the screen.

7.1.7.2 "Additional Password Policy Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "Additional Password Policy Settings" Tab


Password Policy
▨ Password change required at next Login
Password Setup
Minimum Number of Characters present in a password
Capital Letter Quorum:
Lower Letter Quorum:
Digits Quorum:
Special Character Quorum:
Identical Characters Count:
Minimum changes:
Password Character Set:
Minimum activation period (hours):
Password suspended (min):
Maximum Validity Period (days):
Notification time (days):
Password Status
Status Admin Password:
Status User Password:
Password History
Admin Password History Count:
User Password History Count:
Deny time (days):
Allowed failed logins:
Password will expire at
Admin Password :
User Password:

Password Policy

Password change required at next Login

When activated, the user is forced to change his/her password at the next login.

Password Setup

Minimum Number of Characters present in a password.

Capital Letter Quorum

Number of capital letters the password must contain.

Value range: **0** ... **24**

0 = no check

Lower Letter Quorum

Number of lower case letters the password must contain.

Value range: **0** ... **24**

0 = no check

Digits Quorum

Number of digits the password must contain.

Value range: **0** ... **24**

0 = no check

Special Character Quorum

Number of special characters (`-=[];'#\,./!"£$%^&*()_+{}:@~|<>?) the password must contain.

Value range: **0** ... **24**

0 = no check

Identical Characters Count

Maximum number of identical characters the password may contain.

Value range: **0** ... **24**

0 = no check

Minimum changes

The number of characters that must change when the password is changed.

Value range: **0** ... **24**

0 = no check

Password Character Set

Character set to be allowed for the password.

Possible Options:

- **Unlimited**
- **ASCII**
- **PIN**
- **Numbers**

Minimum activation period (hours)

Minimum waiting period before an existing password can be updated, in hours.

Password suspended (min)

When the maximum number of retries has been exceeded, the password is suspended for the period specified here, in minutes.

Maximum Validity Period (days)

Maximum validity period of a password.

Notification time (days)

When the password will expire within the number of days specified here, the user is notified.

0 = no check

Password Status

Status Admin Password

Status of the admin password.

Possible Options:

- **Active**
- **Suspended**
- **Disabled**

Status User Password

Status of the user password.

Possible Options:

- **Active**
- **Suspended**
- **Disabled**

Password History

Admin Password History Count:

Minimum number of admin passwords to store in the history file. New passwords must not match any password in the history file.

Value range: **0** … **999**

User Password History Count:

Minimum number of user passwords to store in the history file. New passwords must not match any password in the history file.

Value range: **0** … **999**

Deny time (days):

Time interval during which a password may not be selected again as a new password by the phone, as it remains in the password history for this time.

Allowed failed logins

Number of attempts a user is given to enter the password before access will be suspended.

Value range: **2** … **5**

Default value: **3**

Password will expire at

Admin Password

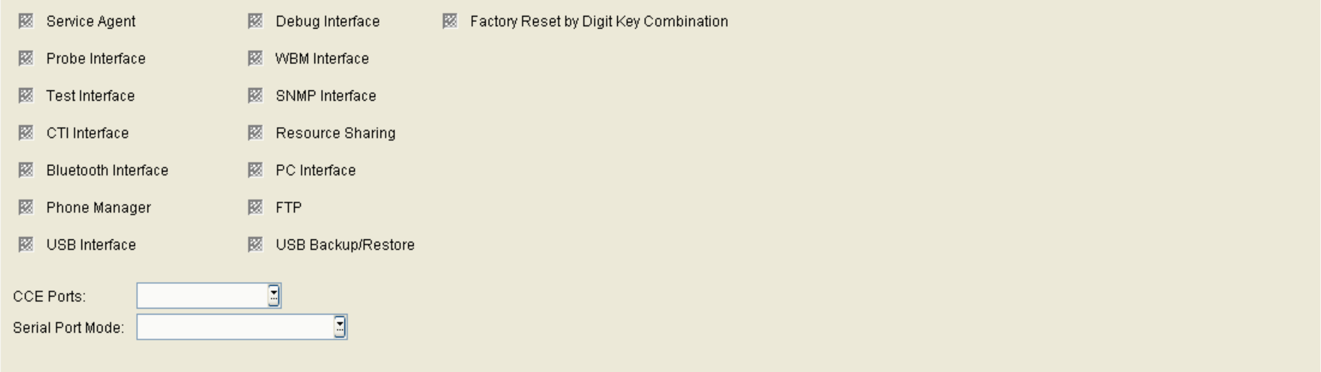
Time and date of admin password expiry.

User Password

Time and date of user password expiry.

7.1.7.3 "Enabled Services (NW Stack)" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "Enabled Services (NW Stack)" Tab



☑ Service Agent
☑ Probe Interface
☑ Test Interface
☑ CTI Interface
☑ Bluetooth Interface
☑ Phone Manager
☑ USB Interface

☑ Debug Interface
☑ WBM Interface
☑ SNMP Interface
☑ Resource Sharing
☑ PC Interface
☑ FTP
☑ USB Backup/Restore

☑ Factory Reset by Digit Key Combination

CCE Ports:
Serial Port Mode:

Service Agent

Checkbox for activating and deactivating the service agent.

Probe Interface

Checkbox for activating and deactivating the probe interface.

Test Interface

Checkbox for activating and deactivating the test interface.

CTI Interface

Checkbox for activating and deactivating the CTI interface.

Bluetooth Interface

This checkbox is activated if you want to activate the Bluetooth interface on OpenStage telephones.

Phone Manager

This checkbox is activated if you want to enable the interface between OpenStage telephones and Phone Manager.

Phone Manager is a PC application for managing particular phone data.

USB Interface

If this checkbox is activated, the USB interface on the IP device can be accessed (OpenStage 60 and OpenStage 80 only).

Debug Interface

Checkbox for activating and deactivating the debug interface.

WBM Interface

Checkbox for activating and deactivating the WBM interface.

> Please note that if you deactivate the WBM interface, you can only reactivate it via DLS as the WBM is no longer available for this.

SNMP Interface

Checkbox for activating and deactivating the SNMP interface (network management function).

Resource Sharing

Checkbox for activating and deactivating resource sharing (shared use of mouse and keyboard).

PC Interface

This checkbox is activated if you want to use the PC interface.

FTP

This checkbox is activated if you want to enable the FTP interface on the OpenStage telephone.

USB Backup/Restore

If this checkbox is activated, IP device data (such as, the screensaver) can be backed up/restored over the USB interface. Codec’s Backup/Restore feature must be called directly on the relevant IP device (OpenStage 60 and OpenStage 80 only).

Factory Reset by Digit Key Combination

When activated, the factory reset by means of a digit key combination is enabled.

CEE Ports

Enable or disable the Comms Channel Extender (CCE) ports for both TCP (port 65531) and UDP (port 65530) access.

Possible Options:

- **Disable all**
- **Enable all**
- **TCP only**
- **UDP only**

Serial Port Mode

Shows password protection mode for the serial port.

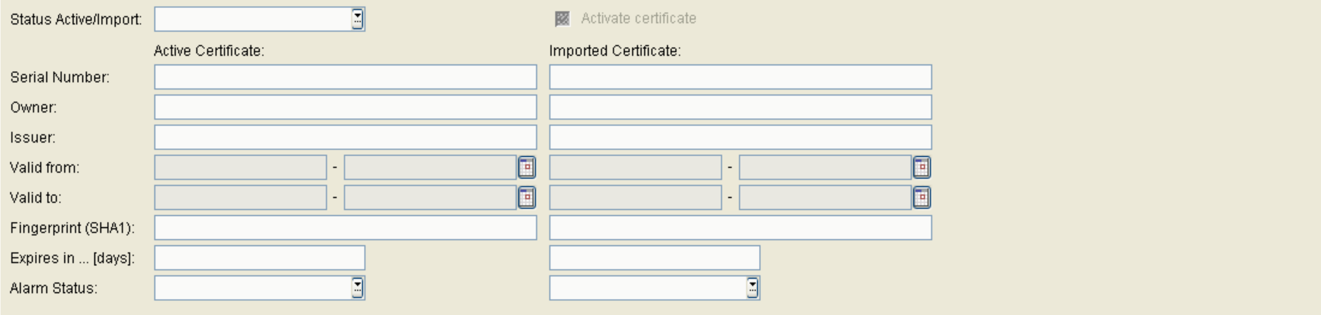
Possible Options

- **Password required**
- **No Password**
- **Unavailable**

7.1.7.4 "WBM Server Certificate" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "WBM Server Certificate" Tab

For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".



Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm **SHA1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]

The certificate validity will expire in the number of days specified.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

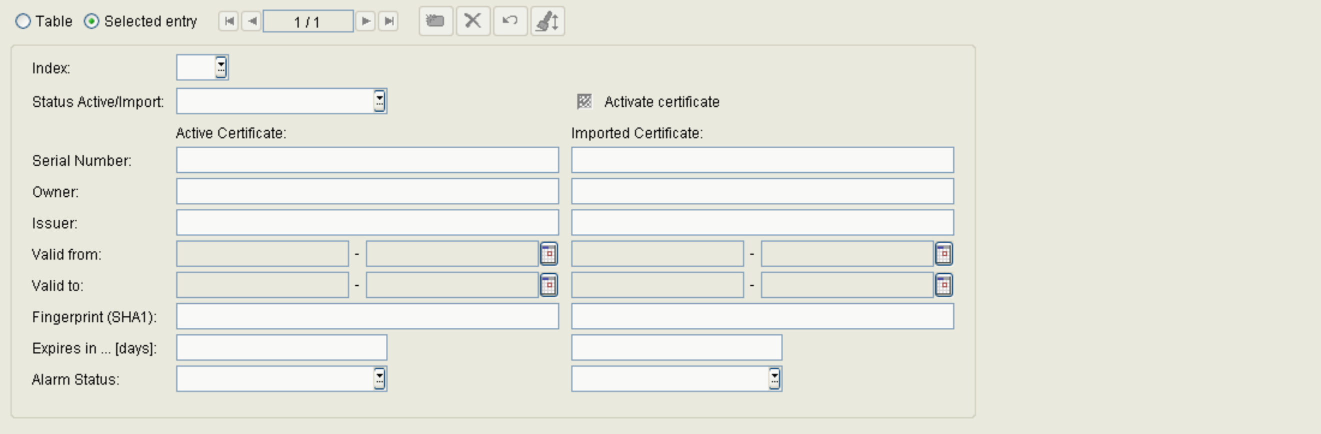
Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.7.5 "HTTPS Server CA Certificates" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "HTTPS Server CA Certificates" Tab

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".



Index

Index of the certificate.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm **SHA1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]

The certificate validity will expire in the number of days specified.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

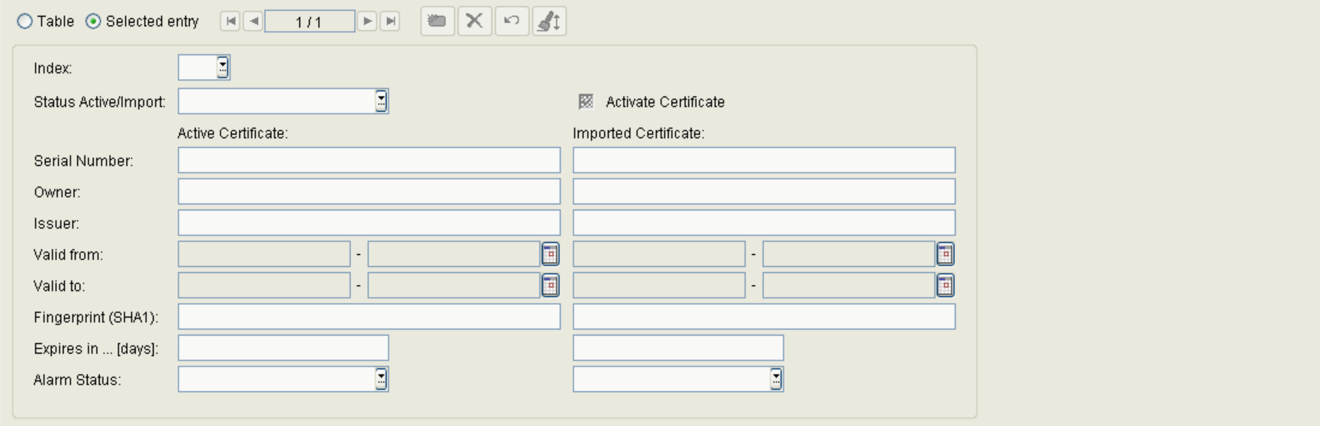
Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.7.6 "OCSR 1 Server CA Certificate" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "OCSR 1 Server CA Certificate" Tab

For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".

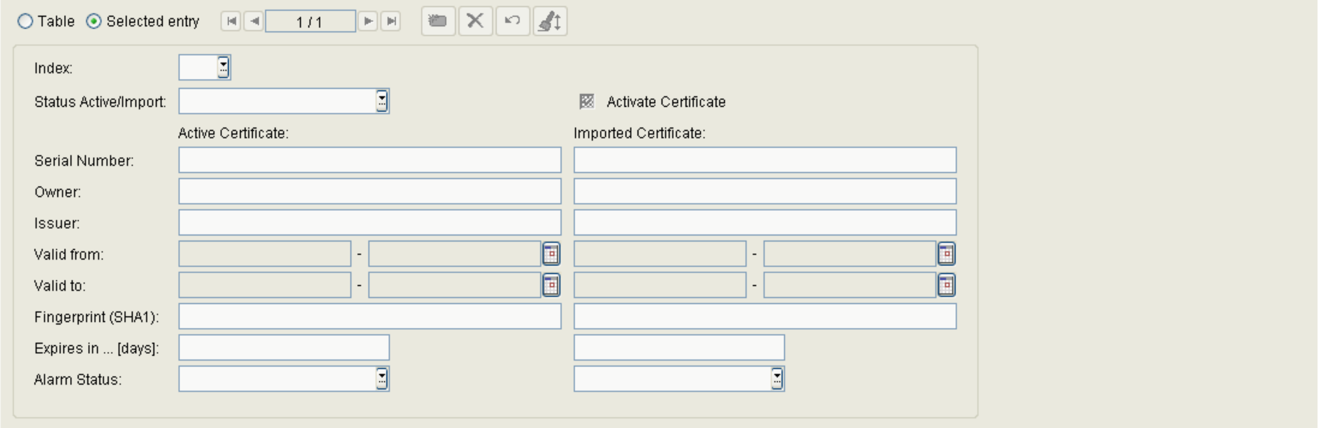


For parameter descriptions, please see Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab".

7.1.7.7 "OCSR 2 Server CA Certificate" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "OCSR 2 Server CA Certificate" Tab

For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".

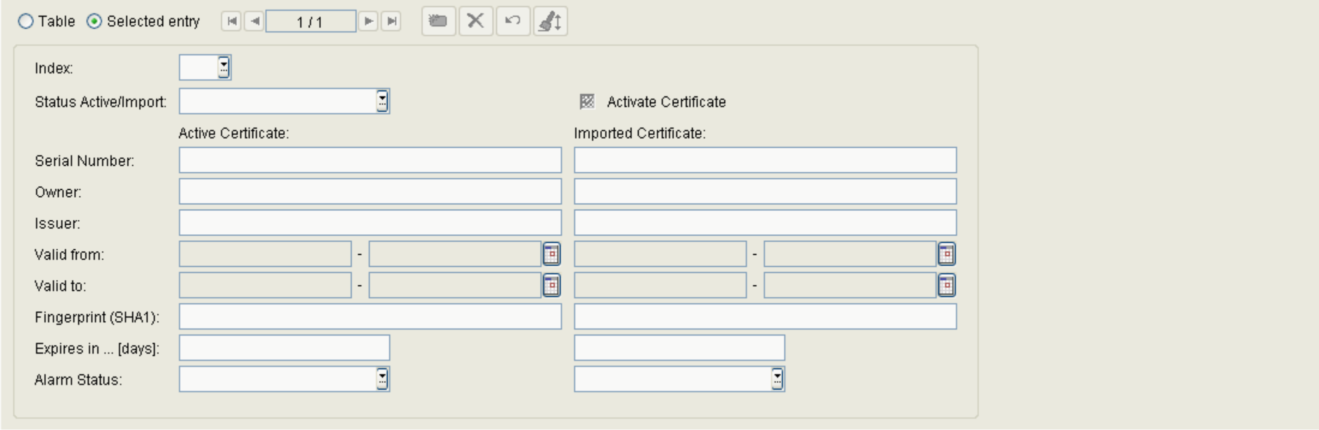


For parameter descriptions, please see Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab".

7.1.7.8 "OCSR 1 Signature CA Certificate" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "OCSR 1 Signature CA Certificate" Tab

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".

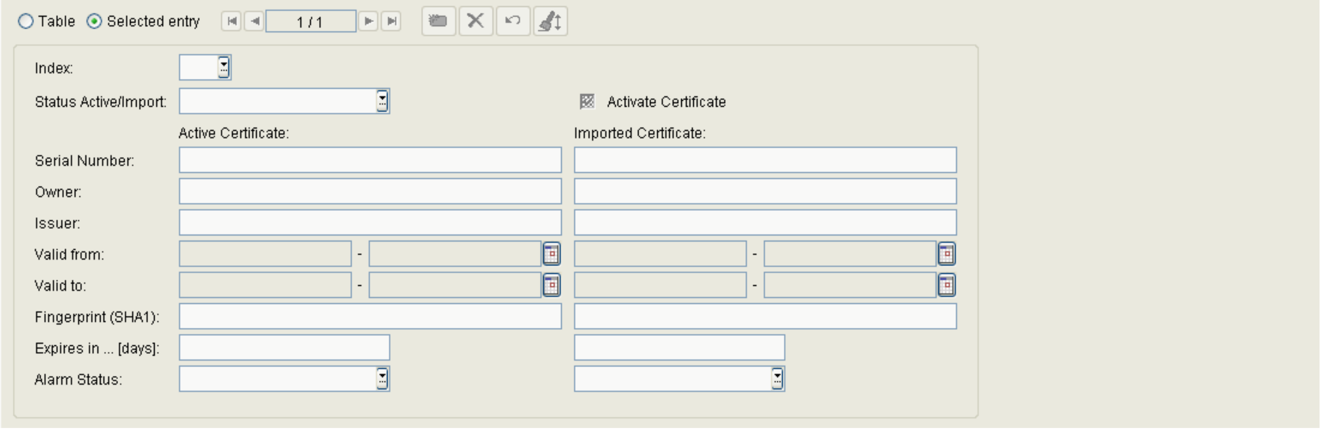


For parameter descriptions, please see Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab"

7.1.7.9 "OCSR 2 Signature CA Certificate" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "OCSR 2 Signature CA Certificate" Tab

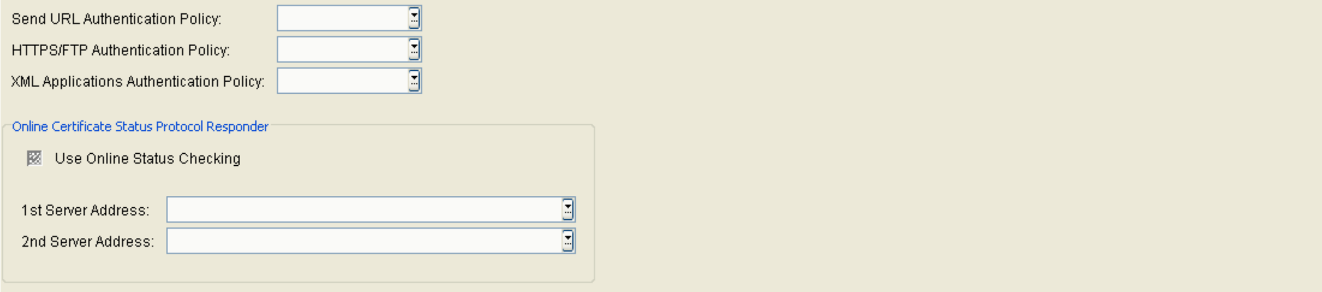
> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".



For parameter descriptions, please see Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab"

7.1.7.10 "Certificate Policy" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Security Settings > "Certificate Policy" Tab



Send URL Authentication Policy:

HTTPS/FTP Authentication Policy:

XML Applications Authentication Policy:

Online Certificate Status Protocol Responder

☒ Use Online Status Checking

1st Server Address:

2nd Server Address:

Send URL Authentication Policy:

Possible values:

- **None**
- **Trusted**
- **Full**

HTTPS/FTP Authentication Policy

Possible values:

- **None**
- **Trusted**
- **Full**

XML Applications Authentication Policy:

Possible values:

- **None**
- **Trusted**
- **Full**

Online Certificate Status Protocol Responder

Use Online Status Checking

Checkbox to activate online status checking.

1st Server Address

Address of the first server for the certificate status protocol.

2nd Server Address

Address of the secondary server for the certificate status protocol.

7.1.8 Telephony

Call: Main Menu > IP Devices > IP Phone Configuration > Telephony

This area features the following components:

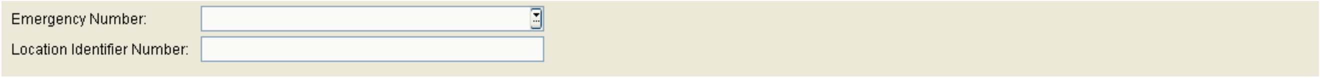
- General Data
- Possible Action Buttons
- "Telephony" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.8.1 "Telephony" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Telephony > "Telephony" Tab


Emergency Number:
Location Identifier Number:

Emergency Number:

Contains the phone number that can be dialed in an emergency.

Location Identifier Number:

Contains an identification number for unique location identification. This number can be used, for example, to pinpoint the **origin** of an emergency call.

7.1.9 Small Remote Site Redundancy

Call: Main Menu > IP Devices > IP Phone Configuration > Small Remote Site Redundancy

This area features the following components:

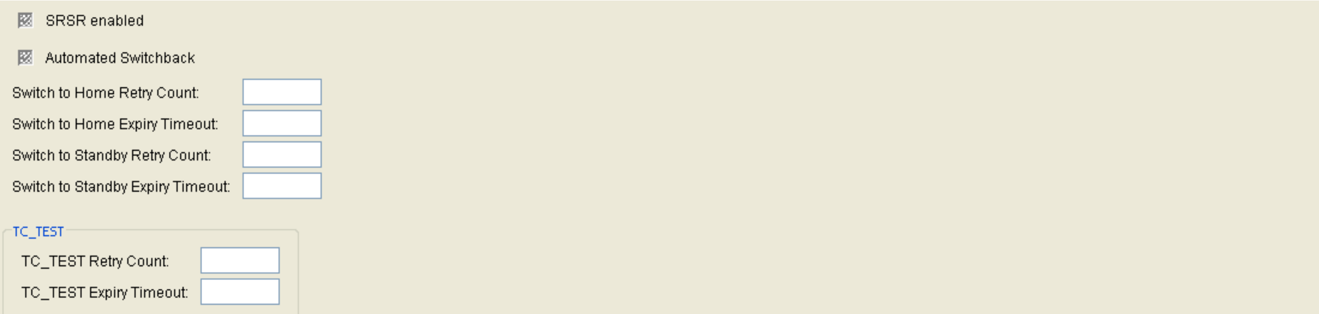
- General Data
- Possible Action Buttons
- "SRSR Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.9.1 "SRSR Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Small Remote Site Redundancy > "SRSR Settings" Tab



▨ SRSR enabled

▨ Automated Switchback

Switch to Home Retry Count:

Switch to Home Expiry Timeout:

Switch to Standby Retry Count:

Switch to Standby Expiry Timeout:

TC_TEST

TC_TEST Retry Count:

TC_TEST Expiry Timeout:

SRSR enabled:

Checkbox for activating small remote site redundancy.

Only available in HFA workpoints.

Automated Switchback:

Checkbox for activating the option for automatic switchback to the main system.

Only available in HFA workpoints.

Switch to Home Retry Count:

Specifies the number of attempts permitted when switching back to the main system.

Value range: **1** ... **255**

Only available in HFA workpoints.

Switch to Home Expiry Timeout:

Timeout for switchover to the main system.

Value range: **1** ... **255** seconds.

Only available in HFA workpoints.

Switch to Standby Retry Count:

Specifies the number of attempts permitted when switching back to the standby system.

Value range: **1** ... **255**

Only available in HFA workpoints.

Switch to Standby Expiry Timeout:

Timeout for switchover to the standby system.

Value range: **1** ... **255** seconds.

Only available in HFA workpoints.

TC_Test

TC_TEST Retry Count:

Specifies the number of positive attempts permitted when switching back to the main system.

Value range: **1** ... **255**

Only available in HFA workpoints.

TC_TEST Expiry Timeout:

Time for a renewed attempt to switch back to the main system.

Value range: **1** ... **255** seconds.

Only available in HFA workpoints.

7.1.10 Dialing Properties

Call: Main Menu > IP Devices > IP Phone Configuration > Dialing Properties

This area features the following components:

- General Data
- Possible Action Buttons
- "Dialing Properties" Tab
- "Canonical Dial Lookup" Tab

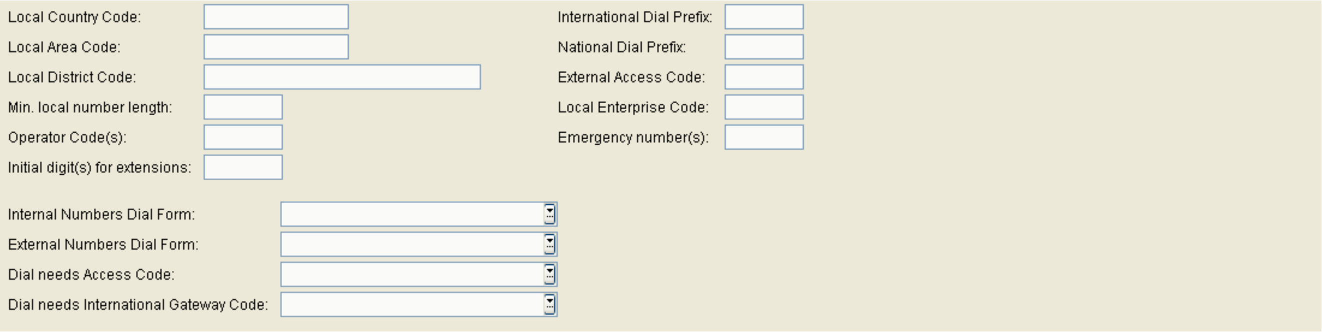
For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.10.1 "Dialing Properties" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Dialing Properties > "Dialing Properties" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").



Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

Local District Code:

Phone number of the company network.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **722** for Siemens Munich Hofmannstraße.

Only available for devices in the optiPoint family.

Min. local number length

Minimum length for a local phone number, that is, within a prefix area.

Example: In Munich (prefix area 089), the minimum length is **6**.

Only available for devices in the OpenStage family.

Operator Code(s):

Number/code for connection to the operator.

Only available for devices in the OpenStage family.

Initial digit(s) for extensions

List of initial digits of all possible extensions in the local enterprise network. When a call number could not be matched as a public network number, the phone checks if it is part of the local enterprise network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly.

Example: If, the extensions 3000-5999 are configured in the OpenScape Voice, each number will start with 3, 4, or 5. Therefore, the digits to be entered are **3, 4, 5**.

International Dial Prefix:

National prefix.

Format: Up to four digits.

Example: **00** in Germany.

National Dial Prefix:

International prefix.

Format: Up to five digits.

Example: **0** in Germany.

External Access Code:

Number for trunk seizure for an outgoing external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Local Enterprise Node:

Call number of the company network.

Example: **722** for Siemens Munich Hofmannstraße.

Only available for devices in the OpenStage family.

Emergency number(s):

One or more emergency numbers can be entered here.

Only available for devices in the OpenStage family.

Internal Numbers Dial Form:

Possible options:

- **Local Company Format**
- **Always Add Node**
- **Use External Number**

External Numbers Dial Form:

Possible options:

- **Local Public Format**
- **National Public Format**
- **International Public Format**

Dial needs Access Code:

Possible options:

- **Not used**
- **For External Number**

Dial needs International Gateway Code

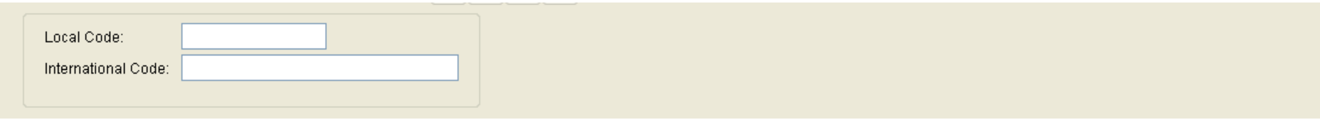
Possible options:

- **Use National Code**
- **Unchanged**

7.1.10.2 "Canonical Dial Lookup" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Dialing Properties > "Canonical Dial Lookup" Tab

This function transforms the entries in the first field ("Local Area Code") on the basis of a particular digit string as specified in the second field ("International Dial Code"). This digit string can be a national or international dial prefix, for example. This allows you to dial frequently used prefixes by entering just one digit.



Local Code:

International Code:

Local Code

Digit or short digit string for dialing a particular prefix, for example.

International Code

Digit string, such as, a prefix, that is dialed at the beginning of the dialing operation using a particular digit.

7.1.11 Time Parameters

Call: Main Menu > IP Devices > IP Phone Configuration > Time Parameters

This area features the following components:

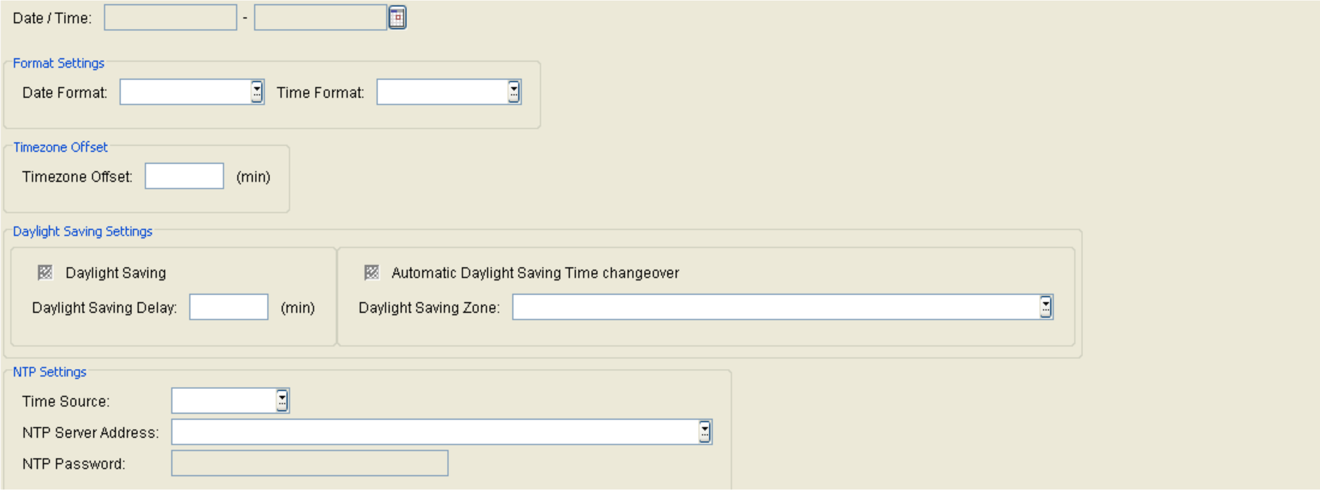
- General Data
- Possible Action Buttons
- "Time" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.11.1 "Time" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Time Parameters > "Time" Tab



Date / Time:

Enter current date and time. Manual entry is only necessary if this information is not automatically transmitted (for example, PBX or DHCP server).

Format Settings

Date Format:

Format for date entry. Manual entry is only necessary if this information is not automatically transmitted by the communications system (for example, OpenScape Voice).

Possible options:

- **DD.MM.YY**
  Example: 05.10.06 for 5.10.2006
- **YY-MM-DD**
  Example: 04-10-06 for 5.10.2006
- **MM/DD/YY**
  Example: 10/05/06 for 5.10.2006

Time Format:

Time format.

Possible options:

- **24 hours**
- **12 hours**

Timezone Offset

Timezone Offset:

Time offset from UTC (Coordinated Universal Time) in minutes.

Value range: **-720** ... **720**

Examples: **60** (phone residing in Munich); **-480** (phone residing in Los Angeles, USA).

Daylight Saving Settings

Daylight Saving

Checkbox for activating the Daylight Saving function.

> ℹ If **Automatic Daylight Saving Time changeover** is deactivated or no SNTP server is in use, you must manually switch between daylight saving and winter time. You must therefore change the status of the **Daylight Saving** checkbox twice a year. Pay particular attention to this when using this parameter in template data.

Daylight Saving Delay:

Difference in minutes to normal or winter time.

Value range: **0** ... **60**

Automatic Daylight Saving Time changeover:

If the checkbox is activated, the daylight saving time is toggled automatically according to the rule of the selecteddaylight saving zone. Start date and end date of daylight saving time are defined hereby.

> ℹ With OpenStage phones, the **Daylight Saving** switch must be activated to enable automatic daylight saving time changeover.

Daylight Saving Zone:

Possible options:

- **Not set**
- **Australia 2007 (ACT, South Australia, Tasmania, Victoria)**
- **Australien 2007 (New South Wales)**
- **Australien (Western Australia)**
- **Australien 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria)**
- **Brasilia**
- **Canada**

- **Canada (Newfoundland)**
- **Europe (PT, UK)**
- **Europe (AT, BE, HR, DK, FR, DE, HU, IT, LU, NL, NO, PL, SK, ES, SE, CH)**
- **Europe (FI)**
- **Mexico**
- **United States**

NTP Settings

Time Source:

Source from where time information is adopted.

Possible options:

- **System**
  The time information is obtained from the communication platform.
- **SNTP**
  The time information comes from the SNTP server (if available).

NTP Server Address:

IP address or host name of the SNTP server if an SNTP server is available.

NTP Password:

If required, a password is entered here for the SNTP server. This parameter is only available for OpenStage telephones.

7.1.12 Audio Settings

Call: Main Menu > IP Devices > IP Phone Configuration > Audio Settings

This area features the following components:

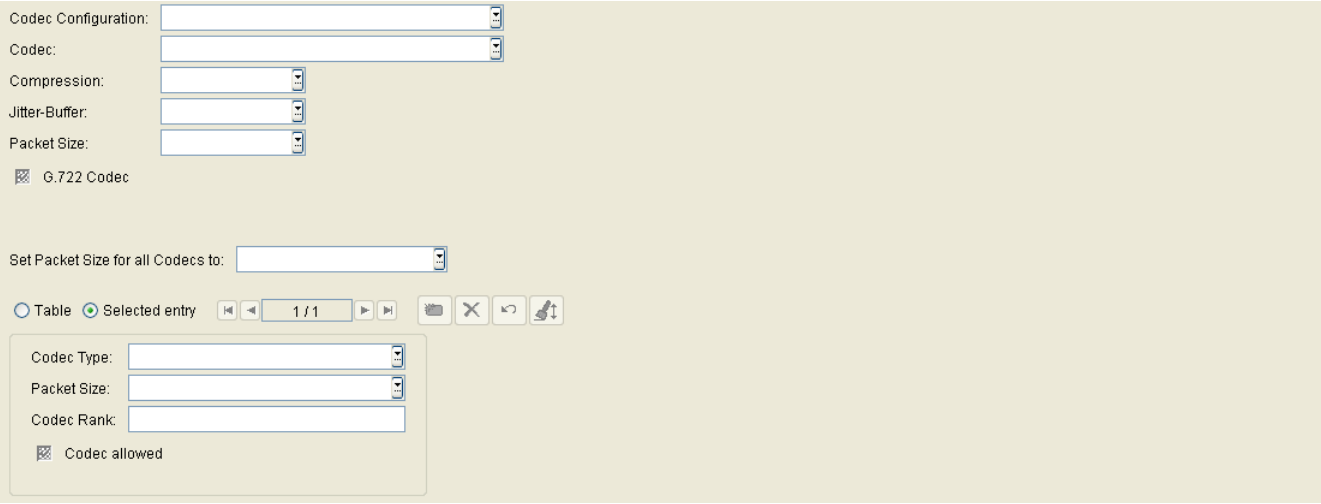
- General Data
- Possible Action Buttons
- "Codecs / Compressing" Tab
- "Codecs / Compressing (Standby)" Tab
- "Audio Settings" Tab
- "Audio Settings (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.12.1 "Codecs / Compressing" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Audio Settings > "Codecs / Compressing" Tab



The settings in the table are made for devices in the OpenStage family because the specification of multiple alternative codecs in these telephones is performed via a list of individual codecs.

Codec Configuration:

Set Codec for WLAN-Phones.

Possible options:

- **G.711 preferred (normal quality)**
- **G.722 preferred (high quality)**
- **G.723 preferred (low bandwidth)**
- **G.729 A/B preferred (low bandwidth)**
- **G.723 only (low bandwidth)**
- **G.729 A/B only (low bandwidth)**

Codec:

Audio transmission principle (codec) used.

Possible options:

- **Low bandwidth only**
  For the optiPoint 410/420/600 families.
- **High quality preferred**
  For the optiPoint 410/420/600 families.
- **Low bandwidth preferred**
  For the optiPoint 410/420/600 families.

- **G.711 Preferred**
  For the optiPoint 400 family.
- **G.723 Preferred**
  For the optiPoint 400 family.
- **G.723 Always**
  For the optiPoint 400 family.

Compression:

Compression procedure when the "LoBand" codec is selected.

Possible options:

- **G.723**
- **G.729**

Jitter Buffer:

Buffering duration (number of data packets).

Possible options:

- **Short**
  two packets
- **Long**
  six packets
- **Normal**
  four packets

Packet Size:

Possible options:

- **10mS**
- **20mS**
- **30mS**
- **Automatic**

G.722 Codec:

Checkbox for activating the G.722 codec.

Set Packet Size for all Codecs to:

Set the Packet Size of all codecs to a common value.

Possible options:

- **10 mS**
- **20 mS**
- **30 mS**

- **Automatic**

Codec Type

Audio transmission principle (codec) used.

Possible options:

- **G.711**
- **G.722**
- **G.729**

Packet Size

Size of the packet used to send the audio data packages. The entry is in milliseconds.

- **Automatic**
- **10 ms**
- **20 ms**
- **30 ms**

Codec Rank

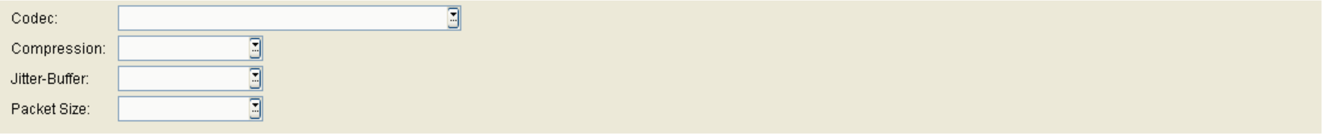
Each available codec is assigned a priority. This is used when negotiating codecs between two devices. Value range: A number between 1 and the number of available codecs.

Codec allowed

Codec usage can be explicitly allowed or denied.

7.1.12.2 "Codecs / Compressing (Standby)" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Audio Settings > "Codecs / Compressing (Standby)" Tab



Codec:

Compression:

Jitter-Buffer:

Packet Size:

Codec:

Audio transmission principle (codec) used.

Possible options:

- **Low bandwidth only**
  For the optiPoint 410/420/600 families.
- **High quality preferred**
  For the optiPoint 410/420/600 families.
- **Low bandwidth preferred**
  For the optiPoint 410/420/600 families.
- **G.711 Preferred**
  For the optiPoint 400 family.
- **G.723 Preferred**
  For the optiPoint 400 family.
- **G.723 Always**
  For the optiPoint 400 family.

Compression:

Compression procedure when the "LoBand" codec is selected.

Possible options:

- **G.723**
- **G.729**

Jitter Buffer:

Buffering duration (number of data packets).

Possible options:

- **Short**
  two packets
- **Long**
  six packets
- **Normal**
  four packets

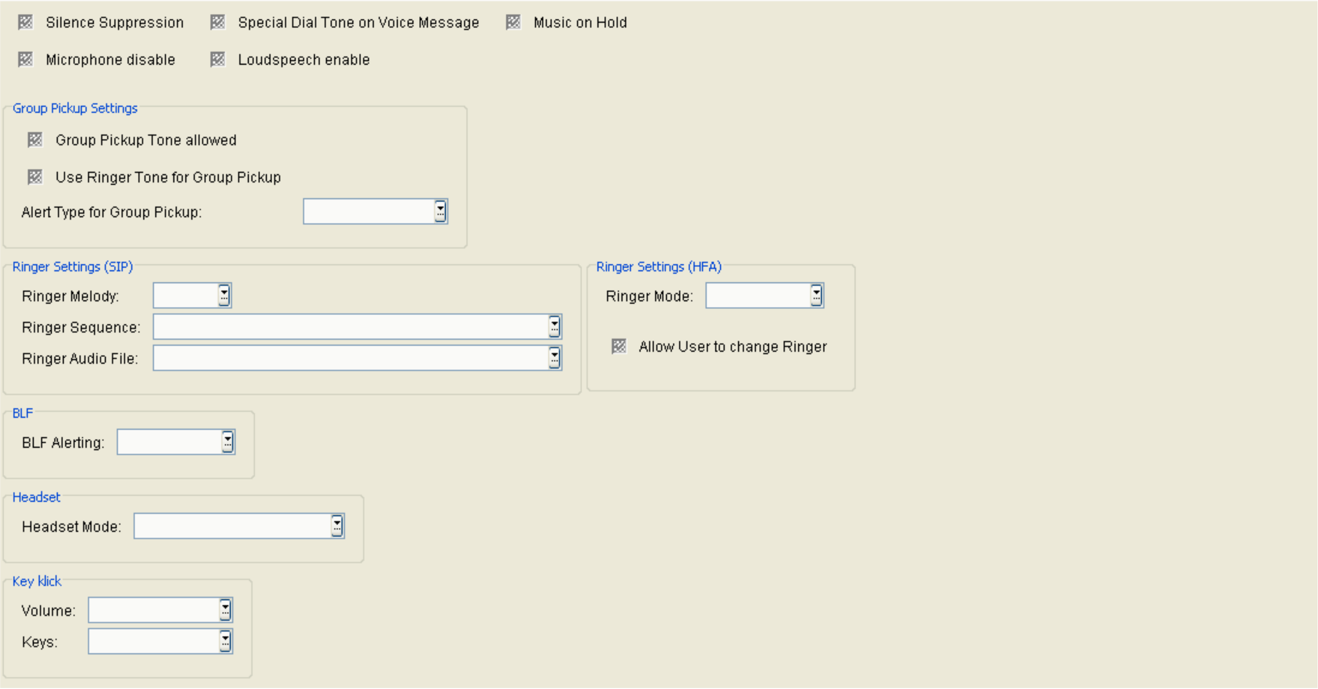
Packet Size:

Possible options:

- **10mS**
- **20mS**
- **30mS**

7.1.12.3 "Audio Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Audio Settings > "Audio Settings" Tab



▨ Silence Suppression ▨ Special Dial Tone on Voice Message ▨ Music on Hold

▨ Microphone disable ▨ Loudspeech enable

Group Pickup Settings

▨ Group Pickup Tone allowed

▨ Use Ringer Tone for Group Pickup

Alert Type for Group Pickup:

Ringer Settings (SIP)

Ringer Melody:

Ringer Sequence:

Ringer Audio File:

Ringer Settings (HFA)

Ringer Mode:

▨ Allow User to change Ringer

BLF

BLF Alerting:

Headset

Headset Mode:

Key klick

Volume:

Keys:

Silence Suppression

Checkbox for activating silence suppression.

Microphone disable

Checkbox for deactivating the microphone.

Special Dial Tone on Voice Message

If this checkbox is activated, a special dial tone is applied when you lift the handset to inform you that you have a new voice message.

Loudspeech enable

Checkbox for activating the speakerphone function.

Music on Hold

Checkbox to activate Music on Hold.

Rollover Ring Volume:

Volume for the ring tone that alerts an incoming call during a conversation.

Group Pickup Settings

Group Pickup Tone allowed

Activates or deactivates the generation of an acoustic signal for incoming pickup group calls.

Use Ringer Tone for Group Pickup

If this is checked, a pickup group call will be signaled by a short standard ringtone. If unchecked, a pickup group call will be signaled by an alert tone.

Alert type for Group Pickup:

Defines the user action required to accept a pickup call.

Possible Options:

- **Prompt**
  An incoming pickup call is signaled by an alert on the phone GUI. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured.
- **Notify**
  An incoming pickup call is signaled by an alert on the phone GUI. To accept the call, the user must confirm the alert or press the corresponding function key, if configured.

Ringer Settings (SIP)

Ringer Melody:

Possible Options:

No.	SIP	HFA	Frequencies (Hz)			Note Length (ms)		
			f1	f2	f3	c1	c2	c3
1	Yes	Yes	457	571	615	45	45	45
2	Yes	Yes	696	762	1067	30	30	30
3	Yes	Yes	400	444	500	35	35	35
4	Yes	Yes	1067	889	696	50	50	50
5	Yes	Yes	762	800	889	30	30	30
6	Yes	Yes	1000	1143	1333	40	40	40
7	Yes	Yes	400	457	593	50	50	50
8	Yes	Yes	533	0	667	90	150	60

Ringer Sequence:

Possible Options:

- **1 sec ON, 4 sec OFF**

- **1 sec ON, 2 sec OFF**
- **0.7 sec ON, 0.7 sec OFF, 0.7 sec OFF, 3 sec OFF**

Ringer Audio File

Name of the file that contains the ringtone.

Ringer Settings (HFA)

Ringer Mode

Possible Values:

- **HiPath**
- **Local Ringer**

Allow User to change Ringer

If switch is active, the user is allowed to change the ringtone.

BLF

BLF Alerting

Optical alerting by key.

Possible Values:

- **Beep**
- **Ring**

Headset

Headset Mode

Connection mode of headset.

Possible Values:

- **Wired Headset**
- **Cordless Headset**
- **Conference Unit**

Key klick

Volume

Defines the volume of key clicks.

Possible Values:

- **Off**

- **Low**
- **Medium**
- **High**

Keys

Defines which keys shall have audible clicks.

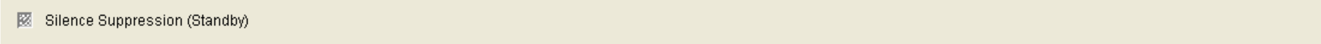
Possible Values:

- **Keypad only**
- **All keys**

7.1.12.4 "Audio Settings (Standby)" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Audio Settings > "Audio Settings (Standby)" Tab

This "standby" data is used when the "home" data for the "Audio Settings" Tab is not available. The SRSR functionality must be configured for this, see Section 7.1.9, "Small Remote Site Redundancy".



☒ Silence Suppression (Standby)

Silence Suppression (Standby)

Checkbox for activating silence suppression.

7.1.13 SNMP Settings

Call: Main Menu > IP Devices > IP Phone Configuration > SNMP Settings

This area features the following components:

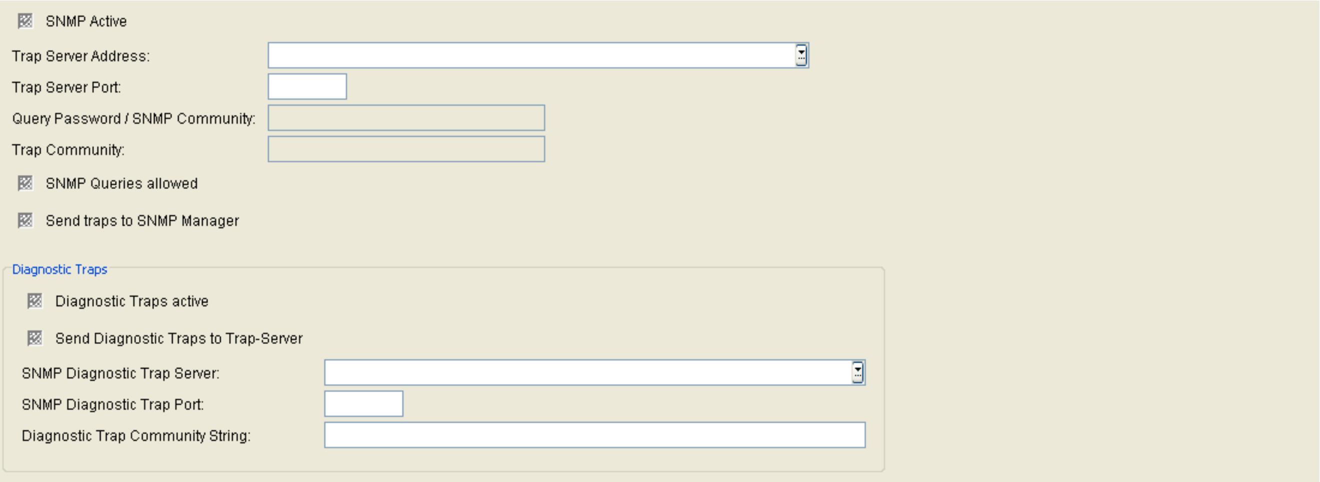
- General Data
- Possible Action Buttons
- "SNMP" Tab
- "Certificate Trap Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.13.1 "SNMP" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > SNMP Settings > "SNMP" Tab



▨ SNMP Active

Trap Server Address:

Trap Server Port:

Query Password / SNMP Community:

Trap Community:

▨ SNMP Queries allowed

▨ Send traps to SNMP Manager

Diagnostic Traps

▨ Diagnostic Traps active

▨ Send Diagnostic Traps to Trap-Server

SNMP Diagnostic Trap Server:

SNMP Diagnostic Trap Port:

Diagnostic Trap Community String:

SNMP Active

Checkbox for activating the SNMP function.

Trap Listener Address:

IP address or host name of the SNMP trap server.

Trap Listener Port:

Port number of the SNMP trap server.

Query Password / SNMP Community:

Community string used for authorization on the SNMP server.

Trap Community:

SNMP community string for the SNMP manager receiving trap messages.

SNMP Queries allowed

Checkbox for activating authorization to query QDC data via SNMP.

Send Traps to SNMP Manager

Checkbox for activating the function that also sends QDC data to an SNMP manager.

Diagnostic Traps

Diagnostic Traps active

If this checkbox is active, diagnostic traps are sent.

Send Diagnostic Traps to Trap Server

If this checkbox is active, the diagnostic traps are sent to the trap server configured.

SNMP Diagnostic Trap Server:

Host name or IP address of the SNMP server that receives diagnostic traps.

SNMP Diagnostic Trap Port:

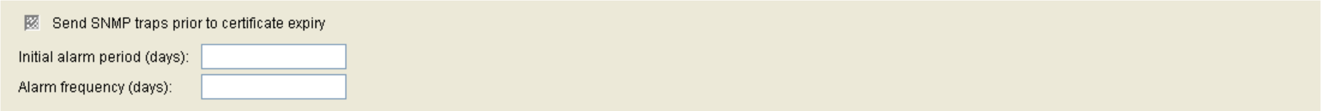
Port used by the SNMP server to receive diagnostic traps.

Diagnostic Trap Community String:

Community string for authentication on the SNMP server that receives diagnostic traps.

7.1.13.2 "Certificate Trap Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > SNMP Settings > "Certificate Trap Settings" Tab



☑ Send SNMP traps prior to certificate expiry

Initial alarm period (days):

Alarm frequency (days):

Send SNMP traps prior to certificate expiry

If this checkbox is activated, SNMP traps are sent for expired certificates to the address entered under the SNMP settings (see "SNMP" Tab).

Initial alarm period (days):

Number of days before certificate expiry when the SNMP trap is sent.

Alarm frequency (days)

Number of days before an SNMP trap for an expired certificate is resent.

7.1.14 Applications

Call: Main Menu > IP Devices > IP Phone Configuration > Applications

This area features the following components:

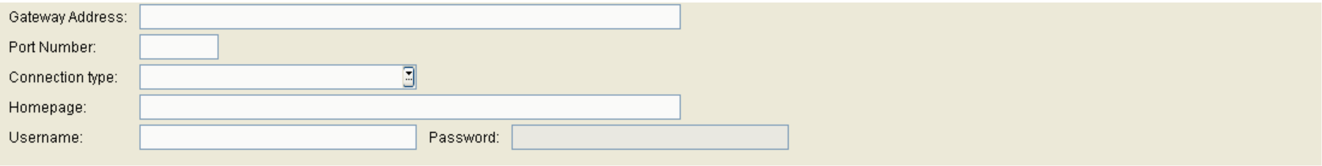
- General Data
- Possible Action Buttons
- "WAP" Tab
- "Java" Tab
- "XML Applications" Tab
- "CA Certificates" Tab
- "Application List" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.14.1 "WAP" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Applications > "WAP" Tab



Gateway Address:

IP address or host name of the WAP server.

Port Number:

Port number of the WAP server.

Connection type:

Protocol type for connection to the WAP server.

Possible options:

- **HTTP**
- **WSP**

Homepage:

URL of the splash screen where the WAP home page is located.

Username

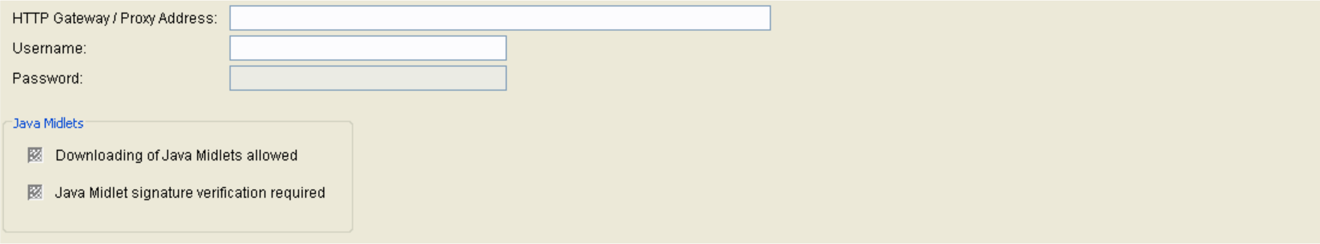
User ID for identification at the WAP server

Password:

Password for the user ID.

7.1.14.2 "Java" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Applications > "Java" Tab



HTTP Gateway / Proxy Address:

Username:

Password:

Java Midlets

▨ Downloading of Java Midlets allowed

▨ Java Midlet signature verification required

HTTP Gateway/Proxy Address:

IP address or host name of the HTTP server.

Username:

User ID for identification at the HTTP gateway.

Password:

Password for the user ID.

Java Midlets

Downloading of Java Midlets allowed

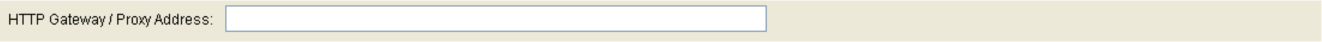
If this checkbox is activated, you can download Java midlets to the workpoint.

Java Midlet signature verification required

If this checkbox is activated, the Java midlet must be verified using a signature.

7.1.14.3 "Java (Standby)" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Applications > "Java" Tab



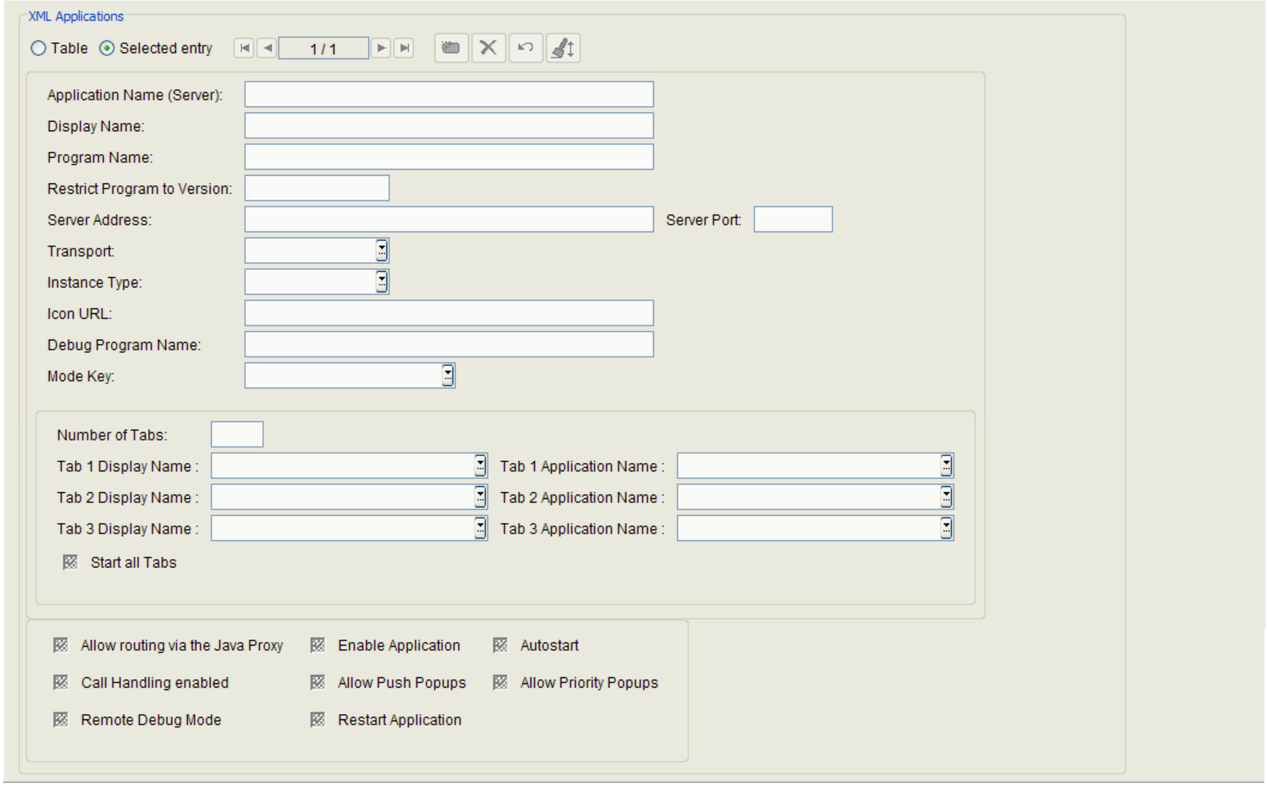
HTTP Gateway / Proxy Address:

HTTP Gateway/Proxy Address:

IP address or host name of the HTTP server.

7.1.14.4 "XML Applications" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Applications > "XML Applications" Tab



These are server-side applications which communicate with the phone software via a specially defined XML interface. The Unified Messaging system HiPath Xpressions also uses this interface. The interface enables the workpoint to send user entries, to display data in textual and graphic form, and to control calls.

To set up an XML application on the workpoint, the following specifications are required: a freely selectable user name, communication protocol to be used; server port to be used; start address of the server-side program.

XML applications are only available in OpenStage 60/80.

XML Applications

Application Name (Server):

This is the name of the HTTP servlet, and it is used internally by the workpoint software to identify the application.

For DLS XML applications, the names must be entered unchangend.

Possible values:

- **DeploymentService**
- **LocationService**
- **NewsService**
- **MakeCall**

Display Name:

This name is used for listing the application on the workpoint menu.

Program Name:

Path of the start file of the server-side program, in relation to the server address. For DLS XML applications, enter the WEB application name, followed by the HTTP servlet name.

Restrict Program to Version:

Server Address:

IP address of the server on which the program is running. For DLS XML Applications enter the IP address of the DLS Server; for MultiNode installations, enter the IP address of the cluster.

Example: **192.168.1.150**

Server Port:

Port used by the server-side program for receiving data from the workpoint. For DLS XML Applications use port 18080, as only HTTP is supported.

Examples: **80** (Apache default port); **8080** (Tomcat default port).

Transport:

Transport protocol used for transmitting XML data.

Possible options:

- **HTTP**
- **HTTPS**

Instance Type:

Selection of the type of instance.

Possible options:

- **Normal**
- **Xpressions**
- **Phonebook**

Icon URL:

URL of the application icon (not yet implemented).

Debug Program Name:

Name and, where applicable, directory path of the program on the server that receives error messages from the terminal's *.XML application platform.

Mode Key:

Select a mode key to start the application.

Possible options:

- **No Mode Key**
- **Phonebook Mode Key**
- **CallLog Mode Key**
- **Messages Mode Key**
- **Help Mode Key**

Number of Tabs:

The number of embedded tabs within the XML application to be shown on phone display.

Value range: **0** ... **3**

> ⓘ For an XML-application with a number of Tabs > 0, one of the entries between **Tab 1 Application Name** and **Tab 3 Application Name** must be set to the same value as the **Application Name (Server)** that it is associated with. When the XML application is started, the tab which has the same name as the XML application is the tab that initially gets focus.

Tab 1 Display Name:

Labeling displayed on the 1st tab header.

Tab 2 Display Name:

Labeling displayed on the 2nd tab header.

Tab 3 Display Name:

Labeling displayed on the 3rd tab header.

Tab 1 Application Name:

The name used by the XML application to identify the application running under the 1st tab. The name must be unique over all XML-applications.

Tab 2 Application Name:

The name used by the XML application to identify the application running under the 2nd tab. The name must be unique over all XML-applications.

Tab 3 Application Name:

The name used by the XML application to identify the application running under the 3rd tab. The name must be unique over all XML-applications.

Start all Tabs

On application start, all tabs will be opened.

Allow routing via the Java Proxy

Enable Application

Autostart

Call Handling enabled

Allow Push Popups

Allow Priority Popups

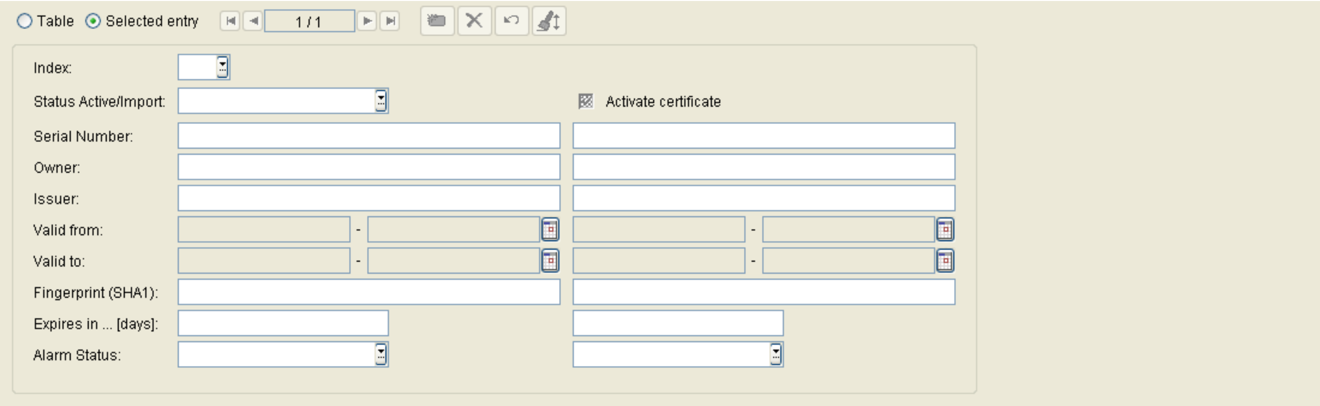
Remote Debug Mode

Restart Application

Restart Application, if it is already running.

7.1.14.5 "CA Certificates" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Applications > "CA Certificates" Tab



The parameters described below are available once for the currently active certificate and once for the imported certificate.

Index:

Serial number of the CA certificate.

Status Active/Import:

Specifies whether a certificate is registered as imported and/or active on the phone. The five statuses listed below are possible.

Possible values:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA 1):

This is the fingerprint extracted from the certificate.

Expires in ... [days]:

Number of days before the certificate expires.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Displays the duration of validity for certificates when searching for certificates due to expire.

Possible values:

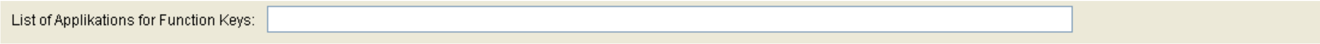
- **valid**
- **soon running out**
- **expired**

Activate certificate

Checkbox for activating the certificate. The active certificate is used to encrypt calls. The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

7.1.14.6 "Application List" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Applications > "Application List" Tab



List of Applikations for Function Keys:

List of Applications for Function Keys

Comma-separated list of names for applications which can be started by means of Function Keys.

7.1.15 LDAP

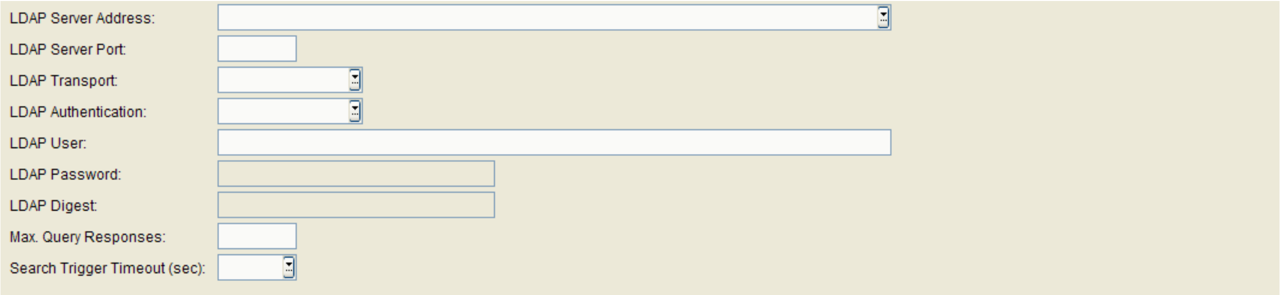
Call: Main Menu > IP Devices > IP Phone Configuration > LDAP

This area features the following components:

- General Data
- Possible Action Buttons
- "LDAP Settings" Tab
- "CA Certificates" Tab

7.1.15.1 "LDAP Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > LDAP > "LDAP Settings" Tab



LDAP Server Address:

IP address or host name of the LDAP server.

LDAP Server Port:

Port number of the LDAP server.

LDAP Transport:

Transport protocol used to transmit LDAP data.

Possible options:

- **TCP**

LDAP Authentication:

Option for selecting the LDAP access.

Possible options:

- **Anonymous**
- **Simple**

LDAP User:

User name for authenticated LDAP access.

LDAP Password:

Password for authenticated LDAP access.

LDAP Digest:

Max. Query Responses:

Maximum number of results in an LDAP search.

Search Trigger Timeout (sec):

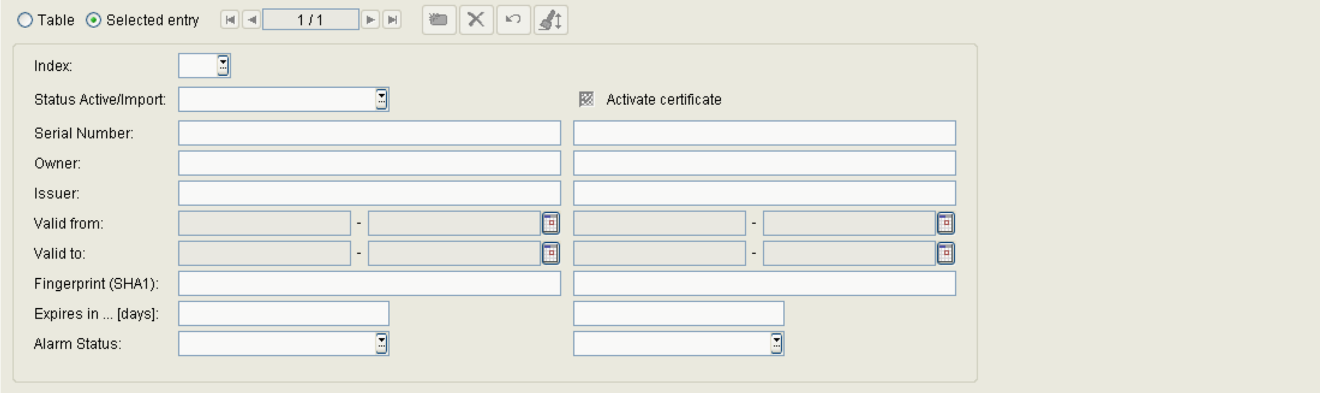
Search Trigger Timeout for LDAP simple search.

Possible options:

- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**
- **60**

7.1.15.2 "CA Certificates" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > LDAP > "CA Certificates" Tab



Index

Certificate index number.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm **SHA1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

> ℹ The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.16 User Settings

Call: Main Menu > IP Devices > IP Phone Configuration > User Settings

This area features the following components:

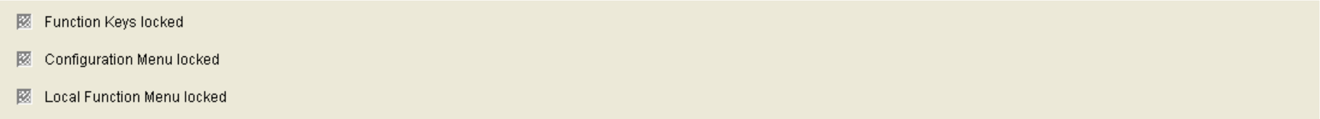
- General Data
- Possible Action Buttons
- "Locks" Tab
- "Locked Configuration Menus" Tab
- "Locked Local Functions" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.16.1 "Locks" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > User Settings > "Locks" Tab



☑ Function Keys locked

☑ Configuration Menu locked

☑ Local Function Menu locked

Function Keys locked

Checkbox for locking function keys on the Mobility Phone for a Mobile User.

Configuration Menus locked

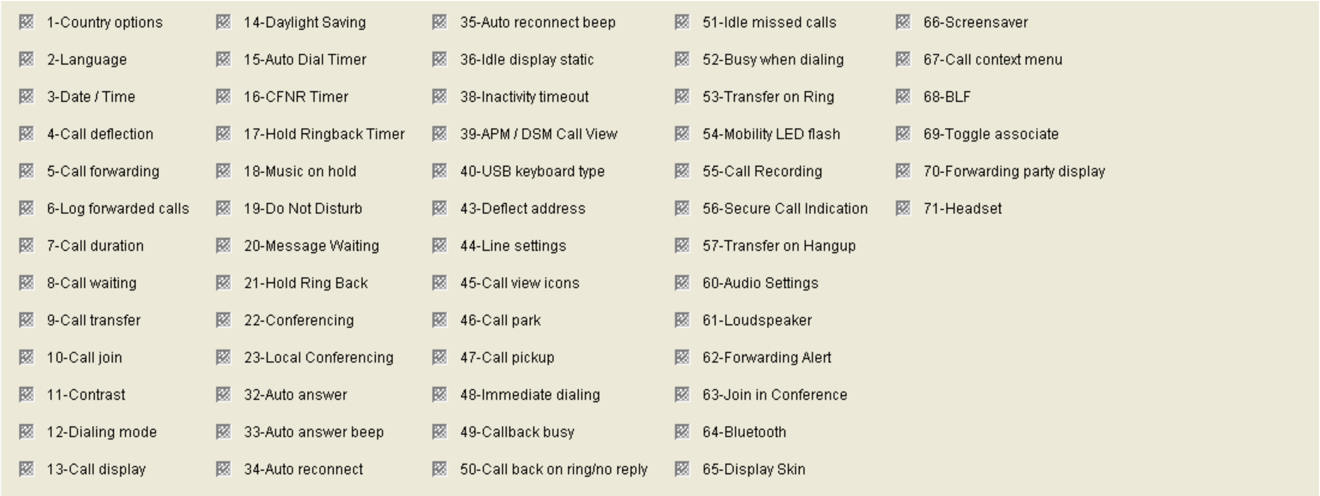
Checkbox for locking configuration menus on the Mobility Phone for a Mobile User.

Local Function Menus locked

Checkbox for locking local function menus on the Mobility Phone for a Mobile User.

7.1.16.2 "Locked Configuration Menus" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > User Settings > "Locked Configuration Menus" Tab



- ☒ 1-Country options
- ☒ 2-Language
- ☒ 3-Date / Time
- ☒ 4-Call deflection
- ☒ 5-Call forwarding
- ☒ 6-Log forwarded calls
- ☒ 7-Call duration
- ☒ 8-Call waiting
- ☒ 9-Call transfer
- ☒ 10-Call join
- ☒ 11-Contrast
- ☒ 12-Dialing mode
- ☒ 13-Call display
- ☒ 14-Daylight Saving
- ☒ 15-Auto Dial Timer
- ☒ 16-CFNR Timer
- ☒ 17-Hold Ringback Timer
- ☒ 18-Music on hold
- ☒ 19-Do Not Disturb
- ☒ 20-Message Waiting
- ☒ 21-Hold Ring Back
- ☒ 22-Conferencing
- ☒ 23-Local Conferencing
- ☒ 32-Auto answer
- ☒ 33-Auto answer beep
- ☒ 34-Auto reconnect
- ☒ 35-Auto reconnect beep
- ☒ 36-Idle display static
- ☒ 38-Inactivity timeout
- ☒ 39-APM / DSM Call View
- ☒ 40-USB keyboard type
- ☒ 43-Deflect address
- ☒ 44-Line settings
- ☒ 45-Call view icons
- ☒ 46-Call park
- ☒ 47-Call pickup
- ☒ 48-Immediate dialing
- ☒ 49-Callback busy
- ☒ 50-Call back on ring/no reply
- ☒ 51-Idle missed calls
- ☒ 52-Busy when dialing
- ☒ 53-Transfer on Ring
- ☒ 54-Mobility LED flash
- ☒ 55-Call Recording
- ☒ 56-Secure Call Indication
- ☒ 57-Transfer on Hangup
- ☒ 60-Audio Settings
- ☒ 61-Loudspeaker
- ☒ 62-Forwarding Alert
- ☒ 63-Join in Conference
- ☒ 64-Bluetooth
- ☒ 65-Display Skin
- ☒ 66-Screensaver
- ☒ 67-Call context menu
- ☒ 68-BLF
- ☒ 69-Toggle associate
- ☒ 70-Forwarding party display
- ☒ 71-Headset

The following functions can be locked for the Mobile User in the configuration menus by activating the relevant checkbox:

1-Country options

The user can select a country from a list to adapt the phone to country specific conditions.

2-Language

The user can set the language for the administration and user menu.

3-Date / Time

The user can set the local time, the current date, and the daylight saving time.

4-Call deflection

The user can activate or deactivate call deflection.

5-Call forwarding

The user can activate or deactivate call forwarding.

6-Log forwarded calls

The user can activate or deactivate the logging of forwarded calls.

7-Call duration

The user can determine whether the call duration is indicated on the display.

Only available in optiPoint workpoints.

8-Call waiting

The user can determine whether a second call is allowed during a connected call. If not, the caller hears the busy tone.

9-Call transfer

The user can allow call transfer.

10-Transfer call

The user can enable or disable the posibility to interlink an active and a held call.

11-Contrast

The user can set the contrast for the display.

12-Dialing mode

The user can determine whether a number only or, alternatively, a name can be used for dialing.

Only available in optiPoint workpoints.

13-Call display

The user defines which information about the caller is displayed on an incoming call.

Only available in optiPoint workpoints.

14-Daylight Saving

The user can set the daylight saving time.

15-Auto dial timer

The delay time between the entry of the last call number digit and the start of the dialing process can be set by the user.

16-CFNR timer

The user can set the delay time that passes before a call is forwarded, if Call Forwarding on No Reply is activated.

17-Hold ringback timer

The user can set the time delay, after which the workpoints indicates that there us a held call.

18-Music on hold

The user can determine whether the music on hold stored in the phone is used. If music on hold is activated, it is played as soon as the phone is put to hold.

19-Do not disturb

The user can determine whether Do Not Disturb is available on the phone. If Do Not Disturb is active, the phone will not ring on an incoming call, and the caller will hear the busy tone.

20-Message waiting

The user can determine whether new messaes in the mailbox are signaled by a LED.

Only available in optiPoint workpoints.

21-Hold ring back

If this function is active and a participant has been put to hold, a signal sounds after a configurable time to remind that a call is on hold. The user can allow this function and set the delay time for the acoustic signal.

22-Conference

The user can allow system based conferences.

Only available in optPoint workpoints.

23-Local conference

The user can allow local 3-party conferences.

32-Auto answer

The user can determine whether incoming calls are accepted automatically by the CTI application which is connected to the phone.

33-Auto answer beep

The user can determine whether a signal will sound when a call that is accepted automatically by the CTI application connected to the phone.

34-Auto reconnect

The user can determine whether a held call can be reconnected automatically by the CTI application.

35-Auto reconnect beep

The user can determine whether a signal will sound when a held call is reconnected by the CTI application.

36-Idle display static

The user can configure the indication of system messages in idle state.

Only available in optiPoint workpoints.

38-Inactivity timeout

The user can set the delay time between the last entry and the return to the idle state.

39-APM / DSM Call View

The user can activate or deactivate the call view on the optiPoint application module.

40-USB keyboard type

The user can modify the language of the USB keyboard connected to an optiPoint phone.

Only available in optiPoint workpoints.

43-Deflect address

The user can enter resp. modify the target number for call deflection.

44-Line settings

The user can modify the settings of a line key.

45-Call view icons

The user can determine whether messages on the optiPoint display module, like, for instance, the list of missed calls, are displayed as text or symbols.

46-Call park

The user can allow call parking.

47-Call pickup

The user can allow pickup of a parked call.

48-Immediate dialing

The user can allow immediate dialing.

49-Callback busy

The user can activate the transmission of a callback request to the system in case the phone is busy.

50-Call back on ring/no reply

The user can activate the transmission of a callback request to the system in case a call is not replied.

Only available in OpenStage workpoints.

51-Idle missed calls

The user can activate missed calls notifications on the display.

Only available on optiPoint workpoints.

52-Busy when dialing

Der Benutzer kann bestimmen, ob ein Abruf abgewiesen wird, der während der Eingabe einer Rufnummer eingeht.

The user can determine whether incoming calls are refused while a call number is entered.

53-Transfer on Ring

The user can determine whether a call is transferred as soon as the third participant’s phone rings, even if the transferring participant has not hung up.

54-Mobility LED flash

The user can determine whether the mobility key LED flashes during data exchange between phone and DLS, like, for instance, while mobility logon and logoff.

Only available in optiPoint workpoints.

55-Call Recording

The user can activate call recording.

Only available in optiPoint workpoints.

56-Secure Call Indication

The user can determine whether an alert tone shall indicate an insecure speech connection.

57-Transfer on Hangup

The user can determine whether, when one call is active and another call is on hold, the user can connect these calls by hanging up.

60-Audio Settings

The user can modify settings like ringtones and room character.

Only available in OpenStage workpoints.

61-Loudspeaker

The user can activate or deactivate handsfree talking.

Only available in OpenStage workpoints.

62-Forwarding Alert

63-Join in Conference

The user can determine whether visual or acoustical warning notifications indicate an incoming call while call forwarding is active.

Only available in OpenStage workpoints.

64-Bluetooth

The user can activate or deactivate bluetooth connectivity.

65-Display Skin

The user can choose the display theme.

Only available in OpenStage 60/80 workpoints.

66-Screensaver

The user can activate the phones's screensaver and set the delay time for starting the screensaver.

Only available in OpenStage 60/80 workpoints.

67-Call context menu

The user can define the displayed menu.

Only available in OpenStage 60/80 workpoints.

68-BLF

The user can define how an incoming call for the phone supervised by the BLF key shall be displayed.

69-Toggle associate

The user can enable or disable the connecting of a first call and a second call by going on-hook. When "Toggle associate" is activated, the following procedure will ensue: The user has accepted a second call, whereby the first call is put to hold. As soon as the user has alternated back to the first call, and then again to the second call, he/she can connect both calling parties by going on-hook.

Available in all OpenStage workpoints.

70- Forwarding party display

For multiple forwarding, the user can determine whether the first forwarding party or the last forwarding party is displayed.

Available in all OpenStage SIP workpoints.

71- Headset

The user can define the type of headset connected to the phone.

Available for OpenStage 40/60/80 SIP/HFA.

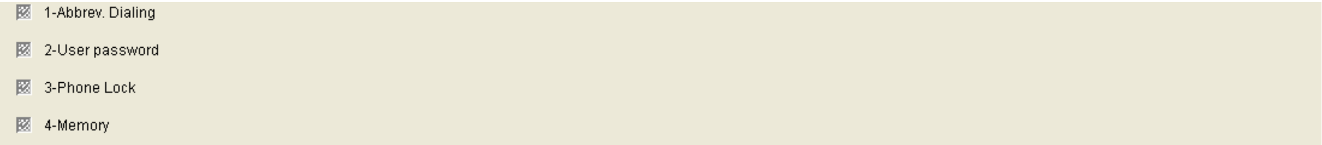
72- Key klick

The user can define the mode of key klick on the phone.

Available for OpenStage 40/60/80 SIP/HFA.

7.1.16.3 "Locked Local Functions" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > User Settings > "Locked Local Functions" Tab



☒ 1-Abbrev. Dialing

☒ 2-User password

☒ 3-Phone Lock

☒ 4-Memory

The following functions can be locked for the Mobile User in the configuration menus by activating the relevant checkbox:

1-Abbreviated dialing

The user can set up abbreviated dialing numbers.

Only available in optiPoint workpoints.

2-User password

The user can change his password.

3-Phone lock

The user can lock the phone. If the phone is locked, no unauthorized person can call from this phone in a regular manner or modify any settings. Only emergency numbers and pre-defined numbers from the dial plan can be dialed.

4-Memory

The user can delete all abbreviated dialing numbers and restore the factory settings.

Only available in optiPoint workpoints.

7.1.17 SIP Mobility

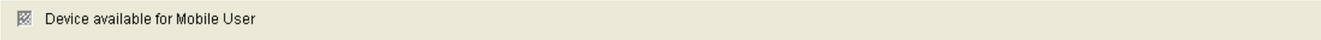
Call: Main Menu > IP Devices > IP Phone Configuration > SIP Mobility

This area features the following components:

- General Data
- Possible Action Buttons
- "SIP Mobility" Tab
- "SIP Mobility Logon/Logoff" Tab
- "SIP Mobility Data" Tab

7.1.17.1 "SIP Mobility" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > SIP Mobility > "SIP Mobility" Tab



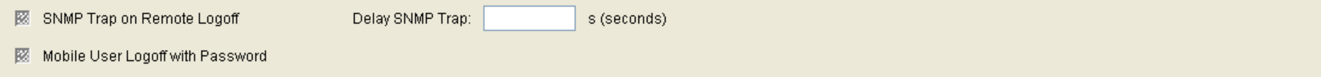
☒ Device available for Mobile User

Device available for Mobile User

If the checkbox is active, the device is available for Mobile User log on.

7.1.17.2 "SIP Mobility Logon/Logoff" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > SIP Mobility > "SIP Mobility Logon/Logoff" Tab



▨ SNMP Trap on Remote Logoff   Delay SNMP Trap: ______ s (seconds)

▨ Mobile User Logoff with Password

SNMP Trap on Remote Logoff

If the checkbox is active, a message is sent to the SNMP server each time an unauthorized remote logoff is attempted. For information on entering SNMP server data, see Section 7.1.13.1, ""SNMP" Tab".

Mobile User Logoff with Password

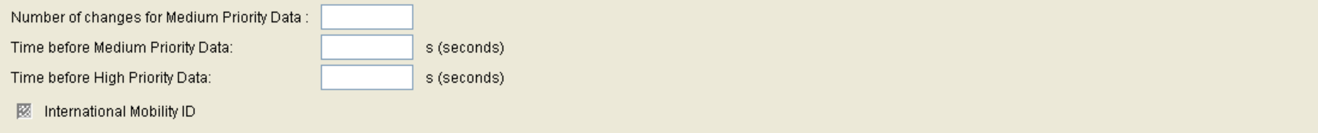
If the checkbox is active, Mobile User logoff is only possible when the password of the currently logged-on Mobile User is entered.

Delay SNMP Trap

Time in seconds until the SNMP trap is sent. For information on entering SNMP server data, see Section 7.1.13.1, ""SNMP" Tab".

7.1.17.3 "SIP Mobility Data" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > SIP Mobility > "SIP Mobility Data" Tab



Number of changes for Medium Priority Data :		
Time before Medium Priority Data:		s (seconds)
Time before High Priority Data:		s (seconds)

☑ International Mobility ID

Number of changes for Medium Priority Data:

Defines how many changes to medium priority data may take place in the workpoint before this data is sent to the DLS.

Time before Medium Priority Data:

Defines the interval after which medium priority data that has been changed in the workpoint is sent to the DLS.

Time before High Priority Data:

Defines the interval after which high priority data that has been changed in the workpoint is sent to the DLS.

International Mobility ID

If this checkbox is activated, the device automatically adds the local country code to the extension, in addition to the trunk number and local area code when a mobile user logs on. The international code is configured under **IP Devices** > **IP Phone Configuration** > **Dialing Properties** > **"Dialing Properties" Tab** -> **International Dial Prefix**.

Example: The user logs on to the device using the extension/mobility ID "31434". If the checkbox is activated, the device sends the number "498972231434". Otherwise, the device sends the number "8972231434".

7.1.18 HFA Mobility

Call: Main Menu > IP Devices > IP Phone Configuration > HFA Mobility

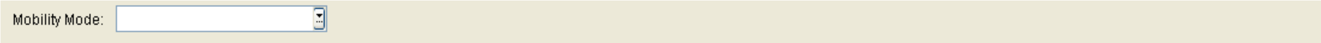
This area features the following components:

- General Data
- Possible Action Buttons
- "HFA Mobility" Tab

7.1.18.1 "HFA Mobility" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > HFA Mobility > "HFA Mobility" Tab

> If the DLS is to store user data like call lists and the phonebook including picture clips, the field **IP Devices** > **IP Phone Configuration** > **HFA Mobility** > **"HFA Mobility" Tab** > **Mobility Mode** must be set to **Data Mobility**. With the values **Data Privacy** and **Basic**, the end device is registered with the DLS, but no further actions are executed in the DLS.


Mobility Mode:

Mobility Mode:

Determines how user data is managed with HFA Mobility.

Possible options:

- **Basic**
- **Data Privacy**
- **Data Mobility**

7.1.19 Keysets/Keylayout

Call: Main Menu > IP Devices > IP Phone Configuration > Keysets/Keylayout

This area features the following components:

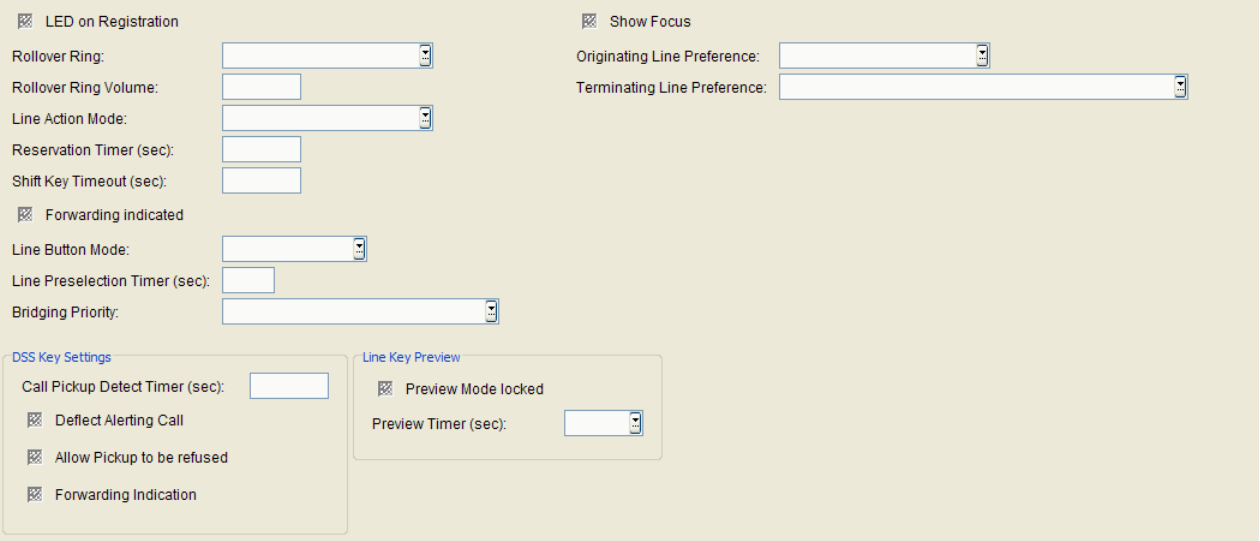
- General Data
- Possible Action Buttons
- "Keysets" Tab
- "Destinations" Tab
- "Send URL Server CA Certificate" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.19.1 "Keysets" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Keysets/Keylayout > "Keysets" Tab



LED on Registration

If the checkbox is activated, the successful workpoint registration after a phone restart will be indicated.

Only available in SIP workpoints.

Rollover Ring:

Type of alerting to be used in the case that, during an active call, an incoming call arrives on a different line.

Possible options:

- **No ring**
- **Alert Ring**
- **Standard**
- **Alerting**

Only available in SIP workpoints.

Rollover Ring Volume:

Volume of alerting when busy.

Only available in SIP workpoints.

Line Action Mode:

Defines what should happen to a line (call) when a connection is established over another line.

Possible options:

- **Call hold**
  The original call is put on hold.
- **Release**
  The connection to the original call is cleared down (the call is ended).

Only available in SIP workpoints.

Reservation Timer (sec):

Time in seconds indicating how long a line reservation can be maintained.

Default: **60** s.

Only available in SIP workpoints.

Shift Key Timeout (sec):

Time in seconds indicating how long the Shift key remains active before the keys recover their original level-1 functions.

Forwarding indicated

Checkbox for activating alerting on a line key when call forwarding is active for its destination.

Only available in SIP workpoints.

Line Button Mode

Possible options:

- **Single button**
  The action associated with the line key is executed as soon as the button is pressed, regardless of whether or not the handset is in the cradle.
- **Preselection**
  Press the line key to preselect a line. This line is used the next time you seize a line (by lifting the handset, for example).

Line Preselection Timer (sec):

Specifies the duration of line key preselection.

Bridging Priority:

Possible options:

- **Bridging overrides preview**
- **Preview overrides bridging**

Show Focus

Checkbox for activating the display showing which line is currently active (line has the focus).

Only available in SIP workpoints.

Originating Line Preference:

Defines the preferred line to be used for outbound calls.

Possible options:

- **Idle line preference**
- **Primary line preference**
- **Last line preference**
- **No preference**

Only available in SIP workpoints.

Terminating Line Preference:

Defines the preferred line to be used for incoming calls.

Possible options:

- **Ringing line preference**
- **Calling line preference with prime line preferred**
- **Ringing line preference**
- **Ringing line preference with prime line preferred**
- **No preference**

Only available in SIP workpoints.

DSS Key Settings

Call Pickup Detect Timer (sec)

Specifies how long group pickup is signaled by the key.

Deflect Alerting Call

If this checkbox is activated, alert tones can be forwarded by pressing a key.

Allow Pickup to be refused

If this checkbox is activated, you can reject group pickup by pressing a key.

Forwarding Indication

If this checkbox is activated and station forwarding is active for this line, the LED of the line key blinks.

Line Key Preview

Preview Mode locked:

Switch to lock preview mode.

Line Key Preview Duration (sec)

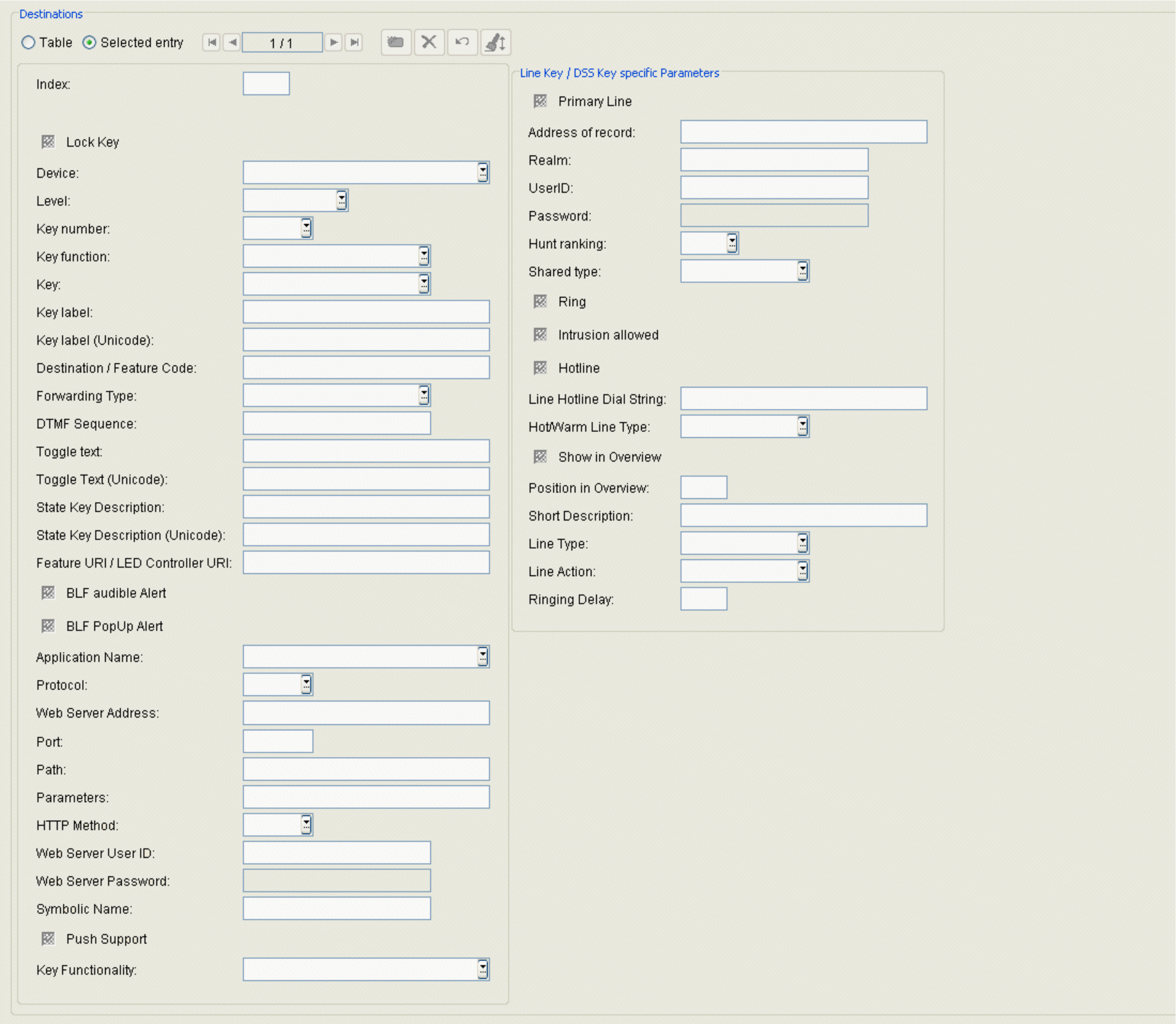
Duration of preview mode in seconds.

Possible options:

- **2**
- **3**
- **4**
- **6**
- **8**
- **10**
- **15**
- **20**
- **30**
- **40**
- **50**
- **60**

7.1.19.2 "Destinations" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Keysets/Keylayout > "Destinations" Tab



Index

Name of the key layout function.

Lock Key

Checkbox for locking the function key.

Device

Specifies the device to which the relevant layout applies.

Possible options:

- **Base device**
- **1st Key module**
- **2nd Key module**
- **1st Self Labeling Key module**
- **2nd Self Labeling Key module**
- **OpenStage 15 Key module**

Only available in SIP workpoints.

Level

Key level for the Shift functionality.

Possible options:

- **1. Level**
- **2. Level**
- **3. Level**
- **4. Level**
- **Fixed Keys**
  Fixed Keys are assigned to a fixed key number. They cannot be deleted or created on the IP Device.

Only available in SIP workpoints.

Key number

Number of the key assigned the relevant function.

Only available in SIP workpoints.

Key function:

The following key functions are supported:

- **Key unused**
- **Selected dialing**
- **Abbreviated dialing**
- **Repeat dialing**
- **Missed calls**
- **Voice messages**
- **Forwarding**
- **Loudspeaker**
- **Mute**
- **Ringer off**
- **Hold**

- **Alternate**
- **Blind Transfer**
- **Join** (optiPoint) **/ Transfer call** (OpenStage)
- **Deflect**
- **Setup menu**
- **Room echoing**
- **Room muffled**
- **Shift**
- **Notebook**
- **Settings**
- **Phone lock**
- **Conference**
- **Local Conference**
- **Headset**
- **Do not disturb**
- **Group pickup**
- **Repertory dial**
- **Line**
- **Feature Toggle**
- **Show Phone Screen**
- **Swap screen**
- **Mobility**
- **Call park**
- **Call pickup**
- **Cancel/Release**
- **Ok Confirm**
- **Callback Request**
- **Cancel Callback**
- **Consultation Transfer**
- **DSS**
- **State Key**
- **Call waiting toggle**
- **Immediate Ring**
- **Preview Key**
- **Call Recording**
- **AICS Zip**
- **Server Feature**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **BLF**

- **Start Application**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **Send URL**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **Built-in Forwarding**
  Only available for ’Fixed Keys’.
- **Built-in Release**
  Only available for ’Fixed Keys’.
- **Built-in Voice Dial**
  Only available for ’Fixed Keys’.
- **Built-in Redial**
  Only available for ’Fixed Keys’.
- **Start Phonebook**

Key:

Indicates whether this key is a ’Fixed Key’or a freely programmable key.

Key label

A key label can be entered here for every key in the case of Self labeling Keys workpoints (for example, optiPoint 420 standard).

Only available in SIP workpoints.

Key label (Unicode)

You can enter the key label in unicode characters for devices in the OpenStage family.

Destination / Feature Code

Destination data to be dialed. This can be a digit string or a URL. Feature codes that need to be sent to external servers (not the SIP server at which the phone is registerd) have the following format:

<feature code>@<IP address>

Example: **123@10.2.54.2**

If the destination has been entered for the "Repertory dial" key function, extra control characters can be entered in a digit string:

- **$Q** = clear (CL)
- **$R** = consult (CS)
- **$S** = OK
- **$T** = Pause (PA)

Only available in SIP workpoints.

Forwarding Type

Possible options:

- **on busy**
- **on no reply**
- **unconditionally**

Only available in SIP workpoints.

DTMF Sequence

DTMF Sequence for this target.

Toggle text

Label for the "Feature Toggle" key function.

Only available in SIP workpoints.

Toggle Text (Unicode)

Label for the "Feature Toggle" key function in unicode.

Only available on devices in the OpenStage family (SIP version).

State Key Description

Description text for the state key.

State Key Description (Unicode)

Description text for the state key in unicode. Only available on devices in the OpenStage family (SIP version).

Feature URI / LED Controller URI

URI used to control this feature on the server.

BLF audible Alert

Audible Alert additional to busy lamp field.

BLF PopUp Alert

Additional to busy lamp field a message pops up in display.

Application Name:

Name of the XML application to be started with the function key.

Protocol

Protocol of Web Server.

Possible options:

- **HTTP**
- **HTTPS**

Web Server Address

Host name, domain name, or IP address of web server.

Port

Port number of web server: If the port is null, the fully qualified URL will not include the port element.

Path

Directory path and name of the program or web page.

Examples: **servlet/IppGenericServlet** or **webpage/checkin.xml**

The path should have a slash at the beginning and no slash at the end. If the slash at the beginning is missing, a slash will be automatically inserted. If there is an additional slash at the end, it will be automatically removed. The slashes in the path should be forward slashes (’/’). If backslashes (’\’) are used instead, the web server may not find the appropriate program or web page.

Parameters

Null, one, or more parameter-value pairs in the format “<parameter>=<value>”, with each pair separated by an ampersand (“&”), e. g. **parameter1=value1&parameter2=value2**. A comma (“,”) is not used as a separator because it could be part of the key or value. If the key or value contains an ampersand, it must be replaced by “&amp;”.

The question mark will be automatically added between the path and the parameters. If there is a question mark at the beginning of the parameters, it will be automatically stripped off.

HTTP Method

HTTP method to be used.

Possible options:

- **Get**
- **Post**

Web Server User ID

User identity known by the server. This information is used for phone authentication by the server.

Web Server Password

Password known by the server. It is used for phone authentication by the server.

Symbolic Name

Symbolic name.

Push Support

Enables or disables push support.

Key Functionality

Possible options:

- **Toggle Call Forwarding**
- **Unspecified Call**
- **Unspecified**

Line Key / DSS Key specific Parameters

Primary Line

Specifies whether the line operates as a primary line.

Only available in SIP workpoints.

Address of record

Line’s phone number and address of record.

Only available in SIP workpoints.

Realm

SIP realm for the line’s address of record.

Only available in SIP workpoints.

UserID

Only available in SIP workpoints.

Password

Only available in SIP workpoints.

Ring

Only available in SIP workpoints.

Hunt ranking

Only available in SIP workpoints.

Shared type

Possible options:

- **Private**
- **Shared**
- **Unknown**

Only available in SIP workpoints.

Intrusion allowed

Checkbox for enabling line intrusion.

Only available in SIP workpoints.

Line Hotline Dest. active

Checkbox for activating a line hotline.

Only available in SIP workpoints.

Line Hotline Dial String:

Subscriber number that is used as a destination for the line hotline.

Only available in SIP workpoints.

Hot/Warm Line Type:

Set device property.

- **Ordinary**
- **Hot Line**
- **Warm Line**

Only available in SIP workpoints.

Show in Overview

Checkbox for activating the line display in the line overview.

Only available in SIP workpoints.

Position in Overview

Position of key in Line Overview.

Only available in SIP workpoints.

Short Description

Description of relevant line.

Only available in SIP workpoints.

Line Type

Possible options:

- **Normal**
- **Direct**

Line Action

Possible options:

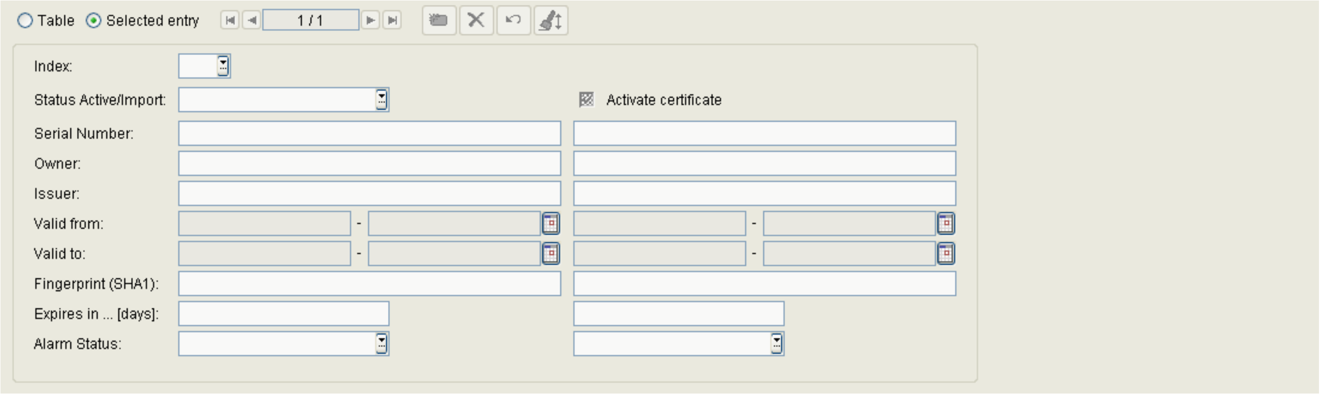
- **Consultation**
- **Transfer**
- **No Action**

Ringing Delay

Time before ringing starts for an alerting call.

7.1.19.3 "Send URL Server CA Certificate" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Keysets/Keylayout > "Send URL Server CA Certificate" Tab



For a parameter description, please refer to **IP Devices** > **IP Phone Configuration** > **LDAP** > **"CA Certificates" Tab**.

7.1.20 WLAN Settings

Call: Main Menu > IP Devices > IP Phone Configuration > WLAN Settings

This area features the following components:

- General Data
- Possible Action Buttons
- "General Data" Tab
- "Security Encryption" Tab
- "Location Server" Tab
- "Advanced Settings" Tab

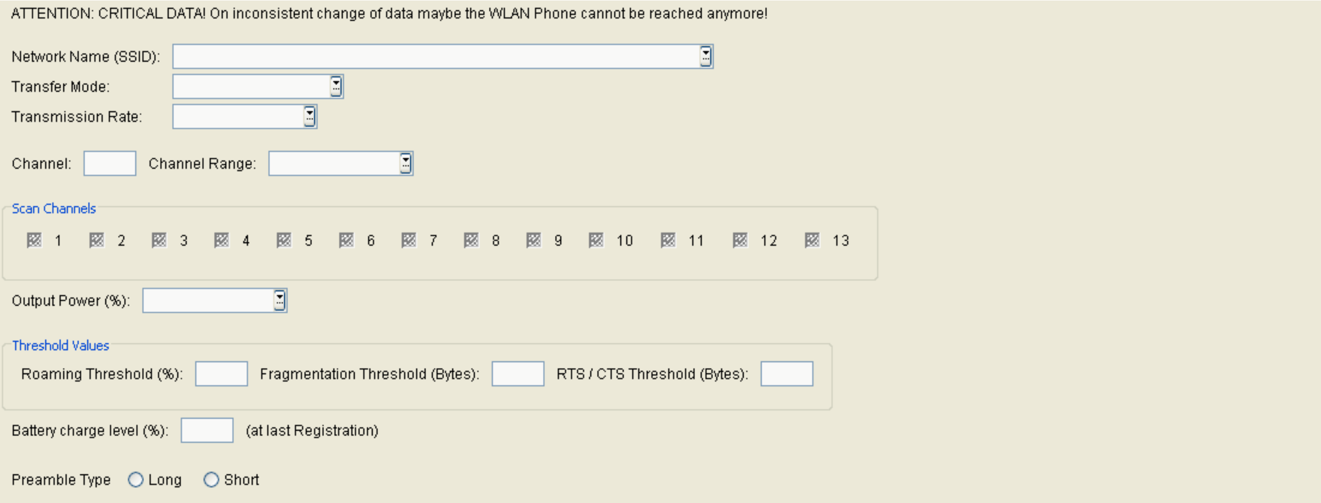
For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

"General Data" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > WLAN Settings > "General Data" Tab

> ⚠ WLAN phone contact may be disrupted if inconsistent data changes are made.



ATTENTION: CRITICAL DATA! On inconsistent change of data maybe the WLAN Phone cannot be reached anymore!

Network Name (SSID)

The SSID is the network name used to identify the WLAN phone. The SSID is defined in the access point (WLAN router).

Transfer Mode:

You can choose the standards IEEE 802.11b (**802.11b only**), or IEEE 802.11b and IEEE 802.11g (**mixed mode**) for data transfer.

The main difference between these standards is the transmission rate. IEEE 802.11g is almost five times faster than the others. If devices in the WLAN use different standards, you must keep the default value (Mixed Mode).

If IEEE 802.11g is entered as a fixed value for transfer mode in the access point or WLAN router, select **Mixed Mode** in this tab.

Possible options:

- **only 802.11b**
- **Mixed Mode**

Transmission Rate:

The transmission rate is the speed in Mbps at which data is transmitted in the WLAN. The transmission rate depends on the transfer mode selected.

Possible options:

- **1.0 Mbps**
- **2.0 Mbps**
- **5.6 Mbps**
- **6.0 Mbps**
- **9.0 Mbps**
- **11.0 Mbps**
- **12.0 Mbps**
- **18.0 Mbps**
- **24.0 Mbps**
- **36.0 Mbps**
- **48.0 Mbps**
- **54.0 Mbps**

Channel:

WLAN radio channel. The channel is configured in the access point or the WLAN router.

Channel Range:

The available channel range in each case can be selected. The restriction is required in some countries due to the fact that the use of channel 12 and 13 is not permitted. Possible values: channel 1-11: for example USA, channel 1-13: for example Germany, channel 1-14: for example Japan.

Scan Channels:

Scan channel selection.

Output Power (%)

Output power that the handset uses to transmit to the access point. Up to 100 mW or 20 dBm (100%) output power is permitted.

Possible options:

- **5 %**
- **10 %**
- **20 %**
- **40 %**
- **100 %**

Threshold Values

Roaming Threshold (%):

Minimum reception strength expressed as a percentage. If the reception strength of the access point currently connected falls below this value, the handset searches for and connects to another access point with better connectivity.

Fragmentation Threshold

Size at which voice packets are fragmented. Fragmenting data packets into smaller packets improves data throughput in a WLAN when the network is running at high capacity.

Value range: **256** ... **2346** bytes.

Default value: **2346** bytes (no fragmenting).

RTS/CTS Threshold:

Minimum packet size in bytes required for transmitting an RTS (Request To Send). Smaller packets are transmitted directly to the access point without an RTS.

Value range: **1** ... **2347** bytes.

Default value: **2347** bytes (RTS/CTS mechanism deactivated).

> ℹ Activating this mechanism may reduce data throughput.

Battery charge level (%): (at last Registration)

Battery charge level in percent of the WLAN phone at the last logon.

Preamble Type

A preamble is set before each data packet is transmitted in a WLAN. It enables the receiver to synchronize with the transmission timing.

A long preamble ensures more stable synchronization. A short preamble enables higher data throughput.

Not all WLAN devices support both preamble types.

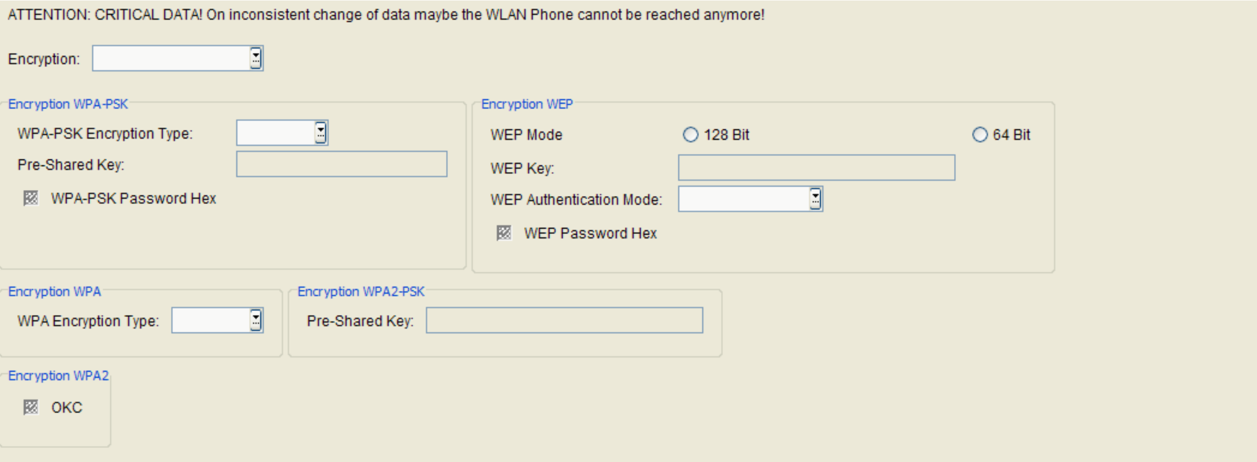
Possible options:

- **Long**
- **Short**

7.1.20.1 "Security Encryption" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > WLAN Settings > "Security Encryption" Tab

> ⚠ WLAN phone contact may be disrupted if inconsistent data changes are made.



ATTENTION: CRITICAL DATA! On inconsistent change of data maybe the WLAN Phone cannot be reached anymore!

> ⓘ Encryption protects data exchange in the WLAN. It does not protect data exchange with Ethernet networks or the Internet.

Encryption:

This field enables you to select the encryption procedure.

Possible options:

- **None**
  Data is not encrypted for transmission in the WLAN.
- **WPA**
  WPA encryption.
- **WPA-PSK**
  WPA-PSK encryption.
- **WEP**
  WEP encryption.
- **WPA2**
  WPA2 encryption
- **WPA2-PSK (AES)**
  WPA2-PSK encryption

Encryption WPA-PSK

WPA-PSK Encryption Type:

Possible options:

- **TKIP**
  Encryption using the TKIP protocol. Designed for use with WPA-PSK.

Pre-Shared Key:

Entry field for PSK encryption key.

WPA-PSK Password Hex

Checkbox for activating the WPA-PSK password hex.

Encryption WPA2-PSK

Pre-Shared Key:

Entry field for WPA2-PSK encryption key.

Encryption WPA2

OKC:

Checkbox for activating the Opportunistic Key Caching (OKC).

Encryption WEP

WEP Mode

Information on the WEP key length. For 128 bits, the key must consist of 13 ASCII characters or 26 hexadecimal characters. For 64 bits, it must consist of five ASCII characters or 10 hexadecimal characters.

WEP Key:

Entry field for WEP encryption key.

WEP Authentication Mode:

Possible options:

- **Open System**
  The WEP key is only used for data encryption, not for authentication.
- **Shared Key**
  The WEP key is also used for authentication in the WLAN. In other words, the handset can only log on to the WLAN if it transmits the correct key.

WEP Password Hex

Checkbox for activating the WEP password hex.

Encryption WPA

WPA Encryption Type:

Possible options:

- **TKIP**

Encryption using the TKIP protocol. Designed for use with WPA.

Encryption WPA2-PSK

Pre-Shared Key

Entry field for PSK encryption key.

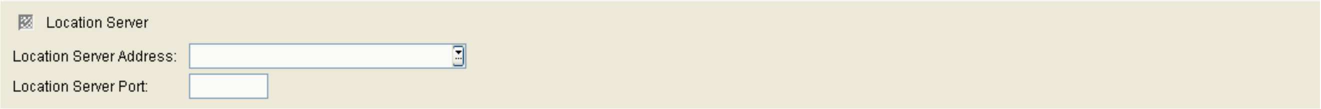
Encryption WPA2

OKC

Switch to activate Opportunistic Key Caching (OKC).

7.1.20.2 "Location Server" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > WLAN Settings > "Location Server" Tab



▨ Location Server

Location Server Address:

Location Server Port:

Location Server

If this checkbox has been enabled, the data for an existing location server is used.

Location Server Address:

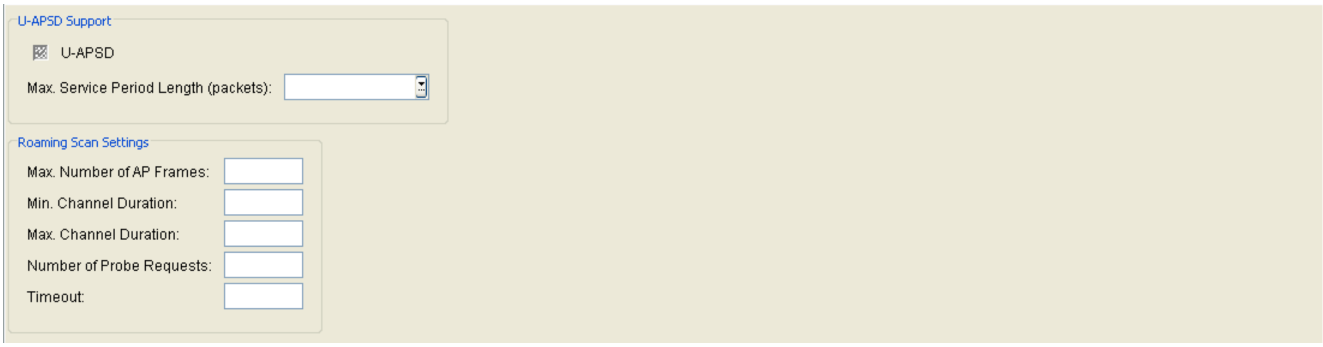
IP address or host name of the location server.

Location Server Port:

Port number of the location server.

7.1.20.3 "Advanced Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > WLAN Settings > "Advanced Settings" Tab



U-APSD Support

U-APSD

Activate U-APSD.

Max. Service Period Length (packets)

Maximum length of the service period, expressed as a number of packets.

Possible Options:

- **unlimited max. 15**
- **2**
- **4**
- **6**

Roaming Scan Settings

Max. Number of AP Frames

Maximum number of AP frames.

Min. Channel Duration

Minimum channel duration.

Max. Channel Duration

Maximum channel duration.

Number of Probe Requests

Number of probe requests.

Timeout

Timeout after seconds.

7.1.21 Signaling and Payload Encryption (SPE)

Call: Main Menu > IP Devices > IP Phone Configuration > Signaling and Payload Encryption (SPE)

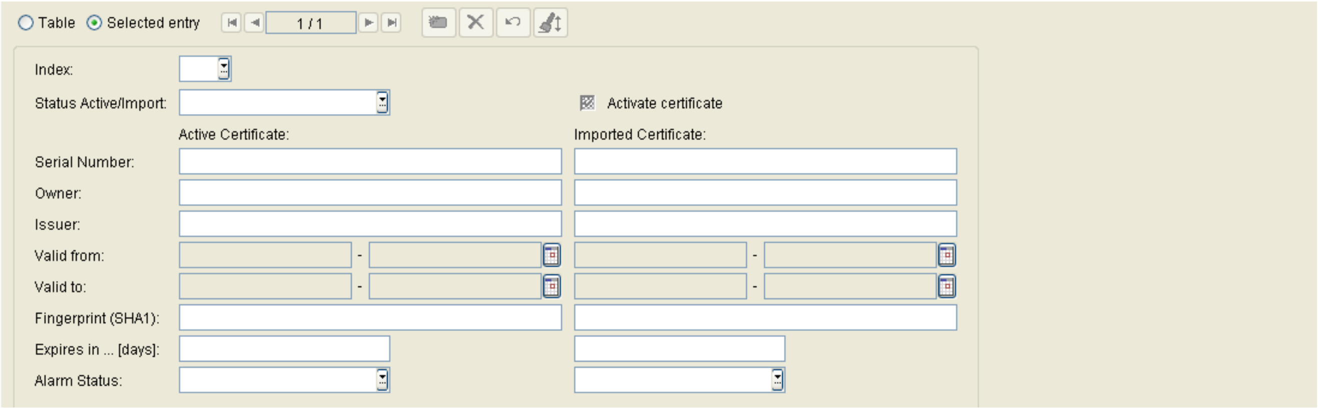
This area features the following components:

- General Data
- Possible Action Buttons
- "SPE CA Certificates" Tab
- "SIP Settings" Tab
- "HFA Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

7.1.21.1 "SPE CA Certificates" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Signaling and Payload Encryption (SPE) > "SPE CA Certificates" Tab



The parameters described below are available once for the currently active certificate and once for the imported certificate.

Index:

Serial number of the CA certificate.

Status Active/Import:

Specifies whether a certificate is registered as imported and/or active on the phone. The five statuses listed below are possible.

Possible values:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA 1):

This is the fingerprint extracted from the certificate.

Expires in ... [days]:

Number of days before the certificate expires.

> ⓘ The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Displays the duration of validity for certificates when searching for certificates due to expire.

Possible values:

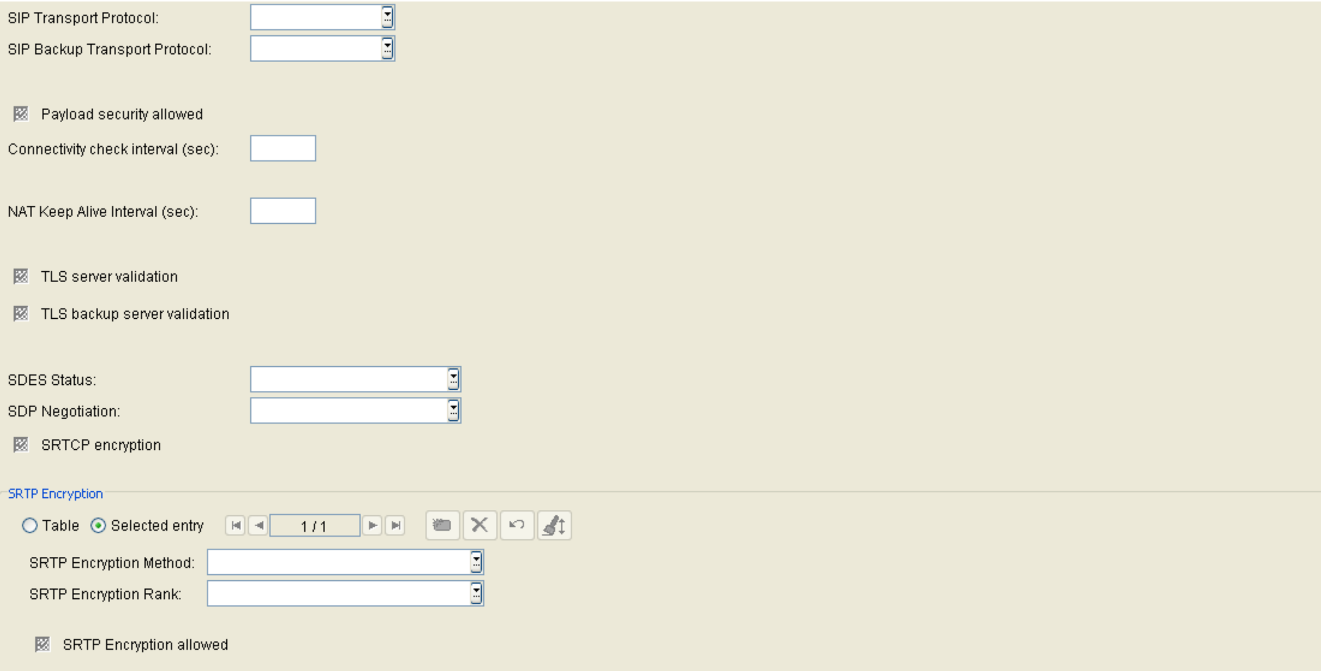
- **valid**
- **soon running out**
- **expired**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted. The active certificate is used to encrypt calls.

7.1.21.2 "SIP Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Signaling and Payload Encryption (SPE) > "SIP Settings" Tab


SIP Transport Protocol:
SIP Backup Transport Protocol:
☒ Payload security allowed
Connectivity check interval (sec):
NAT Keep Alive Interval (sec):
☒ TLS server validation
☒ TLS backup server validation
SDES Status:
SDP Negotiation:
☒ SRTCP encryption

SRTP Encryption Method:
SRTP Encryption Rank:
☒ SRTP Encryption allowed

SIP Transport Protocol:

Protocol for SIP signaling.

Possible options:

- **UDP**
- **TCP**
- **TLS**

SIP Backup Transport Protocol:

Possible options:

- **UDP**
- **TCP**

Payload security allowed

When activated, payload security is allowed.

Connectivity check interval

Connectivity check interval in seconds.

NAT Keep Alive Interval (sec):

Timer interval that controls the transfer rate of keep-alive packets. If the value equals **0**, the NAT keep-alive mechanism is switched off.

SIP server validation

When activated, the TLS connection to the SIP server is validated.

SIP backup server validation

If this checkbox is activated, the TLS connection to the backup SIP server is validated.

SDES Status

Select the SDES status.

Possible options:

- **disabled**
- **enabled**

SDP Negotiation

Select the SDP negotiation.

Possible options:

- **SRTP and RTP**
- **SRTP only**
- **Fallback to RTP**

SRCTP Encryption

When activated, SRCTP encryption will be applied.

SRTP Encryption

SRTP Encryption Method

Selects the SRTP encryption method to be used.

Possible options:

- **SHA1-32**
- **SHA1-80**

SRTP Encryption Rank

Selects the SRTP Encrpytion Rank.

Possible options:

- **Choice 1**

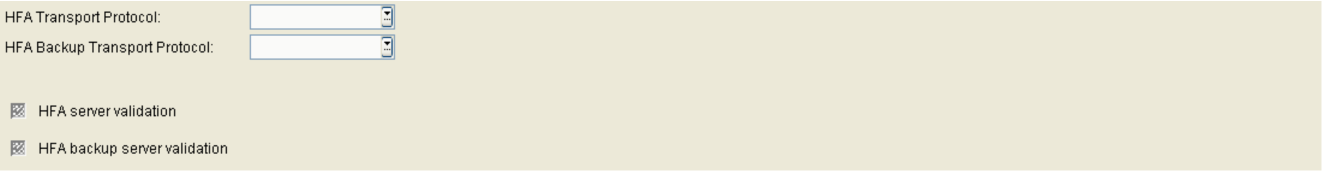
- **Choice 2**

SRTP Encryption allowed

When activated, SRTP will be encrypted.

7.1.21.3 "HFA Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Signaling and Payload Encryption (SPE) > "HFA Settings" Tab



HFA Transport Protocol:

HFA Backup Transport Protocol:

☒ HFA server validation

☒ HFA backup server validation

HFA Transport Protocol:

Protocol for HFA alerting.

Possible options:

- **UDP**
- **TCP**
- **TLS**

HFA Backup Transport Protocol:

Protocol for HFA alerting.

Possible options:

- **UDP**
- **TCP**
- **TLS**

HFA server validation

If this checkbox is activated, the connection to the HFA server is verified.

HFA backup server validation

If this checkbox is activated, the connection to the HFA backup server is verified.

7.1.22 VoIP Security V1

Call: Main Menu > IP Devices > IP Phone Configuration > VoIP Security V1

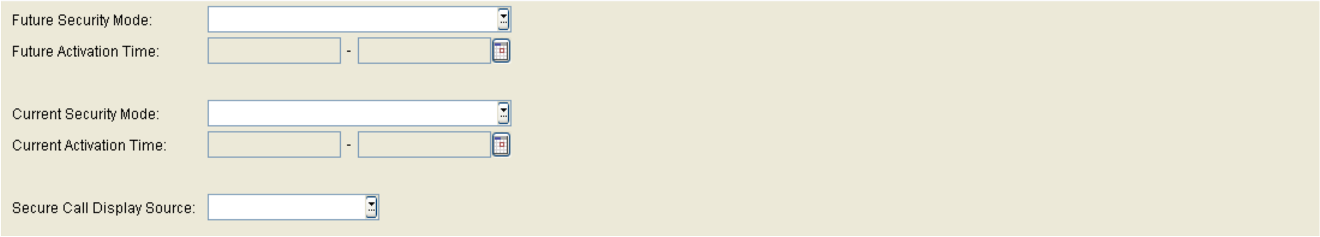
This area features the following components:

- General Data
- Possible Action Buttons
- "HFA Key Distribution" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

7.1.22.1 "HFA Key Distribution" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > VoIP Security V1 > "HFA Key Distribution" Tab



Future Security Mode:	
Future Activation Time:	-
Current Security Mode:	
Current Activation Time:	-
Secure Call Display Source:	

Future Security Mode

Indicates whether encryption will be enabled in the future (read-only).

Possible values:

- **Encryption on**
- **Encryption off**

Future Activation Time:

Time of future activation (read-only).

For selecting a time span, see Section 5.4.2.4, "Time field with calendar button".

Current Security Mode

Indicates whether encryption is enabled (read-only).

Possible values:

- **Encryption on**
- **Encryption off**

Current Activation Time:

Time of the current activation (read-only).

For selecting a time span, see Section 5.4.2.4, "Time field with calendar button".

Secure Call Display Source:

For HFA workpoints, it is possible to indicate on the display whether the call is encrypted. This option determines the source for this information; either from the system or from the phone itself.

Possible options:

- **System**
- **Phone**

7.1.23 IEEE 802.1x

Call: Main Menu > IP Devices > IP Phone Configuration > IEEE 802.1x

> For detailed information on configuring IEE 802.1x, see the "IEE 802.1x Configuration Management" Administration Manual available online at
> http://wiki.siemens-enterprise.com/index.php/VoIP_Security#IEEE_802.1X
> and
> http://wiki.siemens-enterprise.com/images/a/ae/DLS_-_Certificate_Management_for_802_1x.pdf

This area features the following components:

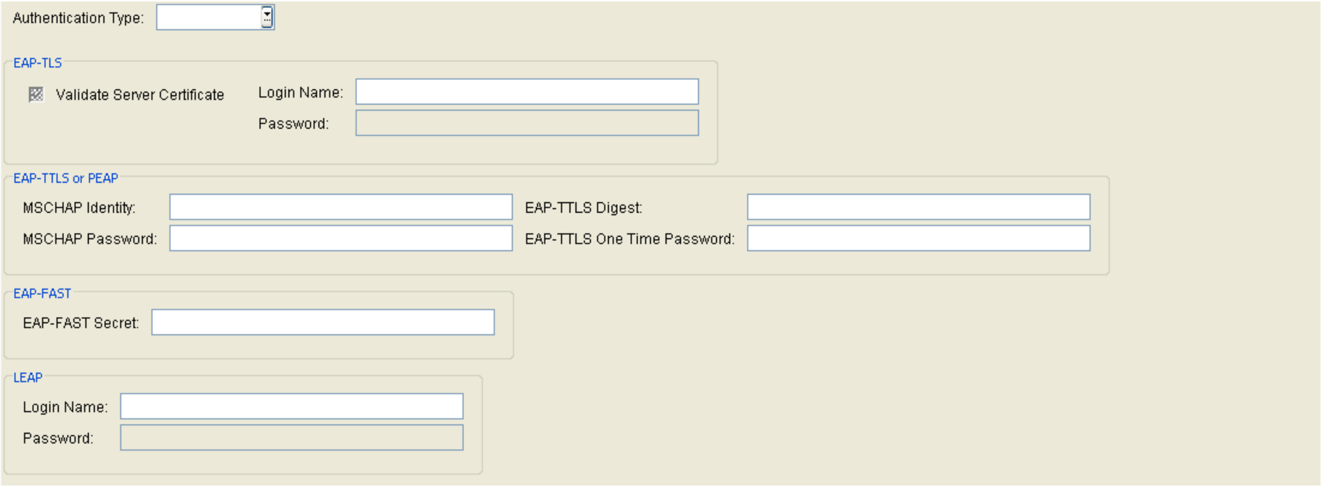
- General Data
- Possible Action Buttons
- "802.1x Settings" Tab
- "Phone Certificate" Tab
- "RADIUS Server CA Certificate 1" Tab
- "RADIUS Server CA Certificate 2" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.23.1 "802.1x Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > IEEE 802.1x > "802.1x Settings" Tab



Authentication Type

Possible values:

- **none**
- **EAP-TLS**
- **EAP-TTLS with digest/OTP**
- **EAP-TTLS with MSCHAP**
- **EAP-FAST**
- **LEAP**
- **PEAP**

EAP-TLS

Validate Server Certificate

If this checkbox is activated, the telephone checks the validity of the server certificate sent by the access point.

Login Name:

Login name for identification.

Password:

Password for identification.

EAP-TTLS or PEAP

MSCHAP Identity:

MSCHAP Password:

EAP-TTLS Digest

EAP-TTLS One Time Password

EAP-FAST

EAP-FAST Secret:

LEAP

Login Name:

Login name for identification on the access point/WLAN router.

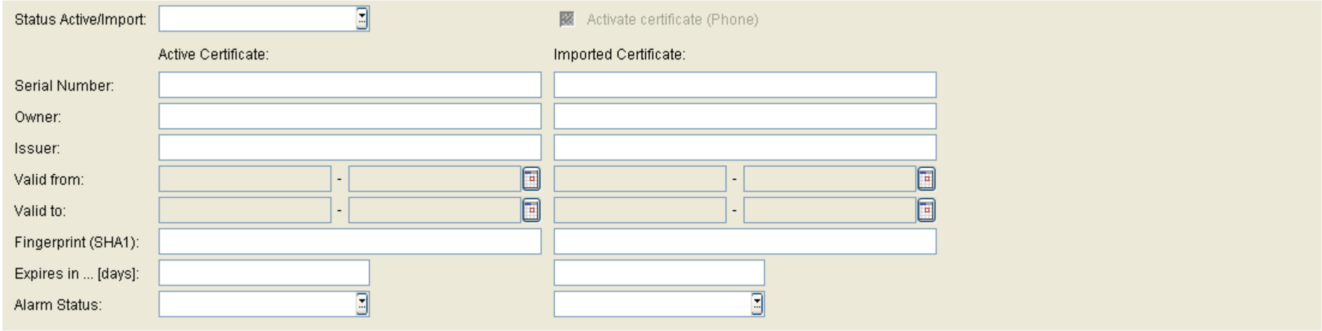
Password:

Password for identification on the access point/WLAN router.

7.1.23.2 "Phone Certificate" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > IEEE 802.1x > "Phone Certificate" Tab

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".



Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate (Phone)

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm **SHA1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Certificate will expire in ... days.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status.

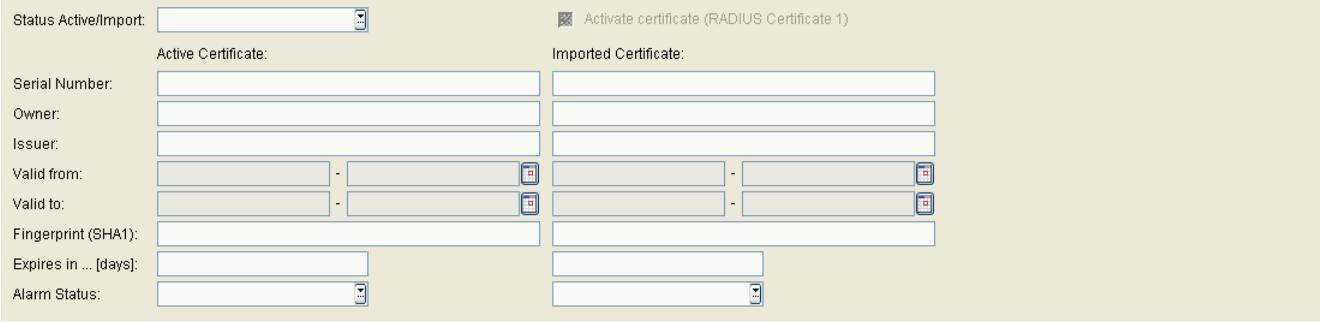
Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.23.3 "RADIUS Server CA Certificate 1" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > IEEE 802.1x > "RADIUS Server CA Certificate 1" Tab

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".



Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate (RADIUS 1)

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm **SHA1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Certificate will expire in ... days.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status.

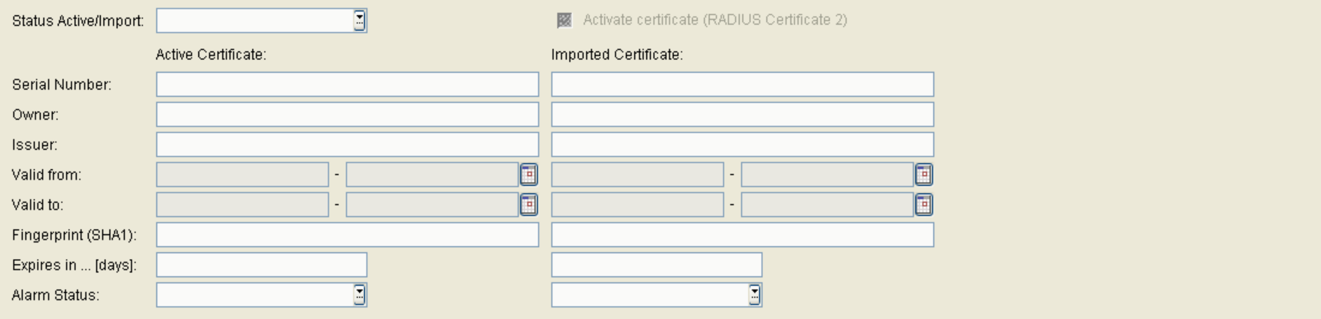
Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.23.4 "RADIUS Server CA Certificate 2" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > IEEE 802.1x > "RADIUS Server CA Certificate 2" Tab

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".



Status Active/Import:

▨ Activate certificate (RADIUS Certificate 2)

	Active Certificate:	Imported Certificate:
Serial Number:		
Owner:		
Issuer:		
Valid from:	-	-
Valid to:	-	-
Fingerprint (SHA1):		
Expires in ... [days]:		
Alarm Status:		

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate (RADIUS 2)

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm **SHA1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Certificate will expire in ... days.

> ℹ The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.24 Diagnosis

Call: Main Menu > IP Devices > IP Phone Configuration > Diagnosis

This area features the following components:

- General Data
- Possible Action Buttons
- "Diagnostic Settings" Tab
- "File Settings" Tab
- "Secure Shell (SSH) access" Tab
- "Remote Trace Settings" Tab
- "Upload Diagnosis- and Security Files" Tab
- "Periodical Upload Diagnosis- and Security Files" Tab

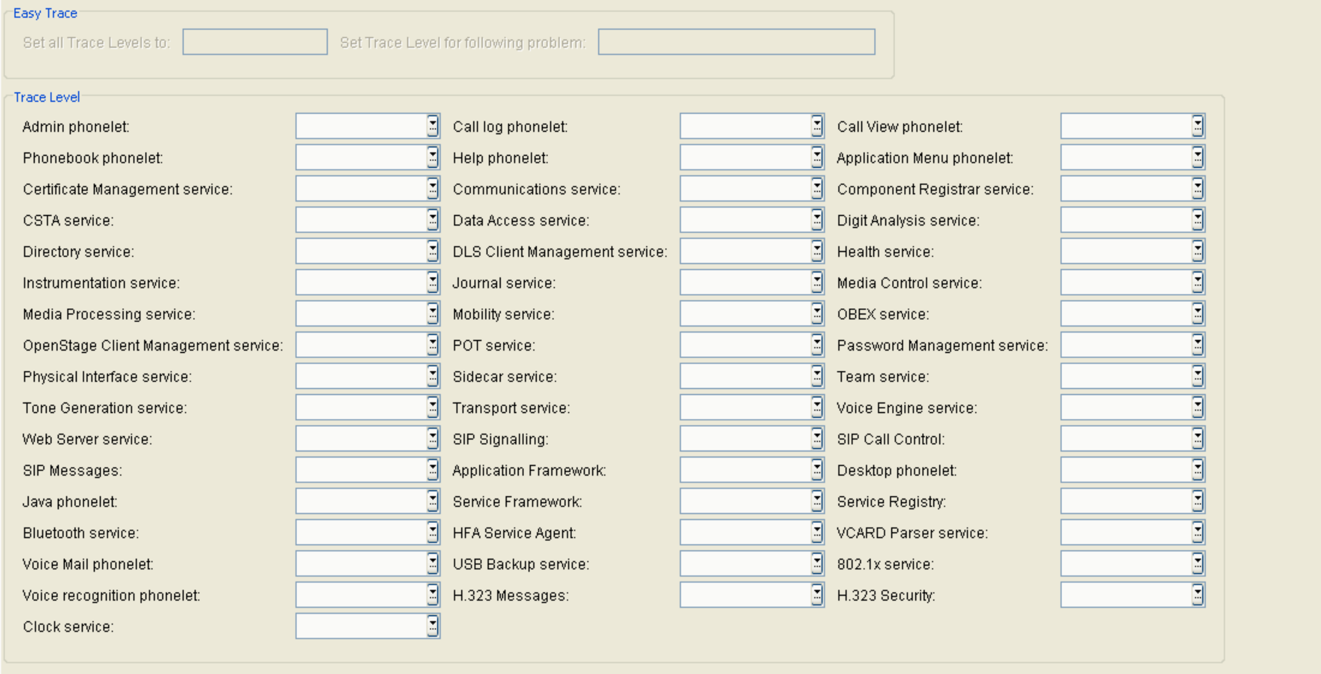
For information on general interface operation, see Section 5.4.2, "Work Area".

7.1.24.1 "Diagnostic Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Diagnosis > "Diagnostic Settings" Tab

Error tracing is defined here for the individual telephone components. The trace files are uploaded from the telephone to a server via FTP or HTTPS.

> These settings are only available on OpenStage phones.



Easy Trace

Set all Trace Levels to:

Set Trace Level for following problem:

Trace Level

Admin phonelet:	Call log phonelet:	Call View phonelet:
Phonebook phonelet:	Help phonelet:	Application Menu phonelet:
Certificate Management service:	Communications service:	Component Registrar service:
CSTA service:	Data Access service:	Digit Analysis service:
Directory service:	DLS Client Management service:	Health service:
Instrumentation service:	Journal service:	Media Control service:
Media Processing service:	Mobility service:	OBEX service:
OpenStage Client Management service:	POT service:	Password Management service:
Physical Interface service:	Sidecar service:	Team service:
Tone Generation service:	Transport service:	Voice Engine service:
Web Server service:	SIP Signalling:	SIP Call Control:
SIP Messages:	Application Framework:	Desktop phonelet:
Java phonelet:	Service Framework:	Service Registry:
Bluetooth service:	HFA Service Agent:	VCARD Parser service:
Voice Mail phonelet:	USB Backup service:	802.1x service:
Voice recognition phonelet:	H.323 Messages:	H.323 Security:
Clock service:		

Easy Trace

Pre-defined profiles facilitate the controlling of trace parameters. Common trace levels for all components can be configured, as well as groups of parameters which belong to a specific funcional area of the phone.

Set all Trace Levels to:

Activates all trace points in code from OpenStage phones. A different value may be set for each trace level.

Possible Options:

- **Off**
- **Fatal**
- **Error**

- **Warning**
- **Trace**
- **Debug**

Set Trace Level for following problem:

Select a functional area in the phone for which the Easy Trace profile is to be set.

Possible Options:

- **Bluetooth headset profile**
- **Bluetooth handsfree profile**
- **Call connection**
- **Call log problems**
- **DAS connection**
- **DLS data errors**
- **Help application problems**
- **Key input problems**
- **LAN connectivity problems**
- **Messaging application problems**
- **Mobility problems**
- **OpenStage manager problems**
- **Phone administration problems**
- **Phonebook (LDAP) problems**
- **Phonebook (local) problems**
- **Server based application problems**
- **Sidecar problems**
- **Speech problems**
- **Tone problems**
- **USB audio features**
- **USB backup/restore**
- **Voice recognition problems**
- **Web based management**
- **802.1x problems**

Trace Level

Activates particular trace points in code from the OpenStage phones and locates errors. A different value may be set for each trace level.

Admin phonelet:

Possible options:

- **Off**

- **Fatal**
- **Error**
- **Warning**
- **Trace**
- **Debug**

Call log phonelet:

Same options as for Admin phonelet:

Call View phonelet:

Same options as for Admin phonelet:

Phonebook phonelet:

Same options as for Admin phonelet:

Help phonelet:

Same options as for Admin phonelet:

Application Menu phonelet:

Same options as for Admin phonelet:

Certificate Management service:

Same options as for Admin phonelet:

Communications service:

Same options as for Admin phonelet:

Component Registrar service:

Same options as for Admin phonelet:

CSTA service:

Same options as for Admin phonelet:

Data Access service:

Same options as for Admin phonelet:

Digit Analysis service:

Same options as for Admin phonelet:

Directory service:

Same options as for Admin phonelet:

DLS Client Management service:

Same options as for Admin phonelet:

Health service:

Same options as for Admin phonelet:

Instrumentation service:

Same options as for Admin phonelet:

Journal service:

Same options as for Admin phonelet:

Media Control service:

Same options as for Admin phonelet:

Media Processing service:

Same options as for Admin phonelet:

Mobility service:

Same options as for Admin phonelet:

OBEX service:

Same options as for Admin phonelet:

OpenStage Client Management service:

Same options as for Admin phonelet:

POT service:

Same options as for Admin phonelet:

Password Management service:

Same options as for Admin phonelet:

Physical Interface service:

Same options as for Admin phonelet:

Sidecar service:

Same options as for Admin phonelet:

Team service:

Same options as for Admin phonelet:

Tone Generation service:

Same options as for Admin phonelet:

Transport service:

Same options as for Admin phonelet:

Voice Engine service:

Same options as for Admin phonelet:

Web Server service:

Same options as for Admin phonelet:

SIP Signaling:

Same options as for Admin phonelet:

SIP Call Control:

Same options as for Admin phonelet:

SIP Messages:

Same options as for Admin phonelet:

Application Framework:

Same options as for Admin phonelet:

Desktop phonelet:

Same options as for Admin phonelet:

Java phonelet

Same options as for Admin phonelet:

Service Framework

Same options as for Admin phonelet:

Service Registry

Same options as for Admin phonelet:

Bluetooth service

Same options as for Admin phonelet:

HFA Service Agent

Same options as for Admin phonelet:

VCARD Parser service

Same options as for Admin phonelet:

Voice Mail phonelet

Same options as for Admin phonelet:

USB Backup service

Same options as for Admin phonelet:

802.1x service

Same options as for Admin phonelet:

Voice recognition phonelet

Same options as for Admin phonelet:

H.323 Messages

Same options as for Admin phonelet:

H.323 Security

Same options as for Admin phonelet:

Clock service

Same options as for Admin phonelet:

Security Log service

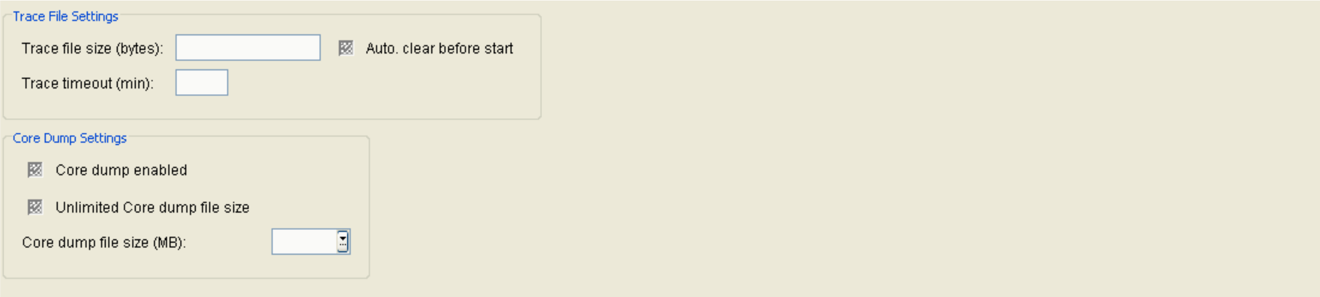
Same options as for Admin phonelet:

Media Recording service

Same options as for Admin phonelet:

7.1.24.2 "File Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Diagnosis > "File Settings" Tab



Trace File Settings

Trace file size (bytes)

Specifies the maximum size of the trace file.

Value range: **65536** ... **4194304** (64KB ... 4MB).

Trace Timeout (min):

Defines the number of minutes after which a timeout for tracing should be activated.

Auto. clear before start

Defines whether the trace memory should be emptied before a new trace is executed.

Core Dump Settings

Core dump enabled

Checkbox for activating the core dump.

Unlimited Core dump file size

If this checkbox is activated, the size of a core dump file is not limited.

Core dump file size (MB)

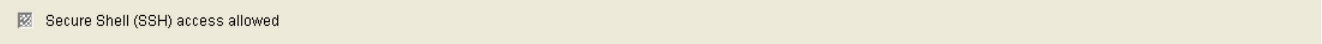
Specifies the maximum size of the trace file.

Value range: **0** ... **1023**

Default value: **1000**

7.1.24.3 "Secure Shell (SSH) access" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Diagnosis > "Secure Shell (SSH) access" Tab



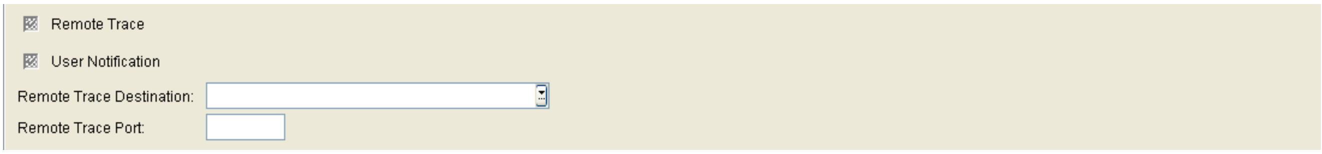
☒ Secure Shell (SSH) access allowed

Secure Shell (SSH) access allowed

If this checkbox is active, the phone can be accessed via SSH.

7.1.24.4 "Remote Trace Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Diagnosis > "Remote Trace Settings" Tab



☒ Remote Trace

☒ User Notification

Remote Trace Destination:

Remote Trace Port:

Remote Trace

If this checkbox is active, the phones sends its trace data directly to the destination entered in **Remote Trace Destination**.

User Notification

If activated, the phone user will be notified when a trace is performed on the phone.

Remote Trace Destination

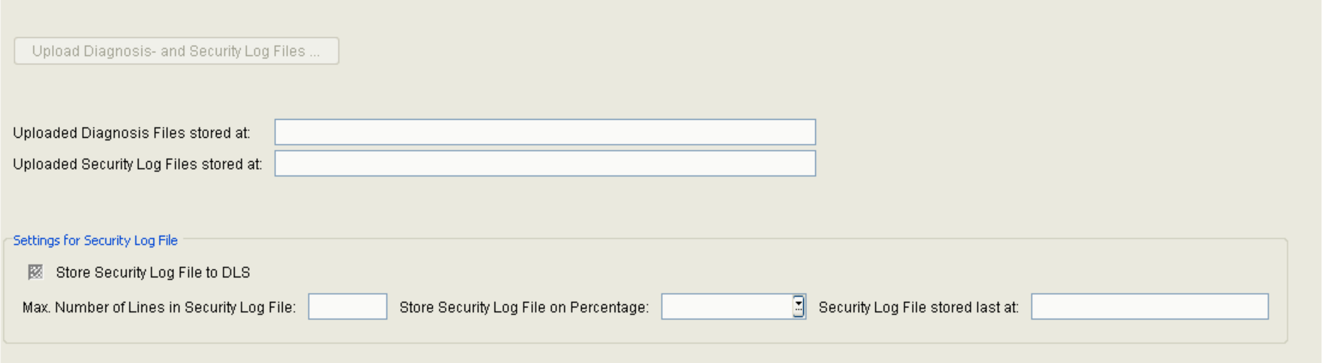
IP address or hostname of the server to which the trace data are sent.

Remote Trace Port

Number of the port at which the server receives the trace data.

7.1.24.5 "Upload Diagnosis- and Security Files" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Diagnosis > "Upload Diagnosis- and Security Files" Tab


Upload Diagnosis- and Security Log Files ...
Uploaded Diagnosis Files stored at:
Uploaded Security Log Files stored at:
Settings for Security Log File
☒ Store Security Log File to DLS
Max. Number of Lines in Security Log File:
Store Security Log File on Percentage:
Security Log File stored last at:

Upload Diagnosis- and Security Log Files ...

Starts a single upload of diagnosis- and security log files, independent of the settings for periodical uploads. The files to be uploaded can be selected in a popup window.

Uploaded Diagnosis Files stored at:

Storage path for the diagnosis files that have been uploaded for this device. The path can be set via **Main Menu** > **Administration** > **File Server** > **OpenStage Diagnosis Files**.

Uploaded Security Log Files stored at:

Storage path for the security log files that have been uploaded for this device. The path can be set via **Main Menu** > **Administration** > **File Server** > **OpenStage Security Log Files**.

Settings for Security Log File

Store Security Log File to DLS

When active, the security log file of this IP Device is stored by the DLS.

Max. Number of Lines in Security Log File:

Sets the maximum number of entries that may be contained in the security log file.

Value range: **100** … **1000**

Store Security Log File on Percentage

Determines the percentage of unstored entries. The percentage depends on the value of **Max. Number of Lines in Security Log File**. When the percentage is exceeded, the security log file is sent to the DLS for storing.

Possible Options:

- **save immediately**

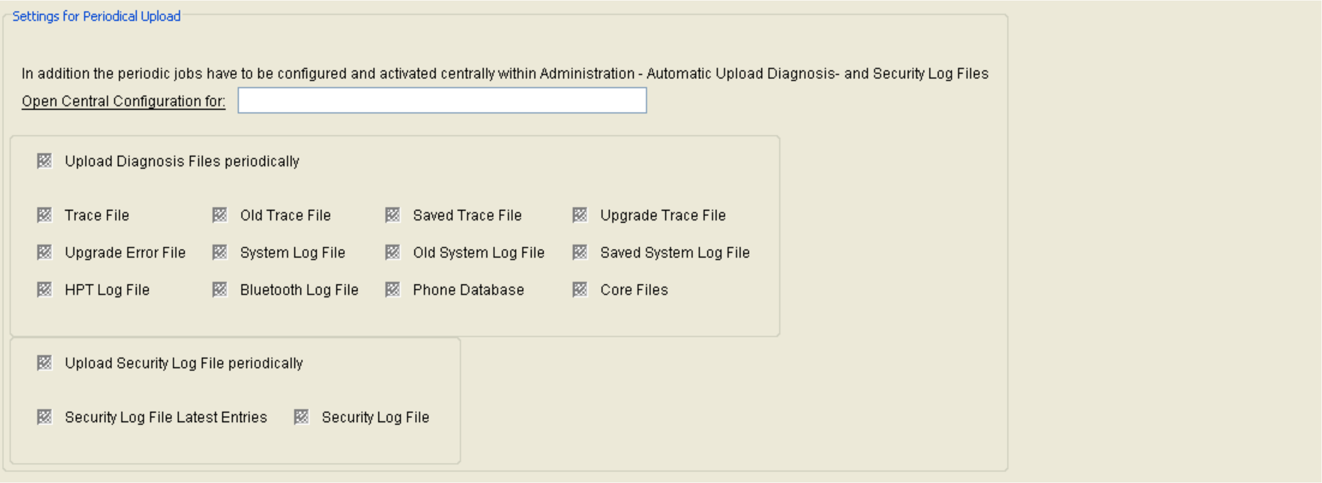
- **10%**
- **20%**
- **30%**
- **35%**
- **40%**
- **45%**
- **50%**
- **55%**
- **60%**
- **65%**
- **70%**
- **80%**
- **90%**

Security Log File stored last at

Date at which the security log file has been stored lastly.

7.1.24.6 "Periodical Upload Diagnosis- and Security Files" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Diagnosis > "Periodical Upload Diagnosis- and Security Files" Tab



Settings for Periodical Upload

In addition the periodic jobs have to be configured and activated centrally within Administration - Automatic Upload Diagnosis- and Security Log Files

Open Central Configuration for:

☑ Upload Diagnosis Files periodically

☑ Trace File ☑ Old Trace File ☑ Saved Trace File ☑ Upgrade Trace File

☑ Upgrade Error File ☑ System Log File ☑ Old System Log File ☑ Saved System Log File

☑ HPT Log File ☑ Bluetooth Log File ☑ Phone Database ☑ Core Files

☑ Upload Security Log File periodically

☑ Security Log File Latest Entries ☑ Security Log File

Settings for Periodical Upload

Open Central Configuration for:

By clicking on the string, the central configuration in **Administration** > **Automatic Upload Diagnosis- and Security Log Files** is opened. The name of the destination mask is displayed in the text field.

Upload Diagnosis Files periodically

When active, diagnosis files of the IP Device are uploaded periodically.

Trace File

When active, the trace file of the IP Device is uploaded periodically.

Old Trace File

If checkbox is active, the old trace file of the IP Device is uploaded periodically.

Saved Trace File

When active, the saved trace file is uploaded periodically.

Upgrade Trace File

When active, the upgrade trace file of the IP Device is uploaded periodically.

Upgrade Error File

When active, the upgrade error file of the IP Device is uploaded periodically.

System Log File

Whens active, the system log file of the IP Device is uploaded periodically.

Old System Log File

When active, the old system log file is uploaded periodically.

Saved System Log File

When active, the saved system log file is uploaded periodically.

HPT Log File

When active, the HPT log file of the IP Device is uploaded periodically.

Bluetooth Log File

When active, the Bluetooth log file of the IP Device is uploaded periodically.

Phone Database

When active, the phone database file is uploaded periodically.

Core Files

When active, the core files of the are IP Device uploaded periodically.

Upload Security Log File periodically

When active, the security log files of the IP Device are uploaded periodically.

Security Log File Last Entries

When active, entries in the security log file of the IP Device that have been added since the last storage are uploaded periodically.

Security Log File

When active, the complete security log file of the IP Device is uploaded periodically.

7.1.25 Miscellaneous

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous

This area features the following components:

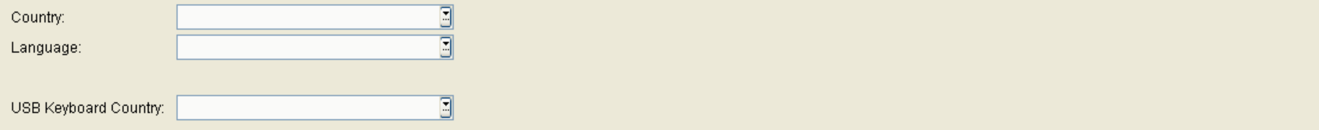
- General Data
- Possible Action Buttons
- "Country & Language" Tab
- "Messaging Services" Tab
- "SIP Error Notification" Tab
- "Display / Phone Settings" Tab
- "Help Internet URL" Tab
- "FTP Server" Tab
- "Call Log" Tab
- "Phone Lock" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.25.1 "Country & Language" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous > "Country & Language" Tab



Country:

Language:

USB Keyboard Country:

Country:

Country where the workpoint is operated. This parameter corresponds to the country setting on the device.

Possible options:

- **AE - United Arab Emirates**
- **AF - Afghanistan**
- **AL - Albania**
- **AM - Armenia**
- **AR - Argentina**
- **AT - Austria**
- **AU - Australia**
- **AZ - Azerbaijan**
- **BA - Bosnia and Herzegovina**
- **BD - Bangladesh**
- **BE - Belgium**
- **BG - Bulgaria**
- **BO - Bolivia**
- **BR - Brazil**
- **BY - Belarus**
- **CH- Switzerland**
- **CI - Ivory Coast**
- **CL - Chile**
- **CM - Cameroon**
- **CN - China**
- **CO - Columbia**
- **CR - Costa Rica**
- **CR - Serbia**
- **CY - Cyprus**
- **CZ - Czech Republic**
- **DE - Germany**
- **DZ - Algeria**

- **DK - Denmark**
- **EC - Ecuador**
- **EE - Estonia**
- **EG - Egypt**
- **ES - Spain**
- **FI - Finland**
- **FR - France**
- **GB - Great Britain**
- **GE - Georgia**
- **GR - Greece**
- **GT - Guatemala**
- **HN - Honduras**
- **HK - Hong Kong**
- **HR - Croatia**
- **HU - Hungary**
- **ID - Indonesia**
- **IE - Ireland**
- **IL - Israel**
- **IN - India**
- **IR - Iran**
- **IT - Italy**
- **JO - Jordan**
- **JP - Japan**
- **KE - Kenya**
- **KG - Kyrgyzstan**
- **KR - Korea**
- **KW - Kuwait**
- **KZ - Kazakhstan**
- **LB - Lebanon**
- **LK - Sri Lanka**
- **LT - Lithuania**
- **LU - Luxembourg**
- **LV - Latvia**
- **MA - Morocco**
- **MD - Moldova**
- **MK - Macedonia**
- **MV - Maldives**
- **MX - Mexico**
- **MY - Malaysia**

- **NA - Namibia**
- **NG - Nigeria**
- **NI - Nicaragua**
- **NL - Netherlands**
- **NO - Norway**
- **NP - Nepal**
- **NZ - New Zealand**
- **OM - Oman**
- **PA - Panama**
- **PE - Peru**
- **PH - Philippines**
- **PK - Pakistan**
- **PL - Poland**
- **PT - Portugal**
- **PY - Paraguay**
- **RO - Romania**
- **RU - Russia**
- **SA - Saudi Arabia**
- **SE - Sweden**
- **SG - Singapore**
- **SI - Slovenia**
- **SK - Slovakia**
- **SV - El Salvador**
- **TH - Thailand**
- **TJ - Tajikistan**
- **TN - Tunisia**
- **TR- Turkey**
- **TM - Turkmenistan**
- **TZ - Tanzania**
- **UA - Ukraine**
- **US - United States of America**
- **UY - Uruguay**
- **UZ - Uzbekistan**
- **VE - Venezuela**
- **VN - Vietnam**
- **ZA - South Africa**
- **ZW - Zimbabwe**

Language:

Language to be used for local applications.

Possible options:

- **bg - bulgarian**
- **ca - catalan**
- **cs - czech**
- **da - danish**
- **de - german**
- **el - greek**
- **en - english (GB)**
- **en - english (US)**
- **en - english**
- **es - spanish**
- **et - estonian**
- **fi - finnish**
- **fr - french**
- **hr - croatian**
- **hu - hungarian**
- **id - indonesian**
- **it - italian**
- **ja - japanese**
- **lv - latvian**
- **mk - macedonian**
- **ms - malayan**
- **nl - dutch**
- **no - norwegian**
- **pl - polish**
- **pt - portuguese**
- **pt-Br - brazilian**
- **ro - romanian**
- **ru - russian**
- **sk - slovak**
- **sl - slovenian**
- **sr - serbian (cyrillic)**
- **sr_Latn - serbian (Latin)**
- **sv - swedish**
- **tr - turkish**
- **zh - chinese**

USB Keyboard Country:

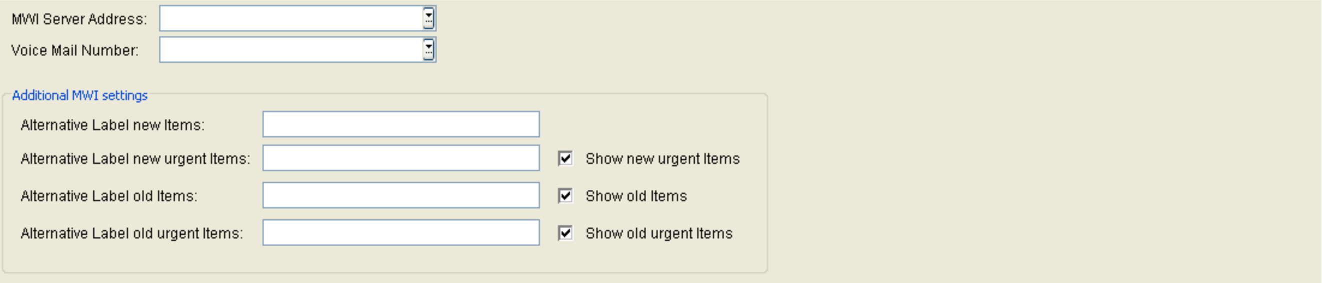
Language-specific keyboard layout when using an external USB keyboard.

Possible options:

- **English**
- **German**
- **French**
- **Spanish**
- **American**
- **Italian**

7.1.25.2 "Messaging Services" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous > "Messaging Services" Tab



MWI Server Address:

Voice Mail Number:

Additional MWI settings

Alternative Label new Items:

Alternative Label new urgent Items: ☑ Show new urgent Items

Alternative Label old Items: ☑ Show old Items

Alternative Label old urgent Items: ☑ Show old urgent Items

MWI Server Address:

IP address or host name of the MWI server.

Voice Mail Number:

Phone number of the voicemail system (message server).

Additional MWI settings

Show new urgent Items

Shows the count of new urgent messages.

Show old urgent Items

Shows the count of old messages.

Show old urgent Items

Shows the count of old urgent messages.

Alternative Label new Items

Label for the count of new messages.

Alternative Label new urgent Items

Label for the count of new urgent messages.

Alternative Label old Items

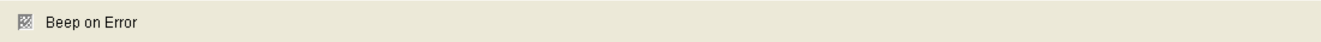
Label for the count of old messages.

Alternative Label old urgent Items

Label for the count of old urgent messages.

7.1.25.3 "SIP Error Notification" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous > "SIP Error Notification" Tab



☒ Beep on Error

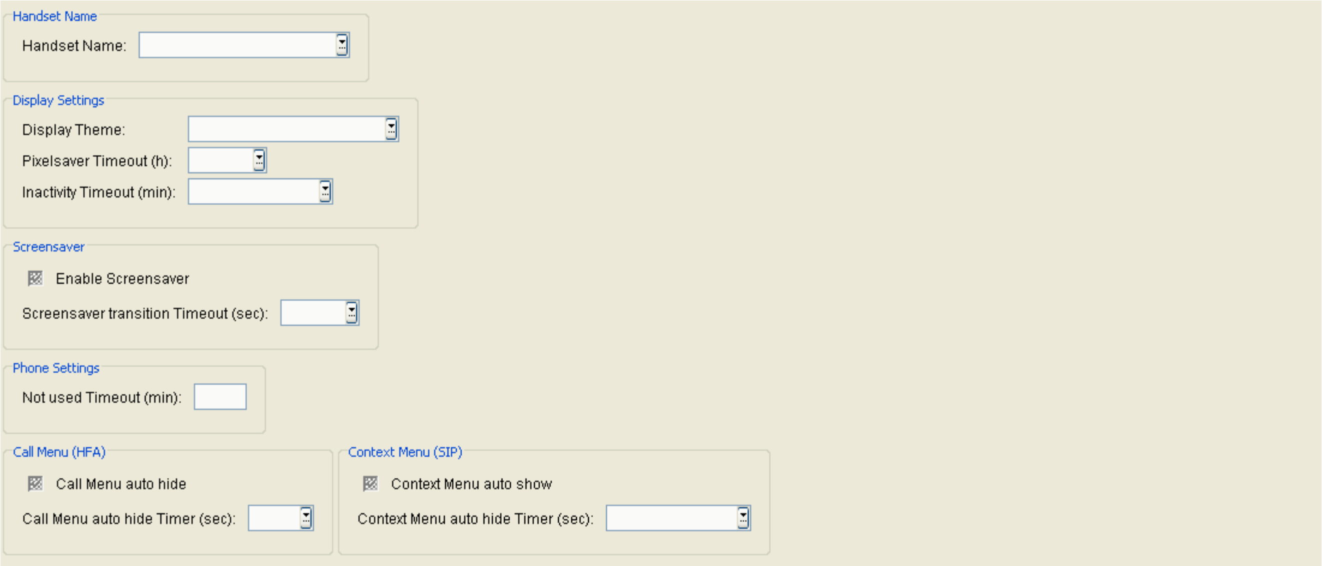
Beep on Error

Checkbox for activating acoustic error signaling during communication with Microsoft RTC.

Only available in SIP workpoints.

7.1.25.4 "Display / Phone Settings" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous > "Display / Phone Settings" Tab



Handset Name

Handset Name:

Name of the WLAN handset shown on the handset's display.

Value range: max. 16 alphanumeric characters.

Display Settings

Display Theme

Defines the layout of the graphical user interface on OpenStage phones.

Possible options:

- **Silver Blue**
- **Anthracite Orange**

Pixelsaver Timeout (h):

After the phone has been in idle state for a timespan exceeding this value, the backlight is shut down.

Possible options:

- **2**
- **3**
- **4**

- **5**
- **6**
- **7**
- **8**

Not used Timeout (min):

Time in minutes before the screen is dimmed, if no activities have taken place on the screen until now.

Possible Options:

- **0 (no timeout)**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Screensaver

Enable Screensaver

This checkbox enables the screensaver.

Screensaver transition Timeout (sec)

Time interval in seconds for changing the images.

Possible Options:

- **5**
- **10**
- **20**
- **30**
- **60**

Phone Settings:

Not used Timeout (min):

Defines how long (in minutes) the telephone will remain inactive before its ends a particular status.

Example: Exit the configuration menu after a specified time.

Call Menu (HFA)

Call Menu auto hide

If the checkbox is checked, the call menu will be hidden after an adjustable timeout.

Call Menu auto hide Timer (sec)

Defines the timeout in seconds, after which the hiding of the call menu starts.

Possible Values:

- **0**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Context Menu (SIP)

Context Menu auto show

When active, the context menu will be shown automatically.

Context Menu auto hide Timer (sec)

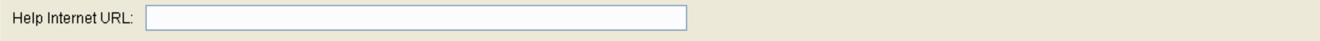
The context menu will be hidden after the timeout specified here, in seconds.

Possible Values:

- **No auto hide**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

7.1.25.5 "Help Internet URL" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous > "Help Internet URL" Tab



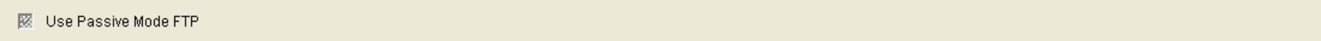
Help Internet URL:

Help Internet URL:

URL of the Web help page on the Internet containing information on the telephone.

7.1.25.6 "FTP Server" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous > "FTP Server" Tab



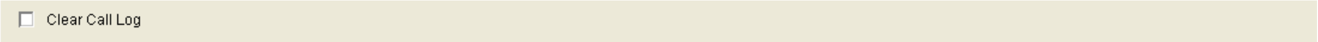
☑ Use Passive Mode FTP

Use Passive Mode FTP

This checkbox activates the passive mode for connections between the telephone and FTP server. Passive mode is used when the FTP server is unable to set up a connection to the client, for example, because of a firewall.

7.1.25.7 "Call Log" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous > "Call Log" Tab



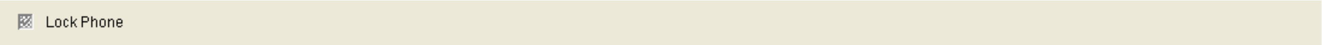
☐ Clear Call Log

Clear Call Log

Deletes the content of the call log.

7.1.25.8 "Phone Lock" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > Miscellaneous > "Phone Lock" Tab



Lock Phone

Locks the phone.

7.1.26 File Deployment

Call: Main Menu > IP Devices > IP Phone Configuration > File Deployment

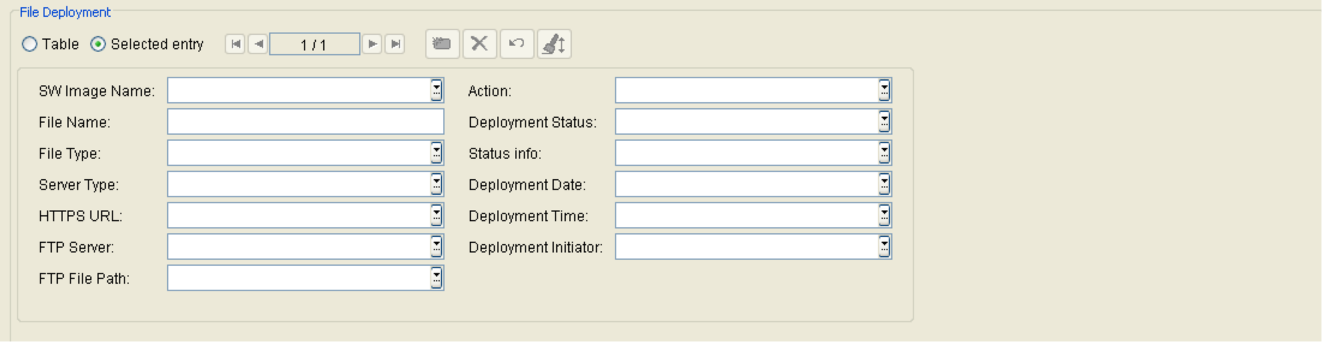
Files which have been read in the DLS database via scan (see Section 6.2.4, "FTP Server Configuration") can be transferred to an IP device. It is possible to transfer multiple files at once. For an overview of all software types supported by the DLS, see Section 3.5, "Overview of Software and File Types".

This area features the following components:

- General Data
- Possible Action Buttons
- "Files" Tab

7.1.26.1 "Files" Tab

Call: Main Menu > IP Devices > IP Phone Configuration > File Deployment > "Files" Tab



File Deployment

SW Image Name:

Name of the Software Image.

File Name:

Name of the file.

File Type:

Usage of the file.

> For many file types on the FTP server can be used for multiple purposes. In such cases, there is a table entry for each usage. For instance, a WAV file can be used as a ringtone and as music on hold. Ringtone and music on hold files must not exceed 1MB in size, while screensaver and logo files should not be larger than 300kB.

Example: **LOGO** (OpenStage 40/60/80) , **SCREENSAVER** (OpenStage 40/60/80).

Server Type:

Protocol used by the server which provides the file.

Possible values:

- **FTP**
- **HTTPS**

HTTPS URL:

URL of the software image, if a HTTPS server is used.

FTP Server:

ID of the FTP server that provides the file. This is necessary if a FTP server is used.

FTP File Path:

Path of the file, if a FTP server is used.

Action:

Indicates what is to be done with the file.

Possible values:

- **delete**
- **deploy**

Deployment Status:

Status of the deployment action.

Status info:

Information about the status.

Deployment Date:

Date of the latest file deployment.

Deployment Time:

Time of the latest file deployment.

Deployment Initiator:

Interface over which the deployment has been initiated.

Possible values:

- **DLS**
- **WBM**
- **Local**

7.2 IP Client Configuration

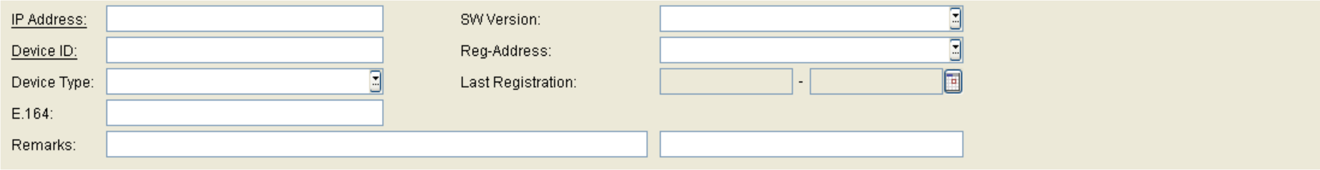
Call: Main Menu > IP Devices > IP Client Configuration

This menu consists of the following submenus:

- CTI Configuration
- Gateway/Server
- Ports
- Quality of Service
- Telephony
- Small Remote Site Redundancy
- Dialing Properties
- Audio/Video Settings
- Directories/Address Books
- Miscellaneous
- Keysets/Keylayout
- Signaling and Payload Encryption (SPE)
- VoIP Security V1
- Dialup Site
- OpenScape
- CTI Configuration

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP clients. The base data associated with the IP clients found is displayed in **Object** view (no changes possible except under **Remarks**).



You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.

All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only **those** IP clients that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of the IP client.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device.

Device Type:

Device type of the IP client.

All IP client types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **optiClient 130**

E.164:

Complete E.164 phone number of the IP client.

Example: **498972212345** (or no input).

For more information, see Chapter 17, "E.164".

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last IP client registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP clients that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Deploy

Starts a job for distributing the configuration changes. For more information, see Section 15.1, "First Steps: Changing IP Device Parameters".

Get

Loads a template that has already been saved. For more information, see Section 15.4, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.4, "Editing Templates".

Rename

Changes the name of a saved template. For more information, see Section 15.4, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.4, "Editing Templates".

7.2.1 CTI Configuration

Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration

This menu consists of the following submenus:

- General Data
- Possible Action Buttons
- CTI HFA Provider
- CSTA Service Provider

7.2.1.1 CTI HFA Provider

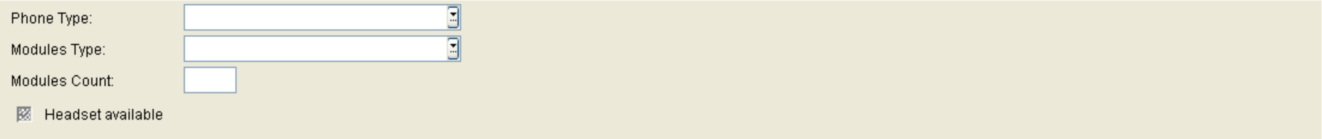
Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CTI HFA Provider

This menu consists of the following submenus:

- General Data
- Possible Action Buttons
- "Device" Tab
- "Connection" Tab
- "Dialup" Tab
- "License" Tab

"Device" Tab

Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CTI HFA Provider > "Device" Tab



Phone Type:

Modules Type:

Modules Count:

▨ Headset available

Phone Type:

Type of the phone which is to be controlled by the CTI provider.

Possible Options:

- **optiSet E advance China**
- **optiPoint 410 standard (DA Mode)**
- **optiPoint 410 standard**
- **optiPoint 410 advance**
- **optiPoint 420 standard**
- **optiPoint 420 advance**
- **optiSet E comfort**
- **optiSet E advance**

Modules Type:

Type of the connected module, if present.

Possible Options:

- **optiPoint Key Module**
- **optiPoint Self Labeling Keys Module**
- **optiSet E Key Module**

Modules Count:

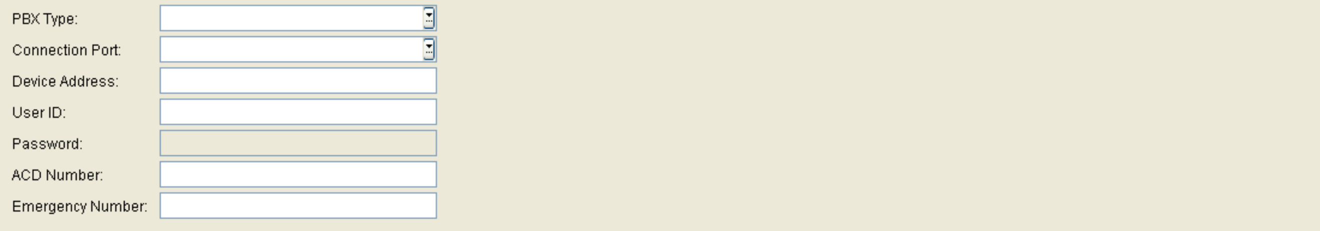
Number of existing modules.

Headset available

Checkbox to determinate whether a headset is connected.

"Connection" Tab

Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CTI HFA Provider > "Connection" Tab



PBX Type:

Connection Port:

Device Address:

User ID:

Password:

ACD Number:

Emergency Number:

PBX Type:

Possible Options:

- **HiPath 3000**
  Includes HiPath, OpenScape MX/LX, and OpenOffice EE, too.
- **HiPath 4000**

Connection Port:

Hardware port used for CTI communication with the device. If USB is used, a special driver is necessary, which emulates a COM port. For futher information, see the administrator dcoumentation for optiClient.

Possible Options:

- **LAN**
- **COM1**
- **COM2**
- **COM3**
- **COM4**
- **COM5**
- **COM6**
- **COM7**
- **COM8**
- **COM9**

Device Address:

IP address of the PBX.

User ID:

User address (extension) for the phone.

Password:

Passwort corresponding to the user ID.

ACD Number:

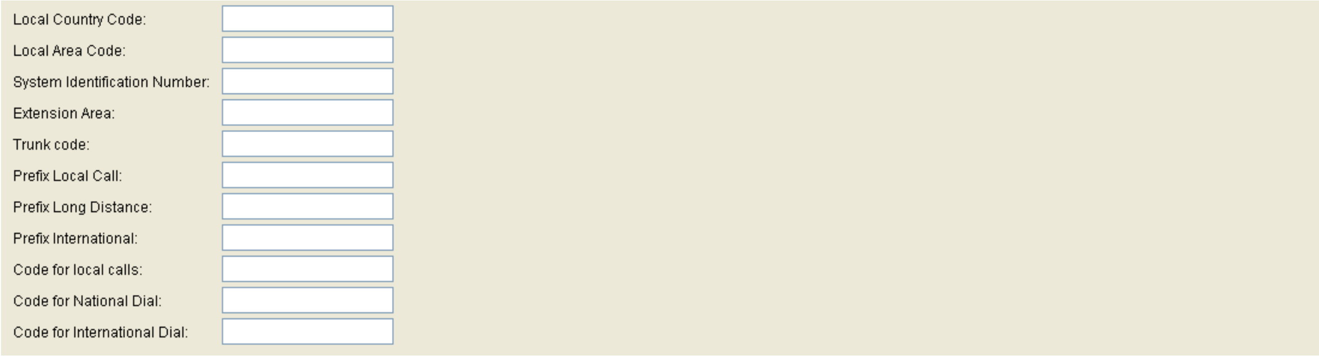
Needed if the user is working as ACD (Automatic Call Distribution) agent.

Emergency Number:

Emergency number configured in the device.

"Dialup" Tab

Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CTI HFA Provider > "Dialup" Tab



Local Country Code:

Local Area Code:

System Identification Number:

Extension Area:

Trunk code:

Prefix Local Call:

Prefix Long Distance:

Prefix International:

Code for local calls:

Code for National Dial:

Code for International Dial:

Local Country Code:

E.164 Country code, without leading zero. Maximum length: 4 digits.

Examples: **49** for Germany, **44** for United Kingdom.

Local Area Code:

Local area code / city code, without leading zero. Maximum length: 21 digits.

Examples: **89** for Munich, **20** for London.

System Identification Number:

Number of the company PBX to which the phone is connected. Maximum length: 21 digits.

Example: **722** for Siemens Munich, Hofmannstraße.

Extension area:

This parameter defines a pattern which enables to discern internal extensions. From a workpoint's point of view, extensions are internal if they are assigned to the same PBX. The extension area can be given as a regular expression.

Example: Let 1xxx, 2xxx, 3xxx, 4xxx , 5xxx be (internal) extensions, and let 6xxx, 7xxx, 8xxx, 9xxx be external call numbers. The regular expression ^[12345] defines that call numbers beginning with a digit from 1 to 5 are internal extensions. If, for instance, the system identification number is 667, the call numbers from 6671xxx to 6675xxx are treated as internal extensions.

Trunk Code:

Access code used for dialing out from a PBX to a PSTN. If multiple trunk codes are configured at the communication system connected, enter them in this field using "|" as a separator (0 and 88 in the example). The first value entered is always used to supplement the call number when dialing. Maximum length: 5 digits.

Examples: **0**, **74**, **9** (USA).

Prefix Local Call:

Prefix for a local call. This data is determined by the network operator, and thus independent of the configuration for the PBX. Maximum length: 21 digits.

Example: **01081**

Prefix Long Distance:

Prefix for a long distance call. This data is determined by the network operator, and thus independent of the configuration for the PBX. Maximum length: 21 digits.

Example: **01081**

Prefix International:

Prefix for an international call. This data is determined by the network operator, and thus independent of the configuration for the PBX. Maximum length: 21 digits.

Example: **01081**

Code for local calls:

This number is designated as call-by-call prefix for local calls. The data is not dependant on the configuration of the provider connected. Maximum length: 21 digits.

Example: **01019**

Code for National Dial:

This number is designated as call-by-call prefix for national calls. The data is not dependant on the configuration of the provider connected. Maximum length: 5 digits.

Example: **01015**

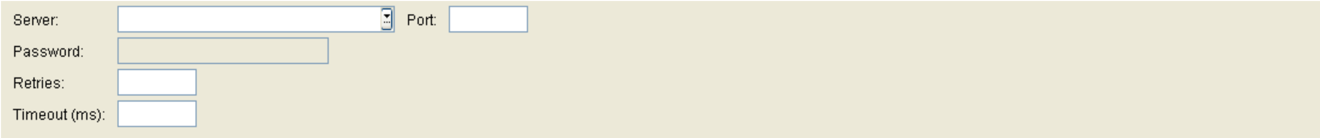
Code for International Dial:

This number is designated as call-by-call prefix for international calls. The data is not dependant on the configuration of the provider connected. Maximum length: 5 digits.

Example: **01015**

"License" Tab

Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CTI HFA Provider > "License" Tab



Server:		Port:	
Password:			
Retries:			
Timeout (ms):			

Server:

IP address of the server that provides the licenses.

Password:

Password for access to the license.

Retries:

Number of retries to establish a connection to the license server.

Timeout (ms):

Timeout for tries to establish a connection to the license server.

Port:

Number of the port used by the license server for delivering licenses.

7.2.1.2 CSTA Service Provider

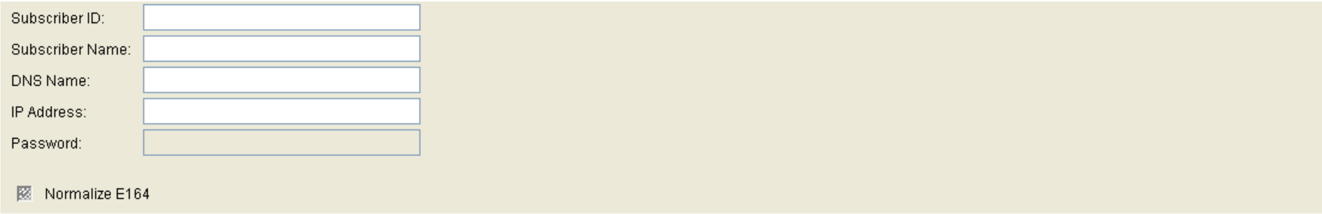
Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CSTA Service Provider

This menu consists of the following submenus:

- General Data
- Possible Action Buttons
- "Connection" Tab
- "Dialup" Tab
- "License" Tab

"Connection" Tab

Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CSTA Service Provider > "Connection" Tab



Subscriber ID:

Subscriber Name:

DNS Name:

IP Address:

Password:

☑ Normalize E164

Subscriber ID:

Subscriber ID resp. extension which is controlled by the CSTA service provider.

Subscriber Name:

Logical name for the extension which is controlled by the CSTA service provider.

DNS Name:

DNS name of the CSTA service provider.

IP Address:

IP address of the CSTA service provider.

Password:

Password required for starting the CSTA service provider.

Normalize E.164:

Activates the normalization of call numbers to E.164 format.

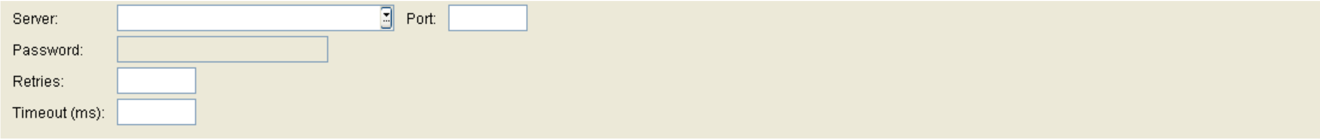
"Dialup" Tab

Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CSTA Service Provider > "Dialup" Tab

See Section 7.2.7.1, ""HFA Dialing Properties" Tab".

"License" Tab

Call: Main Menu > IP Devices > IP Client Configuration > CTI Configuration > CSTA Service Provider > "License" Tab



Server:

IP address of the server that provides the licenses.

Password:

Passwort zum Lizenzserver.

Retries:

Number of retries to establish a connection to the license server.

Timeout (ms):

Timeout for triesto establish a connection to the license server.

Port:

Number of the port used by the license server for delivering licenses.

7.2.2 Gateway/Server

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server

This area features the following components:

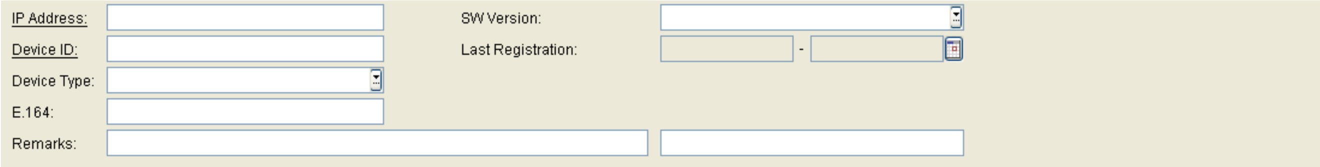
- General Data
- Possible Action Buttons
- "Gateway" Tab
- "Gateway (Standby)" Tab
- "SW Deployment" Tab
- "HFA Settings" Tab
- "SIP Connection" Tab
- "SIP Registrar" Tab
- "SIP Proxy" Tab
- "SIP Gateway" Tab
- "System Services" Tab
- "SIP Survivability" Tab
- "Licenses" Tab
- "VPN Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP clients. The base data associated with the IP clients found is displayed in **Object** view (no changes possible except under **Remarks**).



You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.

All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only **those** IP clients that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of the IP client.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device.

Device Type:

Device type of the IP client.

All IP client types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **optiClient 130**

E.164:

Complete E.164 phone number of the IP client.

Example: **498972212345** (or no input).

For more information, see Chapter 17, "E.164".

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last IP client registration.

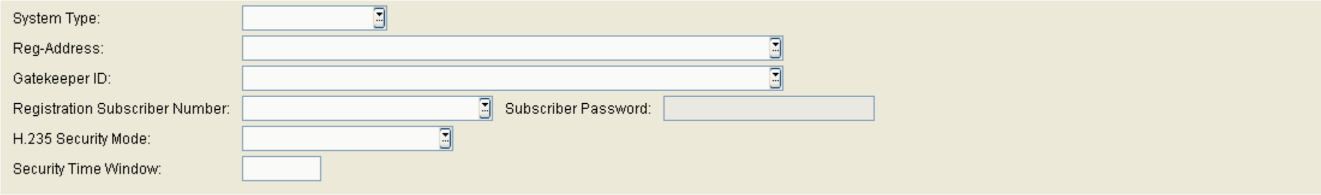
For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Remarks:

Fields for general information.

7.2.2.1 "Gateway" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "Gateway" Tab



System Type:

Type and version of the communication platform at which the workpoint is operated.

Possible options:

- **HiPath 3000**
  Includes HiPath, OpenScape Office MX/LX, and OpenOffice EE, too.
- **HiPath 4000**

Only applies to the HFA configuration of the IP client.

Reg-Address:

IP address or host name of the PBX used to operate the workpoint.

Only applies to the HFA configuration of the IP client.

Gatekeeper ID:

Only applies to the HFA configuration of the IP client.

Registration Subscriber Number:

Phone number of the IP client on the PBX.

Only applies to the HFA configuration of the IP client.

Subscriber Password:

Password of the IP client on the PBX.

Only applies to the HFA configuration of the IP client.

H.235 Security Mode:

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).

- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Only applies to the HFA configuration of the IP client.

Security Time Window:

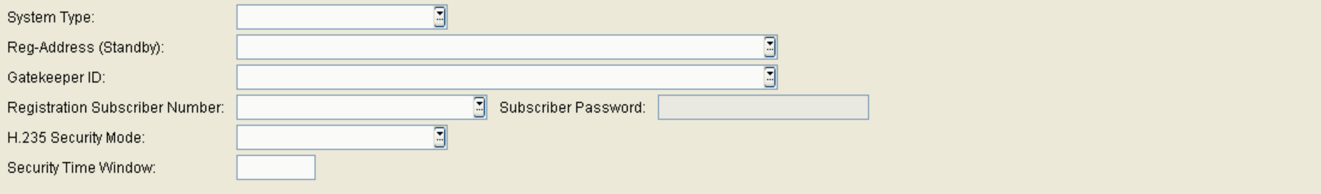
The gateway only accepts messages that arrive during the time window specified here.

Only applies to the HFA configuration of the IP client.

7.2.2.2 "Gateway (Standby)" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "Gateway (Standby)" Tab

> This "standby" data is used when the "home" data for the "Gateway" Tab is not available. The SRSR functionality must be configured for this, see Section 7.2.6, "Small Remote Site Redundancy".



System Type:

Type and version of the communication platform at which the workpoint is operated.

Possible options:

- **HiPath 3000**
  Includes HiPath, OpenScape Office MX/LX, and OpenOffice EE, too.
- **HiPath 4000**
- **No standby system**

Only applies to the HFA configuration of the IP client.

Reg-Address (Standby):

IP address or host name of the standby PBX used to operate the workpoint.

Only applies to the HFA configuration of the IP client.

Gatekeeper ID:

Only applies to the HFA configuration of the IP client.

Registration Subscriber Number:

Phone number of the IP client on the (standby) PBX.

Only applies to the HFA configuration of the IP client.

Subscriber Password:

Password of the IP client on the (standby) PBX.

Only applies to the HFA configuration of the IP client.

H.235 Security Mode:

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Only available on HFA IP clients.

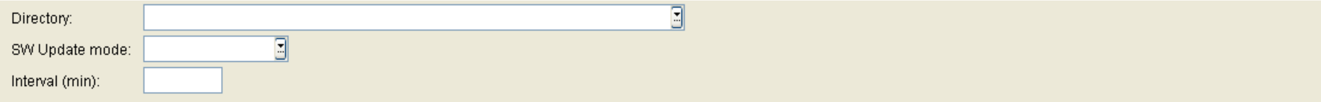
Security Time Window:

The gateway only accepts messages that arrive during the time window specified here.

Only applies to the HFA configuration of the IP client.

7.2.2.3 "SW Deployment" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "SW Deployment" Tab



Directory:

SW Update mode:

Interval (min):

Directory:

Complete path of the directory where the IP client should search for software updates.

SW Update mode

Possible values:

- **None**
  No check.
- **Start**
  Check at program start.
- **Interval**
  Ongoing checks in intervals.

Interval (min):

Interval in minutes for ongoing checks for software updates.

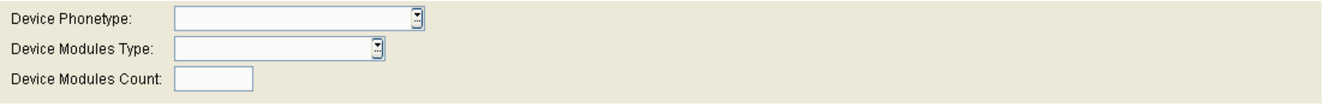
7.2.2.4 "HFA Settings" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "HFA Settings" Tab

The representation of the optiClient 130 telephone is based on the layout of various device phone types.

To display the optiClient 130 telephone and the extended key field, you can choose from a number of different device phone types for telephone and key module.

The telephone and key module type set for optiClient 130 corresponds in terms of display and layout with the relevant desktop devices. Key modules are displayed as columns in optiClient 130's extended key field.



Device Phonetype:

Device Modules Type:

Device Modules Count:

Device Phonetype:

The telephone type defines:

- How many display lines are displayed in optiClient 130's free telephone (always two lines in the main bar in integrated telephones).
- If self labeling keys are available for the optiClients 130 devices
- How many programmable function keys ...
  – are available in optiClient 130.
  – are available in the first column of the extended key field in optiClient 130.

Possible options:

- **optiPoint 420 standard**
- **optiPoint 410 standard (DA Mode)**
- **optiPoint 410 standard**
- **optiPoint 420 advance**
- **optiSet E advance**
- **optiPoint 410 advance**
- **optiSet E comfort**
- **optiSet E advance China**

Device Modules Type:

Possible options:

- **optiPoint Key Module**
- **optiPoint Self Labeling Key Module**
- **optiSet E Key Module**

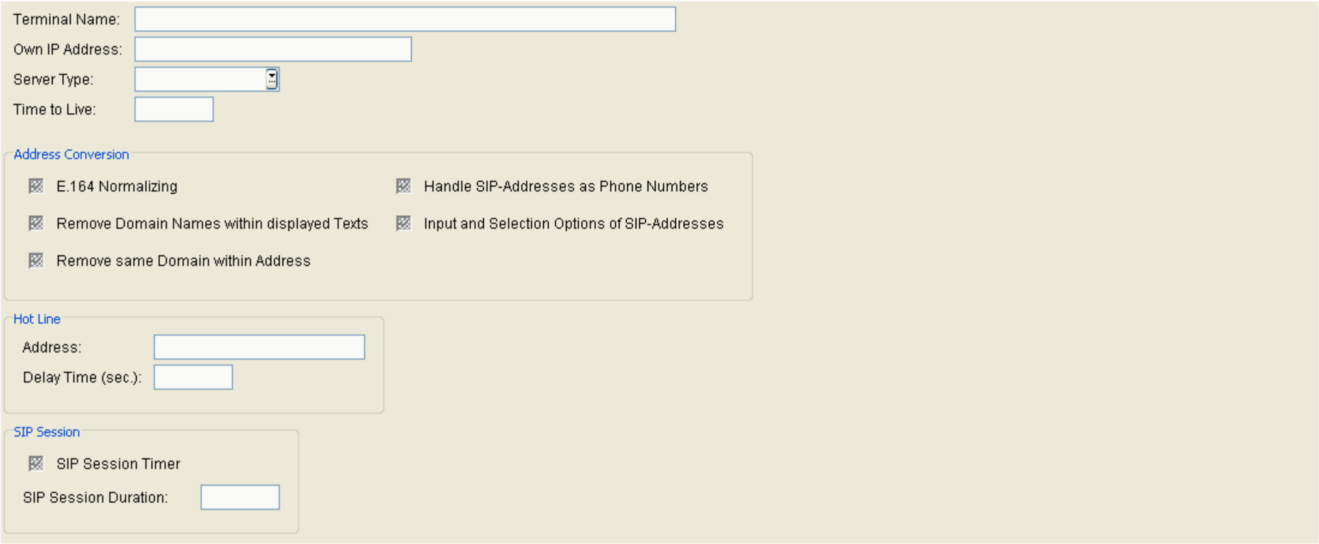
Device Modules Count:

Specifies how many key modules are assigned to the IP client.

Value range: **0** ... **4**

7.2.2.5 "SIP Connection" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "SIP Connection" Tab



Terminal Name

Own IP Address

You can enter the optiClient IP address here. If this field is left empty, the optiClient defines its IP address automatically.

Server Type

Possible options:

- **Standard**
- **OpenScape Voice**
- **hiQ4200**

Time to Live

This value is three times the time taken by the workpoint to register at the gatekeeper to sustain the registration validity. If the value for Time to Live is set to 3 minutes, for example, the workpoint registers every minute.

Value range: **0** ... **4320** minutes.

Address Conversion

E.164 Normalizing

Checkbox for activating phone number normalizing.

Remove Domain Names within displayed Texts

Checkbox for removing the domain name from display texts.

Remove same Domain within Address

Checkbox for removing the domain name from display texts if the called party is located in the same domain.

Handle SIP-Addresses as Phone Numbers

Input and Selection Options of SIP-Addresses

Hot Line

Address:

The address specified here is dialed once the delay time defined for line seizure (for example, on lifting the handset) has elapsed.

Delay Time (sec)

Delay time in seconds for immediate dialing. If the value is 0 the hot line is established without delay.

SIP Session

SIP Session Timer

Checkbox for activating the SIP session timer. The timer is used to monitor the duration of an SIP session.

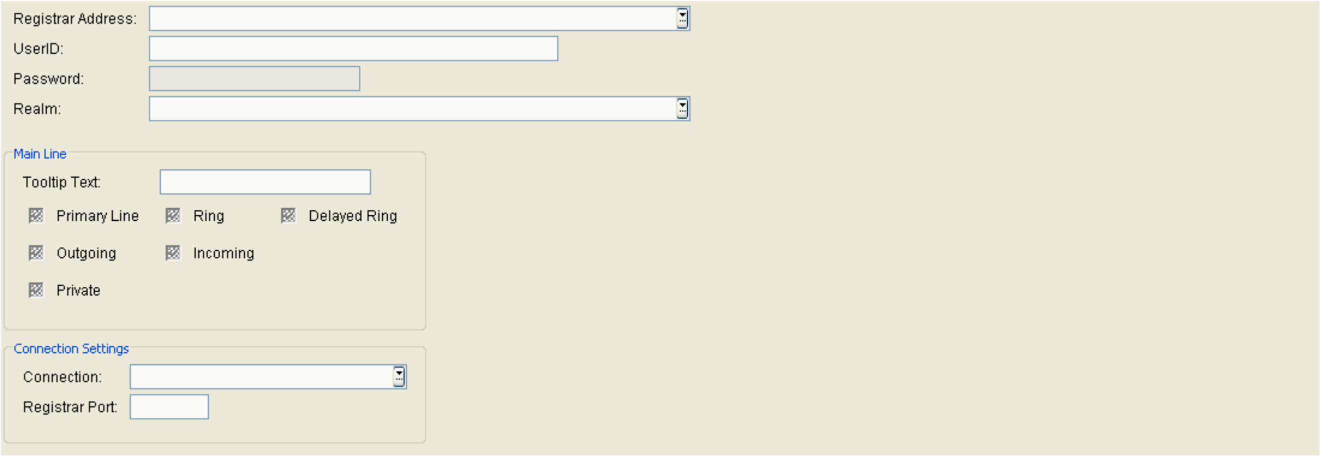
SIP Session Duration:

Highest duration in seconds for an SIP session.

Value range: **0** ... **3600** seconds.

7.2.2.6 "SIP Registrar" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "SIP Registrar" Tab



Registrar Address:

IP address or host name of the SIP registrar.

This setting only applies to the SIP configuration of the IP client.

UserID:

The user ID is the first part of the SIP URL.

Password:

Password required for accessing the SIP server.

Realm:

SIP range in which the workpoint is operated. SIP realm is used to identify the telephone at the SIP server.

Main Line

Tooltip Text:

Defines the display text for the main line.

Primary Line:

Checkbox for marking the main line as a primary line.

Ring

Checkbox for activating the call.

Delayed Ring

Checkbox for activating a delayed call.

Outgoing

Incoming

Private

Connection Settings

Connection

Possible options:

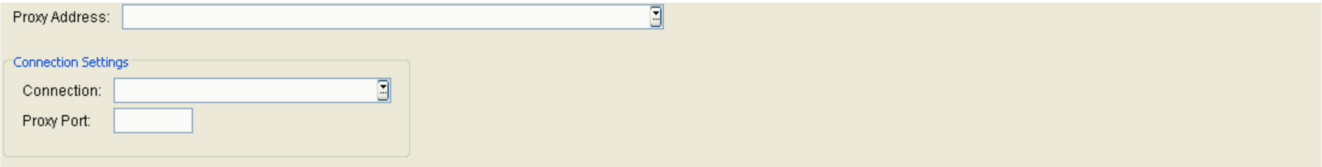
- **Use DNS SRV**
- **Use Standard Port**
- **Use Individual Port**

Registrar Port

Port number of the registrar server.

7.2.2.7 "SIP Proxy" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "SIP Proxy" Tab



Proxy Address

IP address or host name of the SIP proxy.

This setting only applies to the SIP configuration of the IP client.

Connection Settings

Connection

Possible options:

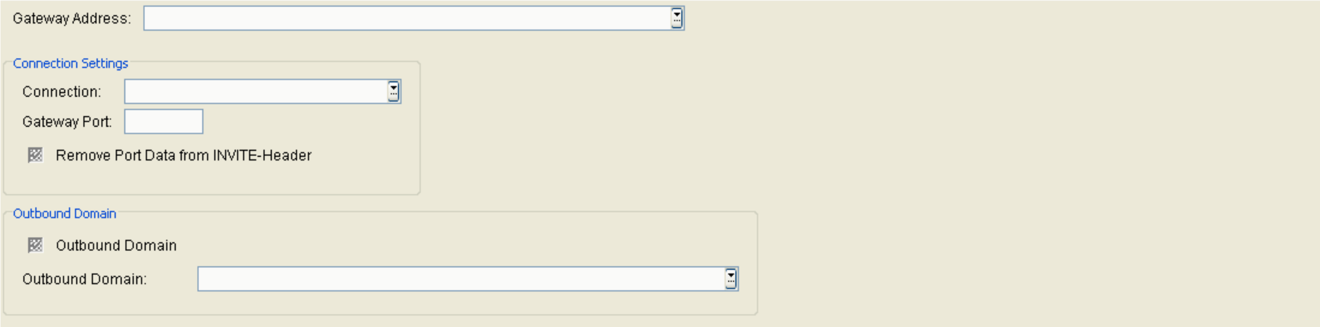
- **Use DNS SRV**
- **Use Standard Port**
- **Use Individual Port**

Proxy Port

Port number of the proxy server.

7.2.2.8 "SIP Gateway" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "SIP Gateway" Tab



Gateway Address:

IP address or host name of the gateway.

This setting only applies to the SIP configuration of the IP client.

Connection Settings

Connection:

Possible options:

- **Use Standard Port**
- **Use Individual Port**

Gateway Port:

Port number of the gateway.

Remove Port Data from INVITE-Header

If this checkbox has been enabled, the port numbers are removed from the INVITE headers.

Outbound Domain

Outbound Domain

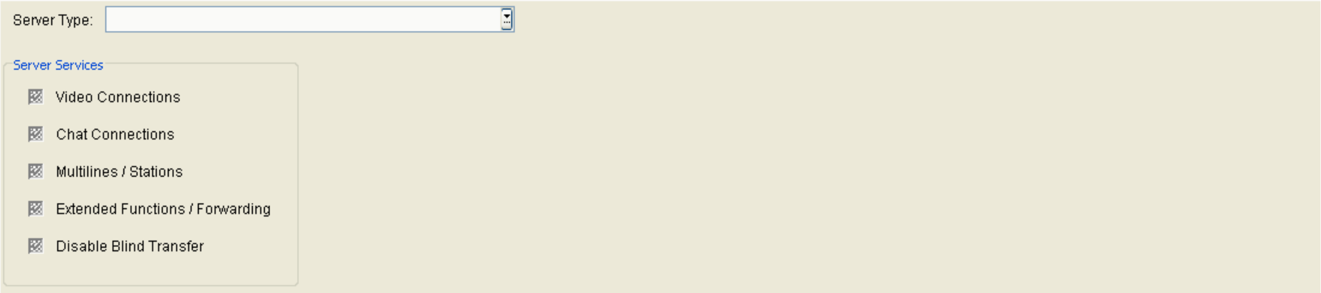
Checkbox for activating the outbound domain.

Outbound Domain:

Name of the outbound domain.

7.2.2.9 "System Services" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "System Services" Tab



Server Type:

Server Services

☑ Video Connections

☑ Chat Connections

☑ Multilines / Stations

☑ Extended Functions / Forwarding

☑ Disable Blind Transfer

Server Type:

Possible options:

- **OpenScape Voice/HQ4200 Chat**
- **OpenScape Voice/HQ4200 Keyset**
- **HiPath 3000/4000/5000 and OpenOffice EE**
- **Standard without Video/Chat**
- **Individual**
- **OpenScape Voice/hiQ4200**
- **OpenScape Voice/hiQ4200 without Video**
- **HiPath 3000 >= V8**
- **HiPath 4000 >= V6**

Server Services

Video Connections

Checkbox for activating video connections.

Chat Connections

Checkbox for activating instant messaging connections.

Multilines / Stations

Checkbox for activating additional lines/stations.

Extended Functions / Forwarding

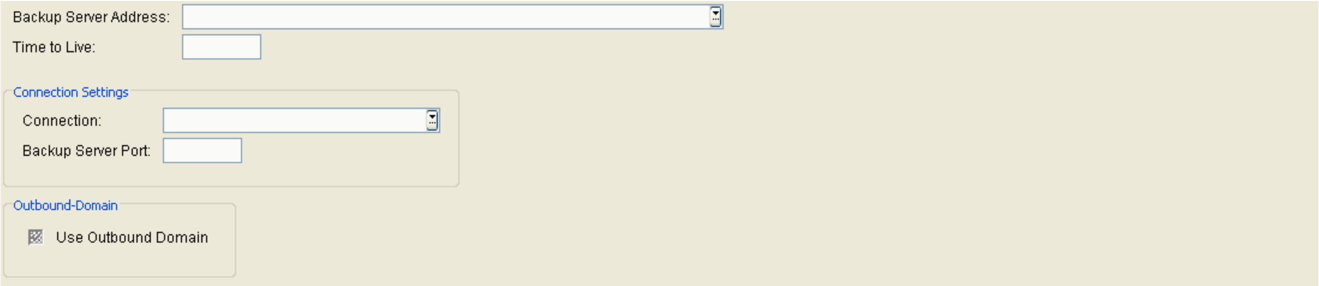
Checkbox for activating enhanced call functions/call forwarding.

Disable Blind Transfer

Switch to disable Blind Transfer

7.2.2.10 "SIP Survivability" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "SIP Survivability" Tab



Backup Server Address:

IP address or host name of the backup server.

Time to Live:

This value is three times the time taken by the workpoint to register at the gatekeeper to sustain the registration validity. If the value for Time to Live is set to 3 minutes, for example, the workpoint registers every minute.

Value range: 0 ... 4320 minutes.

Connection Settings

Connection:

Possible options:

- **Use Standard Port**
- **Use Individual Port**

Backup Server Port:

Port number of the backup server.

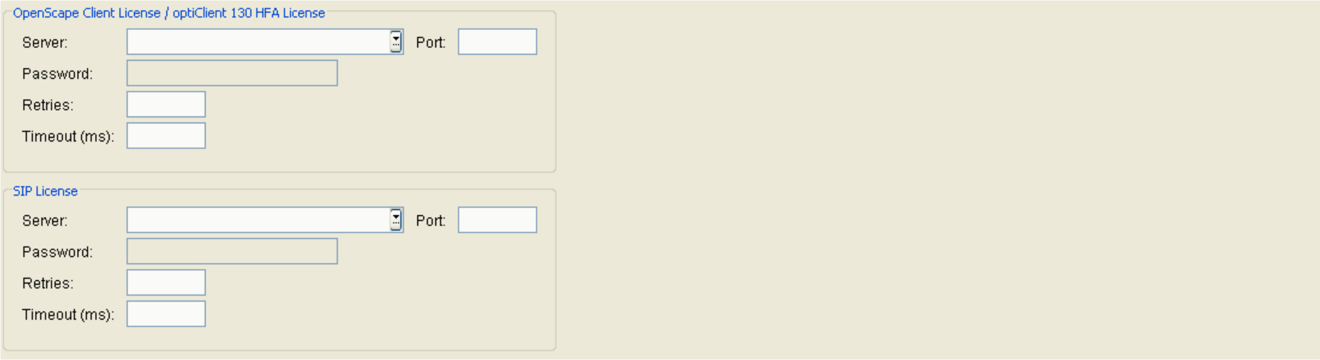
Outbound Domain

Use Outbound Domain

Checkbox for activating use of the outbound domain.

7.2.2.11 "Licenses" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "Licenses" Tab



OpenScape Client License / optiClient 130 HFA License

Server:

IP address or host name of the license server.

Port:

Port number for access to the license server.

Default: **61740**

Password:

Password for access to the license server.

Retries:

Maximum number of connection attempts.

Timeout (ms):

The maximum time (in milliseconds) for the attempt to set up a connection to the license server.

SIP License

Server:

IP address or host name of the license server.

Port:

Port number for access to the license server.

Default: **61740**

Password:

Password for access to the license server.

Retries:

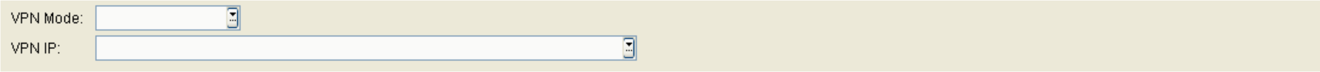
Maximum number of connection attempts.

Timeout (ms):

The maximum time (in milliseconds) for the attempt to set up a connection to the license server.

7.2.2.12 "VPN Settings" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Gateway/Server > "VPN Settings" Tab



VPN Mode:

VPN IP:

VPN Mode:

Possible options:

- **None**
  VPN (Virtual Private Network) is not used.
- **Automatic**
  VPN is used with an automatically determined IP address.
- **Manual**
  VPN is used with the IP address specified in the case of **VPN IP**.

VPN IP:

IP address for the VPN (Virtual Private Network).

7.2.3 Ports

Call: Main Menu > IP Devices > IP Client Configuration > Ports

This area features the following components:

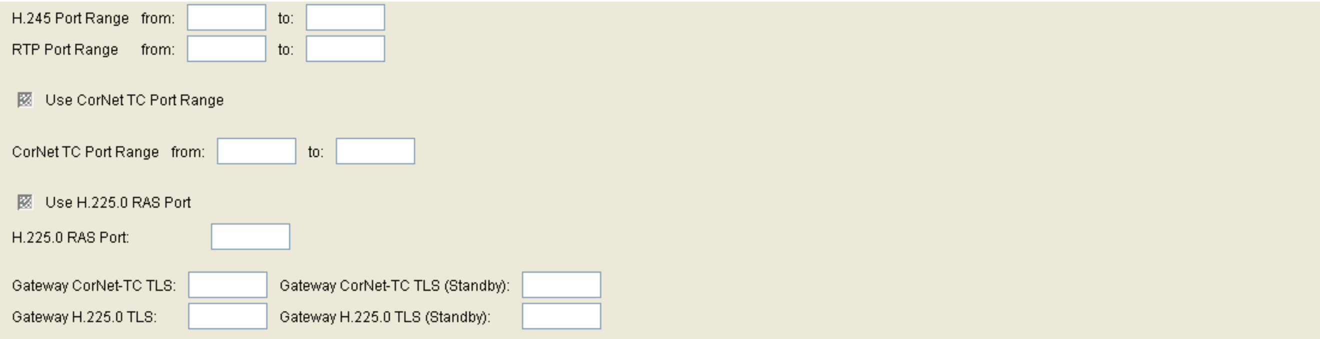
- General Data
- Possible Action Buttons
- "Ports" Tab
- "SIP Ports" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.3.1 "Ports" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Ports > "Ports" Tab



H.245 Port Range from: ______ to: ______

RTP Port Range from: ______ to: ______

☒ Use CorNet TC Port Range

CorNet TC Port Range from: ______ to: ______

☒ Use H.225.0 RAS Port

H.225.0 RAS Port: ______

Gateway CorNet-TC TLS: ______ Gateway CorNet-TC TLS (Standby): ______

Gateway H.225.0 TLS: ______ Gateway H.225.0 TLS (Standby): ______

H.245 Port Range from: ... to:

Port range for H.245.

RTP Port Range from: ... to:

Port range for RTP.

Use Cornet TC Port Range

Checkbox for activating Cornet TC.

Cornet TC Port Range from: ... to:

Port range for Cornet TC.

Use H.225.0 RAS Port

Checkbox for activating Cornet TC.

H.225.0 RAS Port:

For using NetMeeting at the same time as optiClient 130.

Gateway CorNet-TC TLS

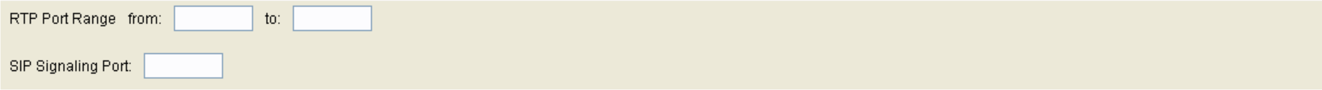
Gateway H.225.0 TLS

Gateway CorNet-TC TLS (Standby)

Gateway H.225.0 TLS (Standby)

7.2.3.2 "SIP Ports" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Ports > "SIP Ports" Tab



RTP Port Range from: to:

SIP Signaling Port:

RTP Port Range from: ... to:

Port range for RTP.

Only applies to the SIP configuration of the IP client.

SIP Signaling Port:

Only applies to the SIP configuration of the IP client.

7.2.4 Quality of Service

Call: Main Menu > IP Devices > IP Client Configuration > Quality of Service

This area features the following components:

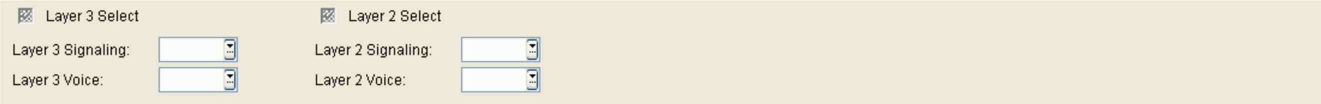
- General Data
- Possible Action Buttons
- "Settings" Tabs
- "Alternate Settings (SIP)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.4.1 "Settings" Tabs

Call: Main Menu > IP Devices > IP Client Configuration > Quality of Service > "Settings" Tabs



☑ Layer 3 Select
Layer 3 Signaling:
Layer 3 Voice:

☑ Layer 2 Select
Layer 2 Signaling:
Layer 2 Voice:

Layer 3 Select

Checkbox for activating layer 3 (network layer).

Layer 3 Signaling:

Priority for layer 3 signaling.

Can only be defined if **Layer 3 Select** is active.

Possible options:

- **Default**
- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CST**

Layer 3 Voice:

Priority for layer 3 voice.

Can only be defined if **Layer 3 Select** is active.

Same options as for **Layer 3 Signaling**.

Layer 2 Select

Checkbox for activating layer 2 (data link layer).

Layer 2 Signaling:

Priority for layer 2 signaling.

Can only be defined if **Layer 2 Select** is active.

Value range: 0 ... 7.

Layer 2 Voice:

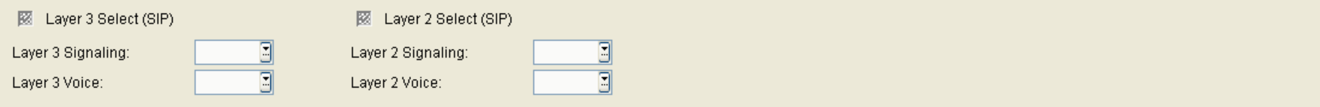
Priority for layer 2 voice.

Can only be defined if **Layer 2 Select** is active.

Same options as for **Layer 2 Signaling**.

7.2.4.2 "Alternate Settings (SIP)" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Quality of Service > "Alternate Settings (SIP)" Tab



Layer 2 Select (SIP)

Checkbox for activating layer 2 (data link layer).

Layer 2 Signaling:

Priority for layer 2 signaling.

Can only be defined if **Layer 2 Select** is active.

Value range: **0** ... **7**

Layer 2 Voice:

Priority for layer 2 voice.

Can only be defined if Layer 2 Select is active.

Same options as for Layer 2 Signaling.

Layer 3 Select (SIP)

Checkbox for activating layer 3 (network layer).

Layer 3 Signaling

Can only be defined if **Layer 3 Select (SIP)** is active.

Possible options:

- **Default**
- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**

- **AF43**
- **EF**
- **CST**

Layer 3 Voice:

Priority for layer 3 voice.

Can only be defined if **Layer 3 Select (SIP)** is active.

Possible options:

- **Default**
- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CST**

7.2.5 Telephony

Call: Main Menu > IP Devices > IP Client Configuration > Telephony

This area features the following components:

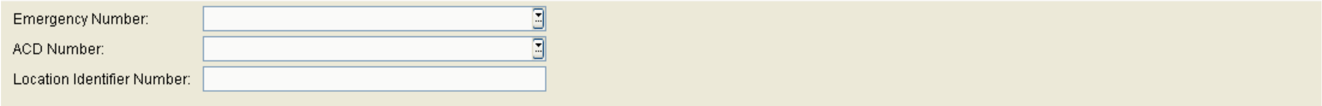
- General Data
- Possible Action Buttons
- "Telephony" Tab
- "Telephony (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.5.1 "Telephony" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Telephony > "Telephony" Tab



Emergency Number:

ACD Number:

Location Identifier Number:

Emergency Number:

Contains the phone number that can be dialed in an emergency.

ACD Number:

ACD agent number if you are working as an ACD agent.

Location Identifier Number

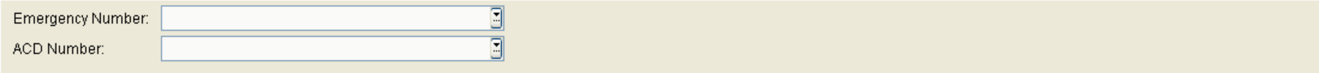
Contains an identification number for unique location identification. This number can be used, for example, to pinpoint the **origin** of an emergency call.

Available for optiClient 130 V4.0 only.

7.2.5.2 "Telephony (Standby)" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Telephony > "Telephony (Standby)" Tab

> This "standby" data is used when the "home" data for the "Telephony" Tab is not available. The SRSR functionality must be configured for this, see Section 7.2.6, "Small Remote Site Redundancy".



Emergency Number:	
ACD Number:	

Emergency Number:

Contains the phone number that can be dialed in an emergency.

ACD Number:

ACD agent number if you are working as an ACD agent.

7.2.6 Small Remote Site Redundancy

Call: Main Menu > IP Devices > IP Client Configuration > Small Remote Site Redundancy

This area features the following components:

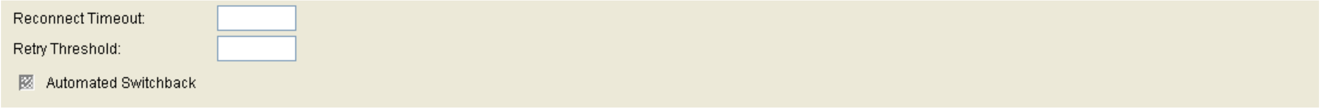
- General Data
- Possible Action Buttons
- "SRSR Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.6.1 "SRSR Settings" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Small Remote Site Redundancy > "SRSR Settings" Tab



Reconnect Timeout:

Retry Threshold:

☑ Automated Switchback

Reconnect Timeout:

Timeout for switchover to the main system.

Value range: **1** ... **255** seconds.

Retry Threshold:

Specifies the number of attempts permitted when switching back to the standby system.

Value range: **1** ... **255**

Automated Switchback

Checkbox for activating the option for automatic switchback to the main system.

7.2.7 Dialing Properties

Call: Main Menu > IP Devices > IP Client Configuration > Dialing Properties

This area features the following components:

- General Data
- Possible Action Buttons
- "HFA Dialing Properties" Tab
- "HFA Dialing Properties (Standby)" Tab
- "SIP Dialing Properties" Tab

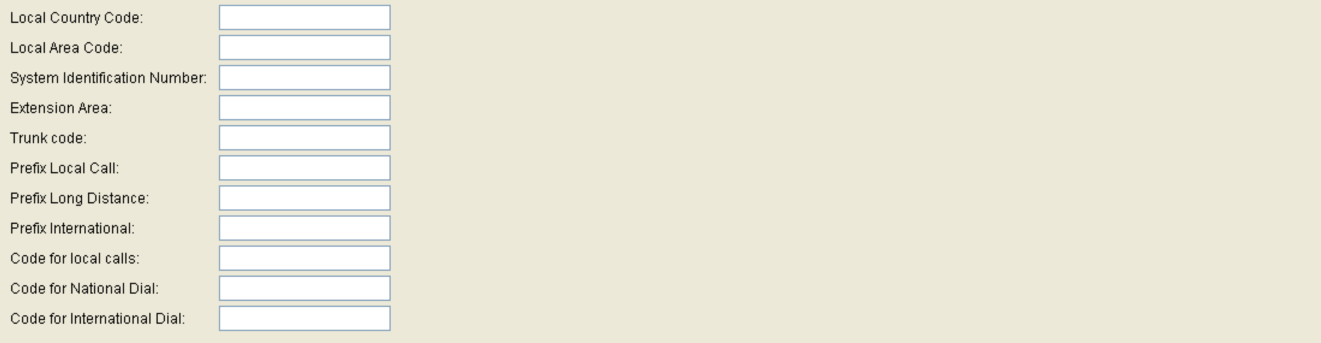
For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.7.1 "HFA Dialing Properties" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Dialing Properties > "HFA Dialing Properties" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").



Local Country Code:	
Local Area Code:	
System Identification Number:	
Extension Area:	
Trunk code:	
Prefix Local Call:	
Prefix Long Distance:	
Prefix International:	
Code for local calls:	
Code for National Dial:	
Code for International Dial:	

Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

System Identification number:

Phone number of the system.

Format: Up to 21 digits.

Example: **722** for Siemens Munich, Hofmannstraße.

Extension Area:

This parameter defines a pattern for detecting internal extension numbers. From the workpoint's perspective, extension numbers are internal if they are assigned to the same system. The extension area can be specified as a regular expression.

Example: 1xxx, 2xxx, 3xxx, 4xxx, 5xxx are extensions and 6xxx, 7xxx, 8xxx, 9xxx are external phone numbers. The regular expression ^[12345] indicates that phone numbers starting with the digits 1 to 5 are internal extension numbers. If for example the system identification number is 667, all numbers from 6671xxxx to 6675xxx will be used as internal extensions.

Trunk code:

Number for trunk seizure for an outbound external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Prefix Local Call:

Format: Up to 21 digits.

Example: **01081**

Prefix Long Distance:

Number for an outbound long distance call.

Format: Up to 21 digits.

Example: **01081**

Prefix International:

Number for an outbound international call.

Format: Up to 21 digits.

Example: **01081**

Code for local calls:

Phone number, for example, of your company.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **722** for Siemens Munich Hofmannstraße.

Code for National Dial:

National prefix.

Format: Up to five digits.

Example: **0** in Germany.

Code for International Dial:

International prefix.

Format: Up to four digits.

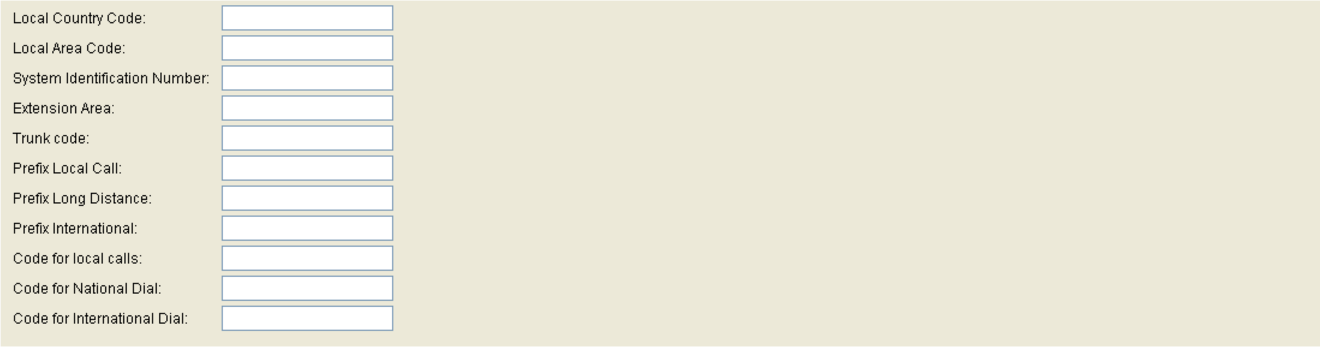
Example: **00** in Germany.

7.2.7.2 "HFA Dialing Properties (Standby)" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Dialing Properties > "HFA Dialing Properties (Standby)" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").

> This "standby" data is used when the "home" data for the "HFA Dialing Properties" Tab is not available. The SRSR functionality must be configured for this, see Section 7.2.6, "Small Remote Site Redundancy".



Local Country Code:

Local Area Code:

System Identification Number:

Extension Area:

Trunk code:

Prefix Local Call:

Prefix Long Distance:

Prefix International:

Code for local calls:

Code for National Dial:

Code for International Dial:

Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

System Identification number:

Phone number of the system.

Format: Up to 21 digits.

Example: **722** for Siemens Munich, Hofmannstraße.

Extension Area:

This parameter defines a pattern for detecting internal extension numbers. From the workpoint’s perspective, extension numbers are internal if they are assigned to the same system. The extension area can be specified as a regular expression.

Example: 1xxx, 2xxx, 3xxx, 4xxx, 5xxx are extensions and 6xxx, 7xxx, 8xxx, 9xxx are external phone numbers. The regular expression ^[12345] indicates that phone numbers starting with the digits 1 to 5 are internal extension numbers. If for example the system identification number is 667, all numbers from 6671xxxx to 6675xxx will be used as internal extensions.

Trunk code:

Number for trunk seizure for an outbound external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Prefix Local Call:

Format: Up to 21 digits.

Example: **01081**

Prefix Long Distance:

Number for an outbound long distance call.

Format: Up to 21 digits.

Example: **01081**

Prefix International:

Number for an outbound international call.

Format: Up to 21 digits.

Example: **01081**

Code for local calls:

Phone number, for example, of your company.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **722** for Siemens Munich Hofmannstraße.

Code for National Dial:

National prefix.

Format: Up to five digits.

Example: **0** in Germany.

Code for International Dial:

International prefix.

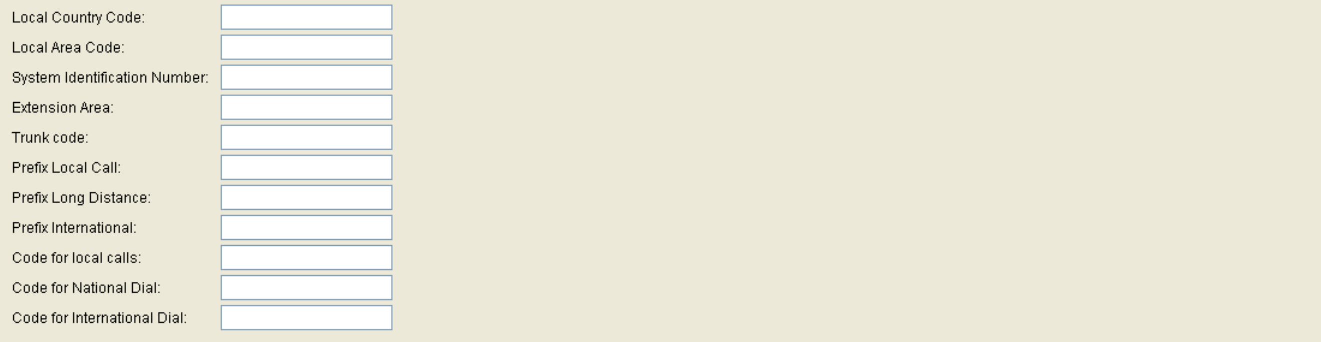
Format: Up to four digits.

Example: **00** in Germany.

7.2.7.3 "SIP Dialing Properties" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Dialing Properties > "SIP Dialing Properties" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").



Local Country Code:	
Local Area Code:	
System Identification Number:	
Extension Area:	
Trunk code:	
Prefix Local Call:	
Prefix Long Distance:	
Prefix International:	
Code for local calls:	
Code for National Dial:	
Code for International Dial:	

Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

System Identification number:

Phone number of the system.

Format: Up to 21 digits.

Example: **722** for Siemens Munich, Hofmannstraße.

Extension Area:

This parameter defines a pattern for detecting internal extension numbers. From the workpoint's perspective, extension numbers are internal if they are assigned to the same system. The extension area can be specified as a regular expression.

Example: 1xxx, 2xxx, 3xxx, 4xxx, 5xxx are extensions and 6xxx, 7xxx, 8xxx, 9xxx are external phone numbers. The regular expression ^[12345] indicates that phone numbers starting with the digits 1 to 5 are internal extension numbers. If for example the system identification number is 667, all numbers from 6671xxxx to 6675xxx will be used as internal extensions.

Trunk code:

Number for trunk seizure for an outbound external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Prefix Local Call:

Format: Up to 21 digits.

Example: **01081**

Prefix Long Distance:

Number for an outbound long distance call.

Format: Up to 21 digits.

Example: **01081**

Prefix International:

Number for an outbound international call.

Format: Up to 21 digits.

Example: **01081**

Code for local calls:

Phone number, for example, of your company.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **722** for Siemens Munich Hofmannstraße.

Code for National Dial:

National prefix.

Format: Up to five digits.

Example: **0** in Germany.

Code for International Dial:

International prefix.

Format: Up to four digits.

Example: **00** in Germany.

7.2.8 Audio/Video Settings

Call: Main Menu > IP Devices > IP Client Configuration > Audio/Video Settings

This area features the following components:

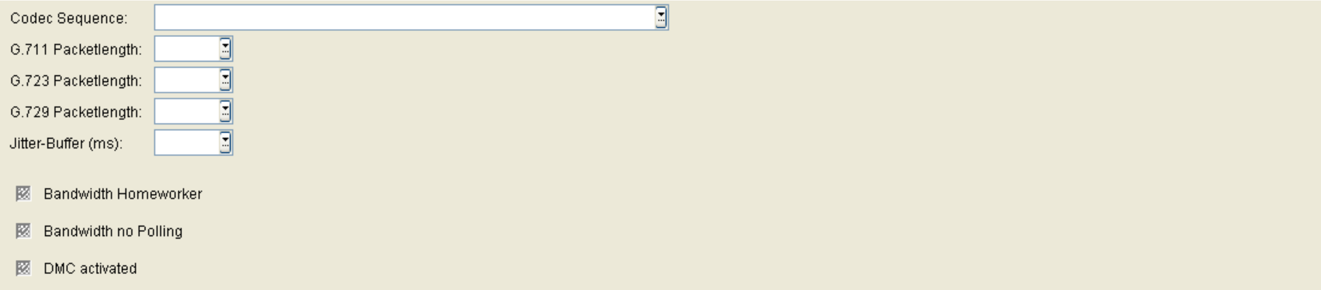
- General Data
- Possible Action Buttons
- "HFA Codec Settings" Tab
- "SIP Codec Settings" Tab
- "Audio Schemes" Tab
- "Available Audio Devices" Tab
- "Video Settings" Tab
- "Available Video Devices"

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.8.1 "HFA Codec Settings" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Audio/Video Settings > "HFA Codec Settings" Tab



Codec Sequence:

G.711 Packetlength:

G.723 Packetlength:

G.729 Packetlength:

Jitter-Buffer (ms):

☒ Bandwidth Homeworker

☒ Bandwidth no Polling

☒ DMC activated

Codec Sequence:

Possible options:

- **not compressing Codecs preferred, besides G.723 preferred**
- **not compressing Codecs preferred, besides G.729 preferred**
- **compressing Codecs preferred, G.723 preferred**
- **compressing Codecs preferred, G.729 preferred**
- **only compressing Codecs, G.723 preferred**
- **only compressing Codecs, G.729 preferred**

G.711 Packetlength:

Possible options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

G.723 Packetlength:

Possible options:

- **30**
- **60**

G.729 Packetlength:

Possible options:

- **10**
- **20**
- **30**

- **40**
- **50**
- **60**

Jitter-Buffer (ms):

Caching duration:

Possible options (in ms):

Value range: **20** ... **190** milliseconds.

Bandwidth Homeworker

Checkbox for activating the bandwidth for homeworker data transmission.

Bandwidth no polling

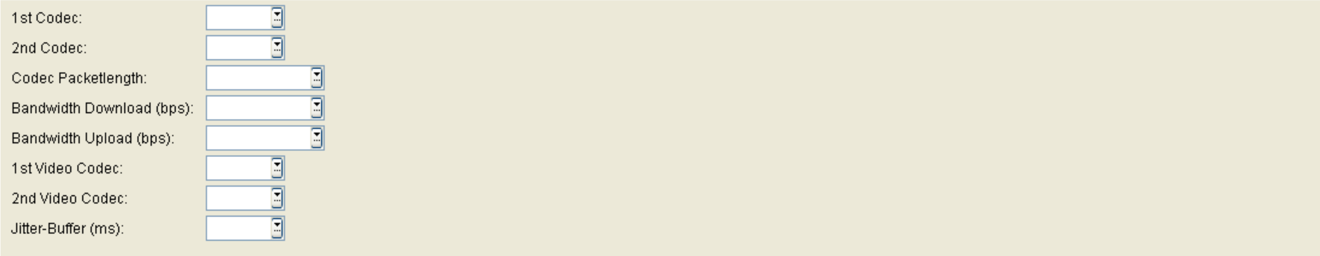
Checkbox for activating the bandwidth with no polling.

DMC activated

Checkbox for activating DMC bandwidth.

7.2.8.2 "SIP Codec Settings" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Audio/Video Settings > "SIP Codec Settings" Tab



1st Codec:

2nd Codec:

Codec Packetlength:

Bandwidth Download (bps):

Bandwidth Upload (bps):

1st Video Codec:

2nd Video Codec:

Jitter-Buffer (ms):

1st Codec:

First compression job.

Possible options:

- **G.711**
- **G.729**

2nd Codec:

Second compression job.

Possible options:

- **G.711**
- **G.729**
- **None**

Codec Packetlength:

Possible options:

- **Automatic**
- **10**
- **20**

Bandwidth Download (bps)

Possible options:

- **56**
- **64**
- **128**
- **256**
- **512**
- **1024**
- **2048**

- **3072**
- **6144**
- **10000**
- **12288**
- **24576**
- **100000**
- **1000000**

Bandwidth Upload (bps)

Possible options:

- **56**
- **64**
- **128**
- **256**
- **512**
- **1024**
- **2048**
- **3072**
- **6144**
- **10000**
- **12288**
- **24576**
- **100000**
- **1000000**

1st Video Codec

Possible options:

- **H.263**
- **H.264**

2nd Video Codec

Possible options:

- **H.263**
- **H.264**
- **None**

Jitter-Buffer (ms)

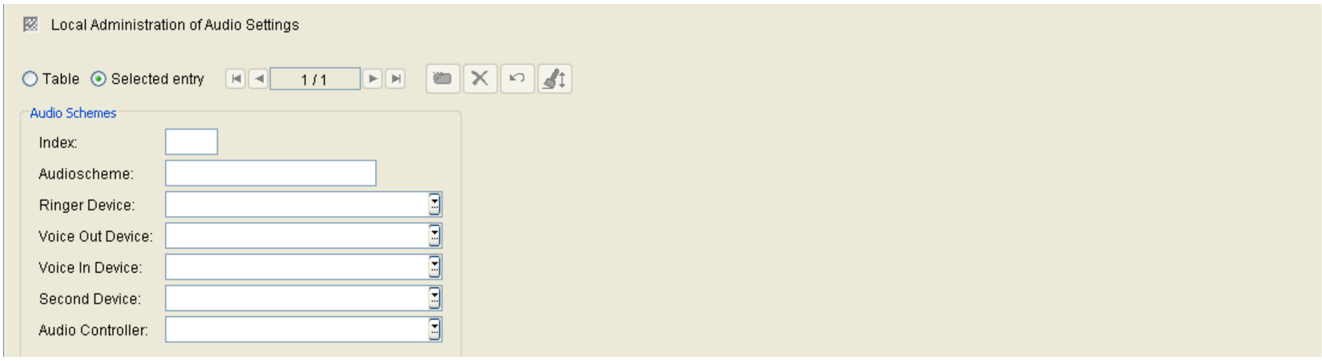
Possible options:

- **20**

- **30**
- **40**
- **50**
- **60**
- **70**
- **80**
- **90**
- **100**
- **110**
- **120**
- **130**
- **140**
- **150**
- **160**
- **170**
- **180**
- **190**

7.2.8.3 "Audio Schemes" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Audio/Video Settings > "Audio Schemes" Tab



These tabs let you define hardware settings for the voice output or ringer devices, for example.

Local Administration of Audio Settings

If this checkbox is activated, the audio settings can be changed only on the optiClient, but not by the DLS. In this case, the fields under **Audio Schemes** are only for display.

If this checkbox is inactive, the audio settings can be changed only by the DLS.

Index

Number of the setting.

Audioscheme

Name of the audioscheme.

Ringer Device

Audio hardware for the ringer device.

Voice Out Device

Audio hardware for the voice out device.

Voice In Device

Audio hardware for the voice in device.

Second Device

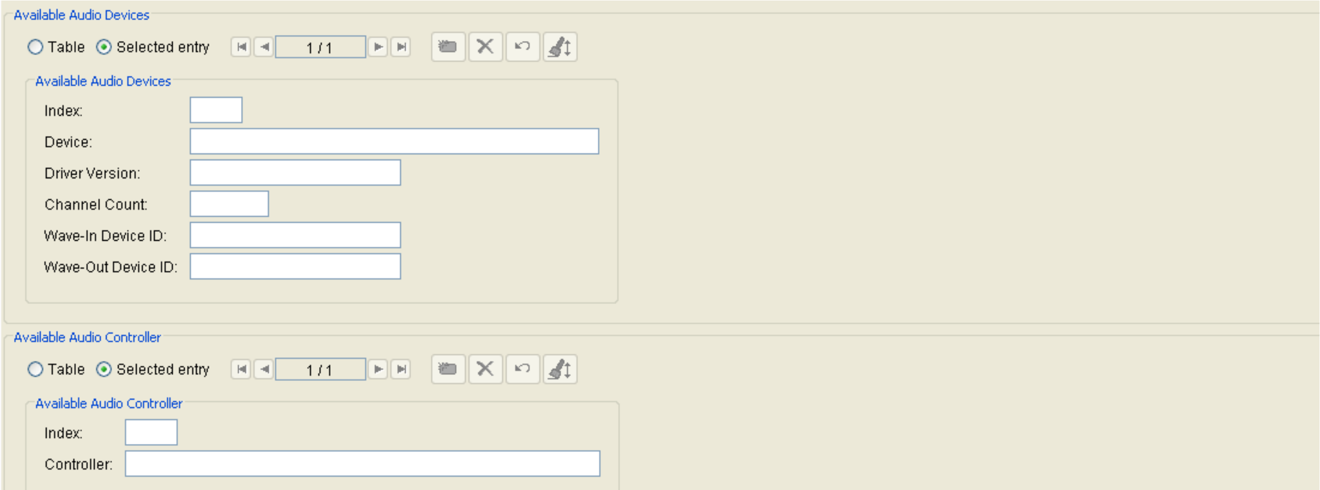
Audio hardware representing a second device. If a second device is selected here and this audioscheme is active, an additional icon appears in the main menu for controlling the second device.

Audio Controller

Additional function for controlling hardware functions.

7.2.8.4 "Available Audio Devices" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Audio/Video Settings > "Available Audio Devices" Tab



Available Audio Devices

○ Table ● Selected entry 1 / 1

Available Audio Devices

Index:

Device:

Driver Version:

Channel Count:

Wave-In Device ID:

Wave-Out Device ID:

Available Audio Controller

○ Table ● Selected entry 1 / 1

Available Audio Controller

Index:

Controller:

Available Devices:

Index

Serial number of the audio device.

Device

Name of the audio device for alerting and voice.

Driver Version

Driver version for the audio device.

Channel Count

Number of available audio channels.

Wave-In Device ID

Wave-Out Device ID

Available Audio Controller:

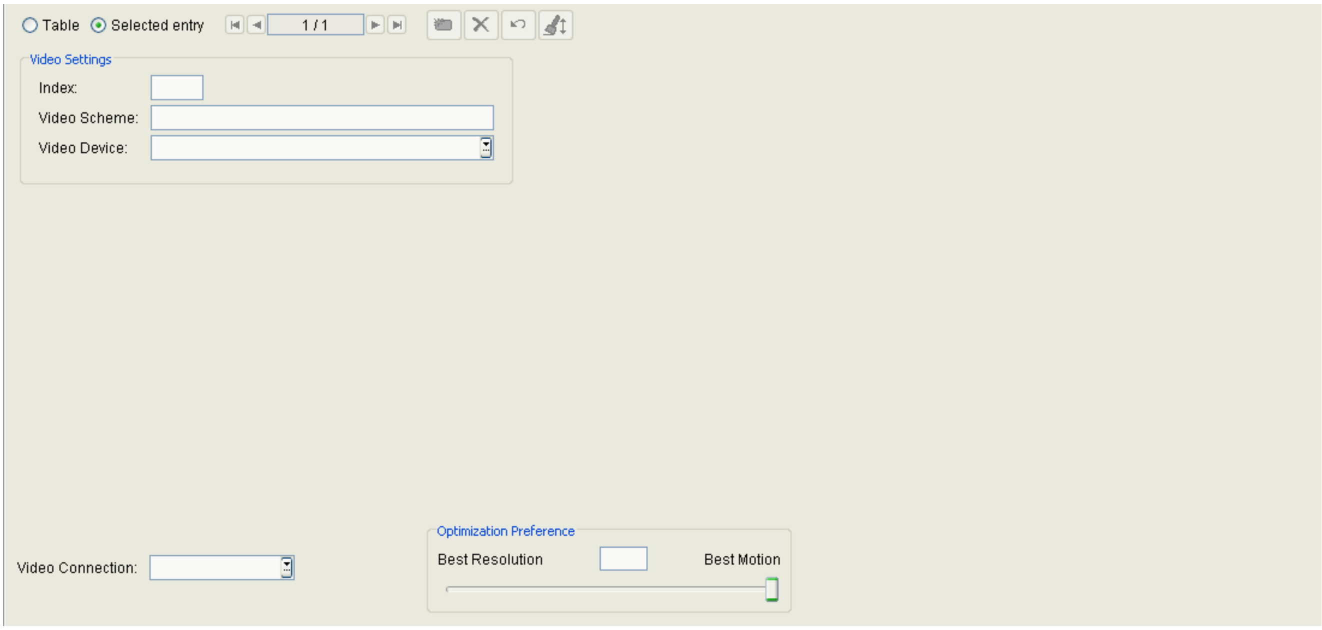
Index

Number of the setting

Controller

7.2.8.5 "Video Settings" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Audio/Video Settings > "Video Settings" Tab



Index

Number of the setting.

Video Scheme

Name of the video scheme.

Video Device

Camera for transmitting the picture in video connections.

Video Connection

optiClient 130 allows parties to connect their video pictures providing both parties have an operational video system.

Possible options:

- **Locked**
- **Optional**

Optimization Preference

Best Resolution

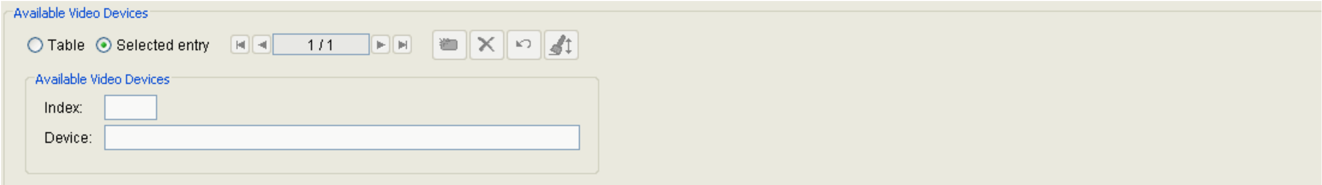
Optimization to the highest possible resolution.

Best Motion

Optimization to the best possible reproduction of movement.

7.2.8.6 "Available Video Devices"

Call: Main Menu > IP Devices > IP Client Configuration > Audio/Video Settings > "Available Video Devices"



Index

Number of the setting.

Device

All cameras installed on the workstation are listed. Select the camera you wish to use. If no cameras are listed here, your PC is not equipped with a video camera.

7.2.9 Directories/Address Books

Call: Main Menu > IP Devices > IP Client Configuration > Directories/Address Books

This area features the following components:

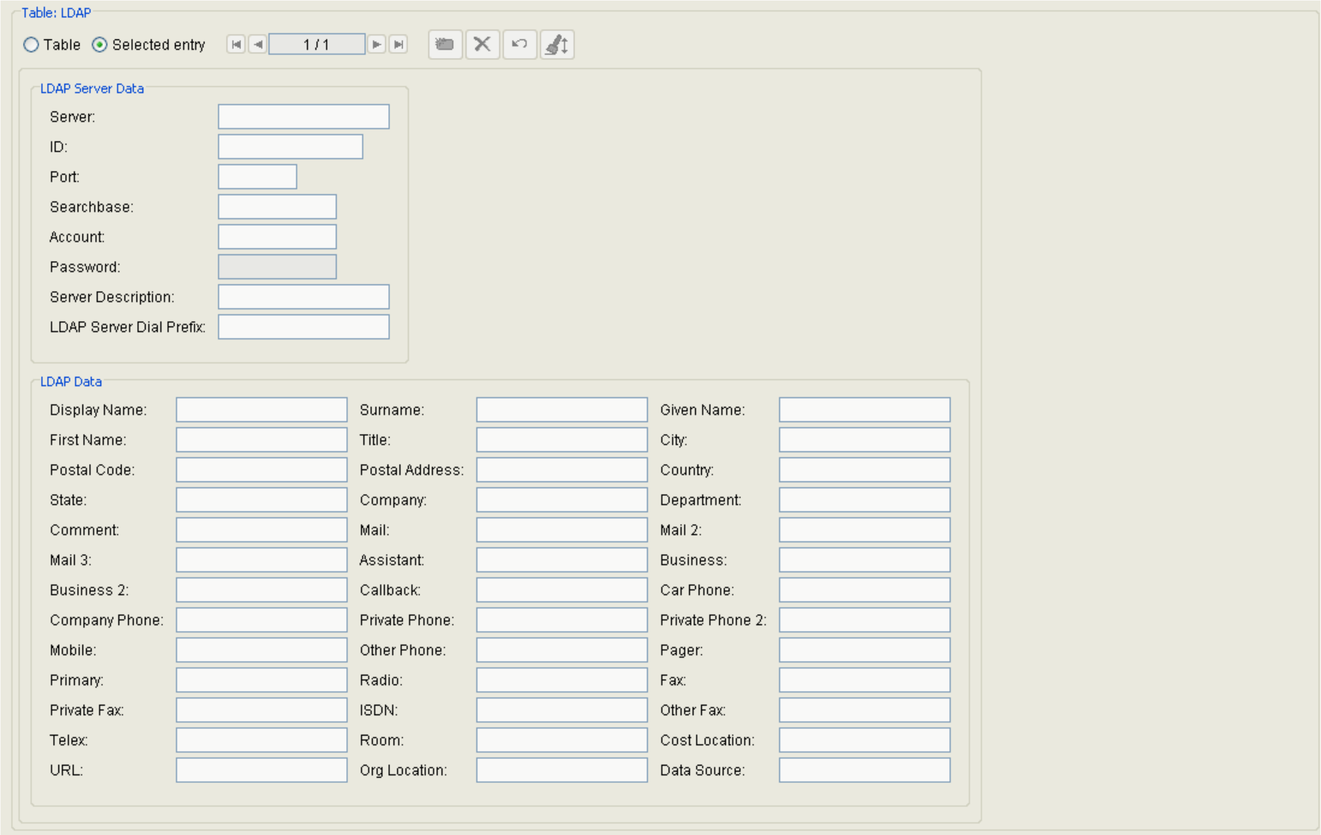
- General Data
- Possible Action Buttons
- "LDAP" Tab
- "Directory Service" Tab
- "Internet Pages" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.9.1 "LDAP" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Directories/Address Books > "LDAP" Tab



You can configure access to any LDAP directories in the network.

Server

IP address or host name of the LDAP server.

ID

Name of the LDAP server.

Port

Port number of the LDAP server.

Account

LDAP server account.

Password

Password for accessing the LDAP server.

Server Description

Descriptive text for the LDAP server.

Searchbase

During LDAP server configuration, this function allows you to specify a base level

which is used as a starting point for searching or displaying optiClient 130 entries in this LDAP directory.

You can use two different formats to define a base level:

`<level 3>=<name>, <level 2>=<name>, <level 1>=<name>` or

`<level 1>=<name>/<level 2>=<name>/<level 3>=<name>`

Example of an LDAP directory with the following elements:

- Level 1: c (for example for "country"), name, for example: US
- Level 2: o (for example, for "organization"), name, for example, Siemens
- Level 3: ou (for example for "organization unit"), name, for example, COM

To specify this level as a searchbase, enter the following information in **Searchbase**:

`ou=COM, o=Siemens, c=US` or `c=US/o=Siemens/ou=COM`.

If you do not restrict the searchbase, the entire LDAP directory is used as the searchbase.

LDAP Server Dial Prefix

If LDAP directory services are generally available in the network and configured in the user settings, these are available under the configured name (for example, "Siemens Corporate Directory"). This means you can configure and use several LDAP directories.

Display Name

Activates display name display and the entry of a label for the display name.

Surname

Activates name display and the entry of a label for the name.

Given Name

Activates second name display and the entry of a label for the second name.

First Name

Activates first name display and the entry of a label for the first name.

Title

Activates title display and the entry of a label for the title.

City

Activates city display and the entry of a label for the city.

Postal Code

Activates postal code display and the entry of a label for the postal code.

Postal Address

Activates postal address display and the entry of a label for the postal address.

Country

Activates country display and the entry of a label for the country.

State

Activates state display and the entry of a label for the state.

Company

Activates company display and the entry of a label for the company.

Department

Activates department display and the entry of a label for the department.

Comment

Activates comment display and the entry of a label for the comment.

Mail

Activates mailbox display and the entry of a label for the mailbox.

Mail 2

Activates second mailbox display and the entry of a label for the second mailbox.

Mail 3

Activates third mailbox display and the entry of a label for the third mailbox.

Assistant

Activates assistant display and the entry of a label for the assistant.

Business

Activates business display and the entry of a label for the business area.

Business 2

Activates second business display and the entry of a label for the second business area.

Callback

Activates callback number display and the entry of a label for the callback number.

Car Phone

Activates car phone number display and the entry of a label for the car phone number.

Company Phone

Activates company phone number display and the entry of a label for the company phone number.

Private Phone

Activates private phone number display and the entry of a label for the private phone number.

Private Phone 2

Activates second private phone number display and the entry of a label for the second private phone number.

Mobile

Activates mobile phone number display and the entry of a label for the mobile phone number.

Other Phone

Activates another phone number display and the entry of a label for the other phone number.

Pager

Activates pager number display and the entry of a label for the pager number.

Primary

Radio

Fax

Activates fax number display and the entry of a label for the fax number.

Private Fax

Activates private fax number display and the entry of a label for the private fax number.

ISDN

Activates ISDN number display and the entry of a label for the ISDN number.

Other Fax

Activates another fax number display and the entry of a label for the other fax number.

Telex

Activates telex number display and the entry of a label for the telex number.

Room

Activates room number display and the entry of a label for the room number.

Cost Location

Activates cost location display and the entry of a label for the cost location.

URL

Activates URL display and the entry of a label for the URL.

Location

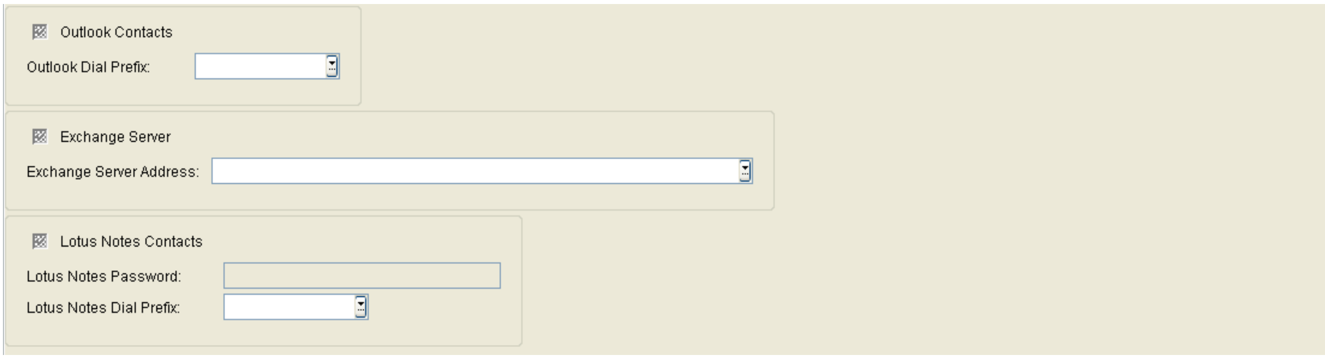
Activates location display and the entry of a label for the location.

Data Source

Activates data source display and the entry of a label for the data source.

7.2.9.2 "Directory Service" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Directories/Address Books > "Directory Service" Tab



You can configure different settings for accessing central and local directories. This access enables you to work with directories and address books in optiClient 130.

Outlook Contacts

This directory contains all entries from the Contacts folder in a local Microsoft Outlook installation. If Outlook is not installed or this directory is not configured for your users, then this directory is not available.

This checkbox creates a directory containing Outlook contact information in the optiClient 130.

Outlook Dial Prefix:

This directory contains all entries from the Contacts folder in a local Microsoft Outlook installation. If Outlook is not installed or this directory is not configured for your users, then this directory is not available.

Exchange Server

This directory contains all entries from the Microsoft Exchange Server Global Address Book (if installed).

This checkbox creates a directory containing Microsoft Exchange Server Information in the optiClient 130.

Exchange Server Address:

IP address or host name of the Microsoft Exchange Server.

Lotus Notes Contacts

This directory contains all entries from the Contacts folder in your local Lotus Notes installation (if installed).

This checkbox creates a directory containing Lotus Notes contact information in the optiClient 130.

Lotus Notes Password:

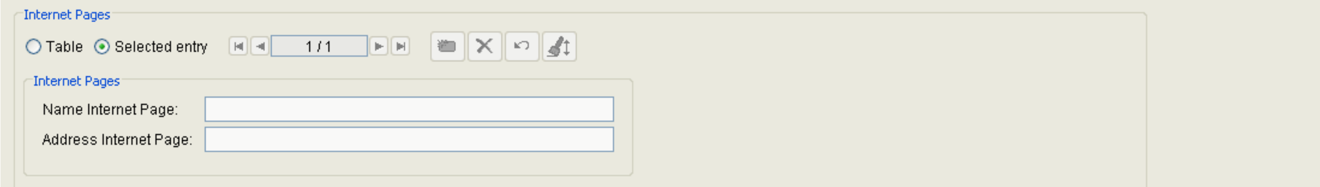
Password for accessing Lotus Notes.

Lotus Notes Dial Prefix:

This directory contains contact entries from your local Lotus Notes installation. If Lotus Notes is not installed or this directory is not configured for your users, then this directory is not available.

7.2.9.3 "Internet Pages" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Directories/Address Books > "Internet Pages" Tab



Name Internet Page:

Address Internet Page:

Name Internet Page:

Random name of the Internet page.

Address Internet Page:

URL of the Internet page.

7.2.10 Miscellaneous

Call: Main Menu > IP Devices > IP Client Configuration > Miscellaneous

This area features the following components:

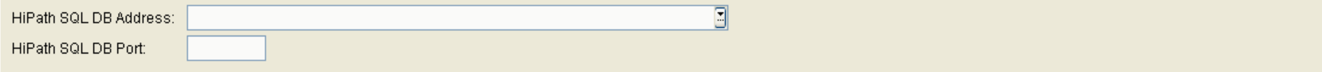
- General Data
- Possible Action Buttons
- "HiPath SQL DB" Tab
- "System Functions" Tab
- "SIP Features" Tab
- "SIP Features 2" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.10.1 "HiPath SQL DB" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Miscellaneous > "HiPath SQL DB" Tab



HiPath SQL DB Address:

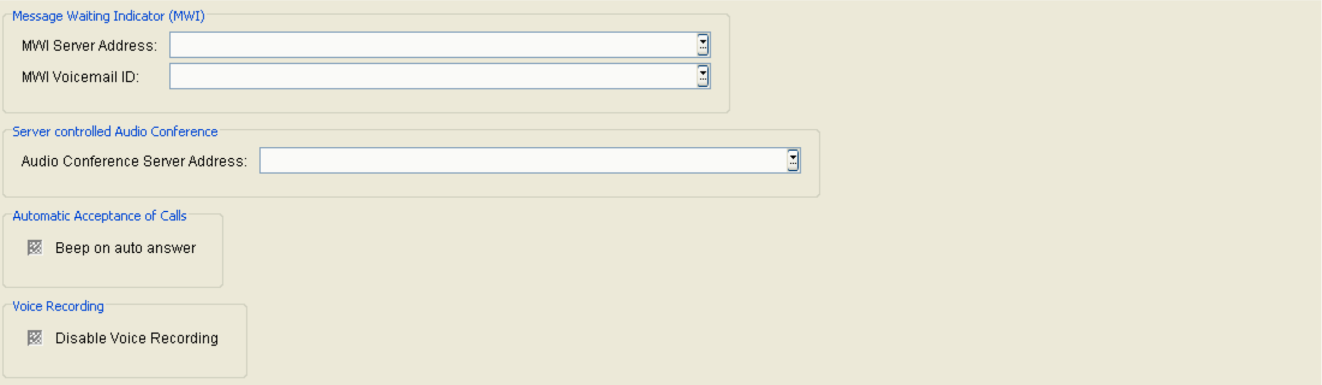
IP address or host name of the HiPath SQL DB.

HiPath SQL DB Port:

Port number for the HiPath SQL DB.

7.2.10.2 "System Functions" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Miscellaneous > "System Functions" Tab



Message Waiting Indicator (MWI)

MWI Server Address:

MWI Voicemail ID:

Server controlled Audio Conference

Audio Conference Server Address:

Automatic Acceptance of Calls

▨ Beep on auto answer

Voice Recording

▨ Disable Voice Recording

Message Waiting Indicator (MWI)

MWI Server Address:

IP address or host name of the MWI server.

MWI Voicemail ID:

Identification number for accessing the MWI server.

Server Controlled Audio Conference

Audio Conference Server Address:

IP address or host name for the audio conference server.

Automatic Acceptance of Calls

Beep on auto answer

Activates beep on auto answer.

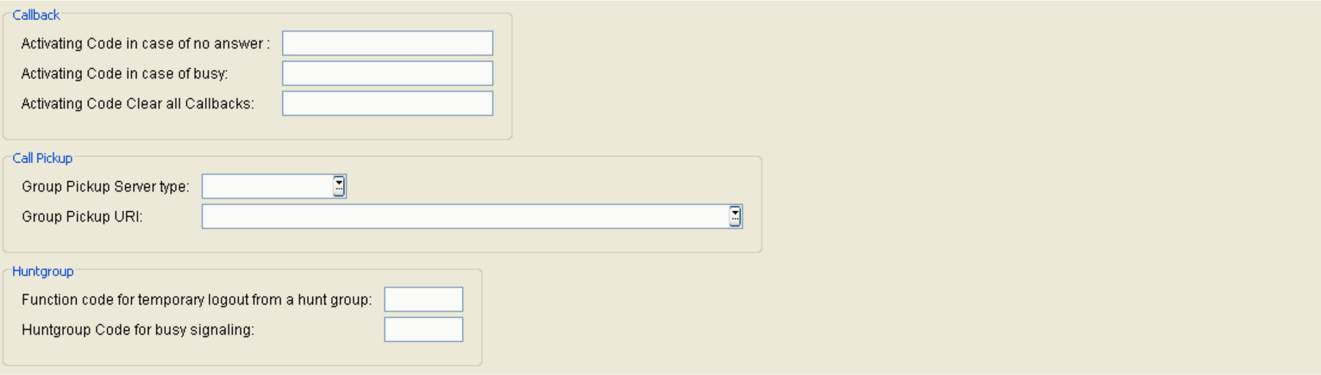
Voice Recording

Disable Voice Recording

Activates or deactivates voice recording.

7.2.10.3 "SIP Features" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Miscellaneous > "SIP Features" Tab



Callback

Activating Code in case of no answer :

Activating Code in case of busy:

Activating Code Clear all Callbacks:

Call Pickup

Group Pickup Server type:

Group Pickup URI:

Huntgroup

Function code for temporary logout from a hunt group:

Huntgroup Code for busy signaling:

Callback

Activating Code in case of no answer:

Code for controlling the "Callback-no reply" function on the server.

Activating Code in case of busy

Code for controlling the "Callback-busy" function on the server.

Activating Code Clear all Callbacks

Code that deletes all callback jobs on the server.

Call Pickup

Group Pickup Server type:

Possible options:

- **Other**
- **OpenScape Voice**
- **Broadsoft**
- **Sylantro**
- **HiQ8000**
- **Genesys**

Group Pickup URI:

IP address or host name of the server for providing the call pickup feature.

Huntgroup

Function Code for temporary logout from a hunt group

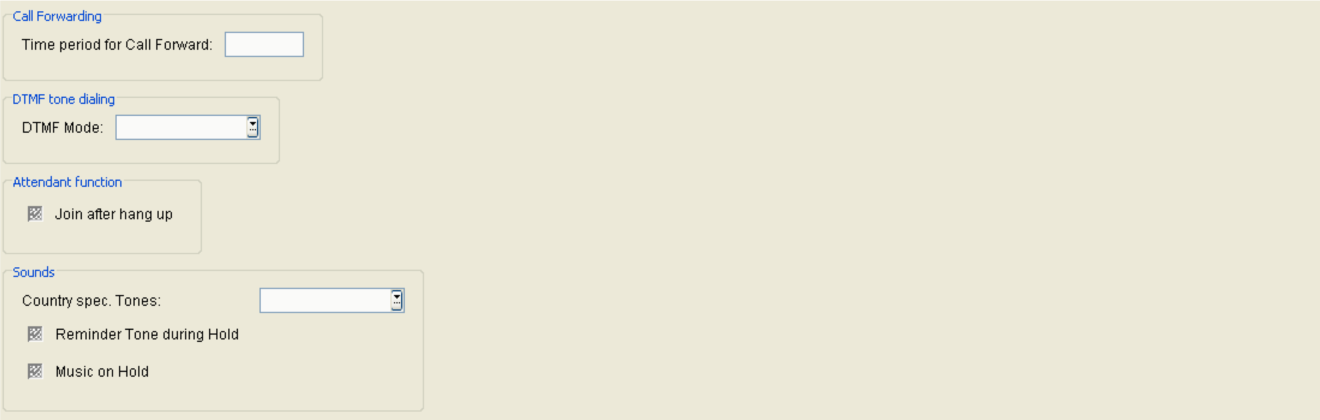
Huntgroup Code for "temporary logout".

Huntgroup Code for busy signaling

Function code for "busy signaling in a hunt group".

7.2.10.4 "SIP Features 2" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Miscellaneous > "SIP Features 2" Tab



Call Forwarding

Time period for Call Forward

Enter the time after which unanswered calls are forwarded when call forwarding is active.

DTMF tone dialing

DTMF Mode:

Possible options:

- **Automatic**
- **Inband**

Attendant Function

Join after hang up:

Activate this checkbox when you have two active connections (for example, during consultation hold) and then hang up. If the checkbox is active, the two connected parties are connected to each another; if the checkbox is not active, both connections are ended.

Sounds

Country spec. Tones:

Possible options:

- **Brazil**
- **China**
- **Germany**

- **France**
- **Great Britain**
- **International**
- **Italy**
- **Netherlands**
- **Portugal**
- **Spain**
- **USA**

Reminder Tone during Hold:

Activate this checkbox if you want a reminder tone to signal held calls.

Music on Hold:

Activate this checkbox if you want music on hold to be played in certain situations (for example, call forwarding, call hold, consultation).

7.2.11 Keysets/Keylayout

Call: Main Menu > IP Devices > IP Client Configuration > Keysets/Keylayout

This area features the following components:

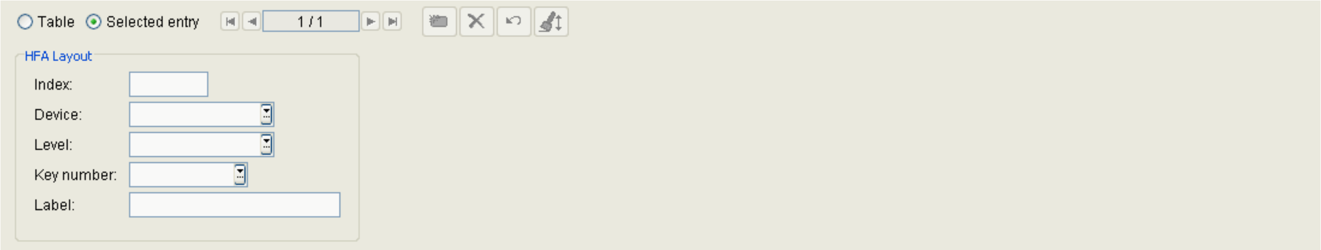
- General Data
- Possible Action Buttons
- "HFA Layout" Tab
- "HFA Layout (Standby)" Tab
- "SIP Keysets" Tab
- "SIP Line Keys" Tab
- "SIP Station Keys (DSS)" Tab
- "SIP Call Forwarding" Tab
- "SIP Keypad" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.11.1 "HFA Layout" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Keysets/Keylayout > "HFA Layout" Tab



Index

Name of the key layout function.

Device

Device selection for the programmed key.

Possible options:

- **1st Sidecar**
- **2nd Sidecar**
- **3rd Sidecar**
- **4th Sidecar**
- **Base Device**

Level

Level number of the programmed key.

Key number

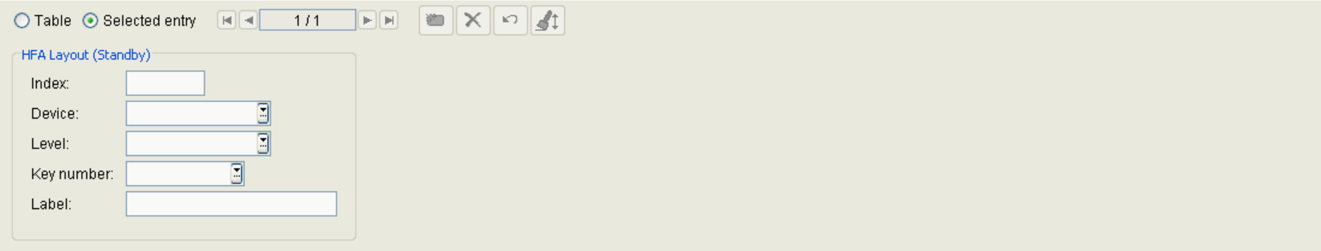
Key number of the programmed key.

Label

Label displayed for the programmed key.

7.2.11.2 "HFA Layout (Standby)" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Keysets/Keylayout > "HFA Layout (Standby)" Tab



HFA Layout (Standby)

Index:	
Device:	
Level:	
Key number:	
Label:	

Index

Name of the key layout function.

Device

Device selection of the programmed key.

Possible options:

- **1st Sidecar**
- **2nd Sidecar**
- **3rd Sidecar**
- **4th Sidecar**
- **Base Device**

Level

Level number of the programmed key.

Key number

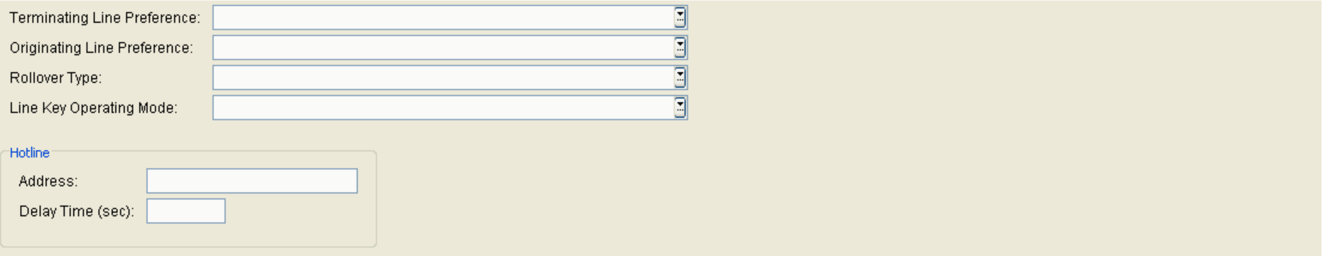
Key number of the programmed key.

Label

Label displayed for the programmed key.

7.2.11.3 "SIP Keysets" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Keysets/Keylayout > "SIP Keysets" Tab



Terminating Line Preference:

Originating Line Preference:

Rollover Type:

Line Key Operating Mode:

Address:

Delay Time (sec):

Terminating Line Preference:

Possible options:

- **Idle line preference**
- **Ringing line preference**

Originating Line Preference:

Possible options:

- **Idle line preference**
- **Primary line preference**

Rollover Type:

Type of alerting to be used in the case that, during an active call, an incoming call arrives on a different line.

Possible options:

- **No tone**
- **Normal beep**
- **Special beep**

Line Key Operating Mode:

Defines what should happen to a line (call) when a connection is established over another line.

Possible options:

- **Hold first call**
- **Clear first call**

Hot Line

Address

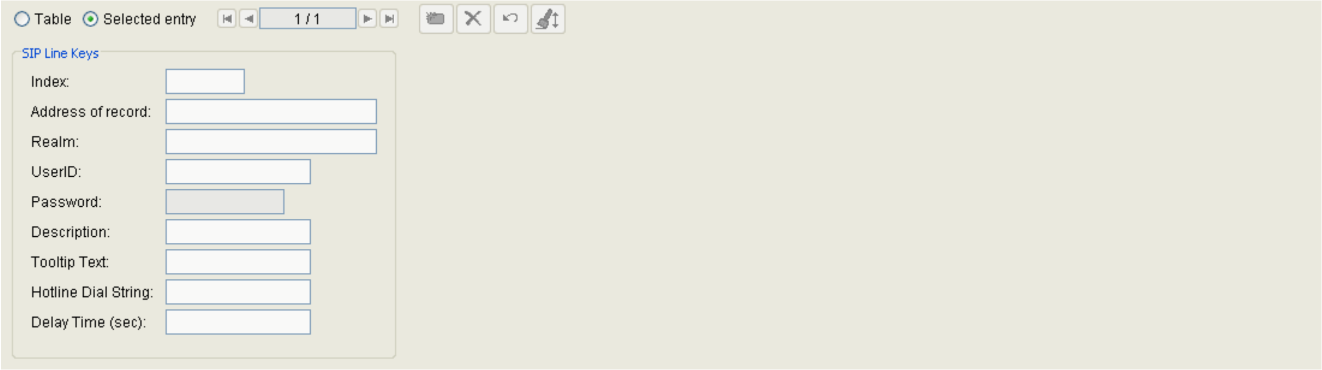
Address resp. call number which is dialed after the line has been activated (e. g. by going off-hook) and the delay time has expired.

Delay Time (sec)

Dialing delay in seconds. If delay time = 0, the connection is established immediately.

7.2.11.4 "SIP Line Keys" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Keysets/Keylayout > "SIP Line Keys" Tab



Index:

Line key number

Address of record:

Phone number for the line belonging to this line key.

Realm:

SIP realm for the line’s address of record

UserID:

SIP user name of the line’s address of record

Password:

Password for the SIP user name.

Description:

Description of the line.

Tooltip Text:

Text that appears in the ToolTip for the line.

Hotline Dial String:

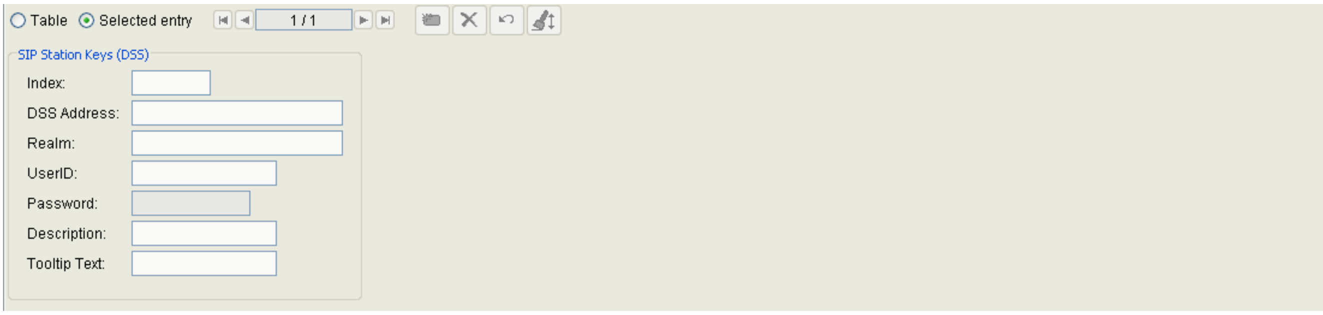
Number called if the line is configured as the hotline.

Delay Time (sec):

Delay between line seizure (for example, by lifting the handset) and hotline number dialing.

7.2.11.5 "SIP Station Keys (DSS)" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Keysets/Keylayout > "SIP Station Keys (DSS)" Tab



Index

Index number of the key function.

DSS Address

Phone number of the DSS (Direct Station Select) line.

Realm

SIP realm of the DSS line.

UserID

SIP user name of the DSS line's address of record.

Password

Password for the SIP user name.

Description

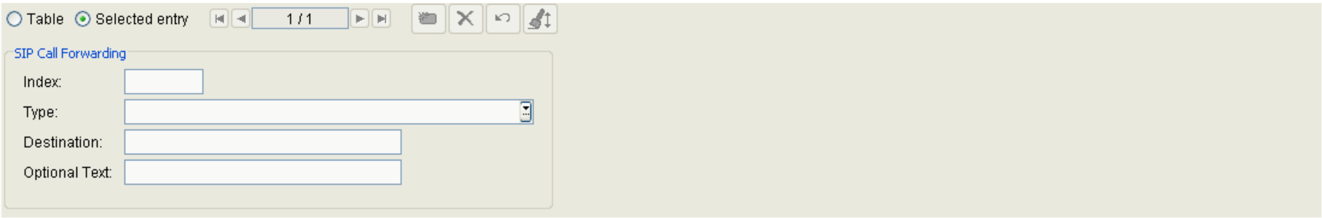
Description of the DSS line.

Tooltip Text

Text entry that appears in the ToolTip for the DSS line key.

7.2.11.6 "SIP Call Forwarding" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Keysets/Keylayout > "SIP Call Forwarding" Tab



Index

Index number of the call forwarding key.

Type

Selection of conditions, under which call forwarding is executed.

- **All calls**
- **External calls (HiPath 3000)**
- **Internal calls (HiPath 3000)**
- **on busy (SIP, HiPath 4000)**
- **on no answer (SIP, HiPath 4000)**
- **on busy / no answer (HiPath 4000)**
- **on logout (HiPath 3000, HiPath 4000)**

Destination

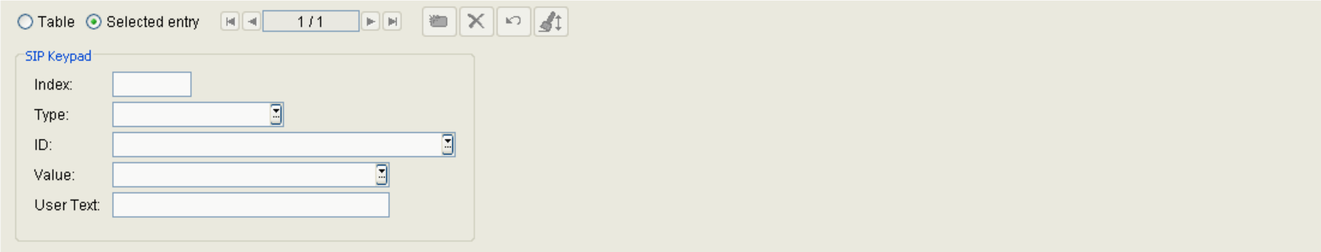
Destination of SIP call forwarding.

Optional Text

Description of the type of SIP call forwarding configured here.

7.2.11.7 "SIP Keypad" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Keysets/Keylayout > "SIP Keypad" Tab



Index

Index number of the key function.

Type

Type of SIP keypad.

ID

SIP keypad ID.

Value

Value of the key.

User Text

Descriptive label for the SIP keypad.

7.2.12 Signaling and Payload Encryption (SPE)

Call: Main Menu > IP Devices > IP Client Configuration > Signaling and Payload Encryption (SPE)

This area features the following components:

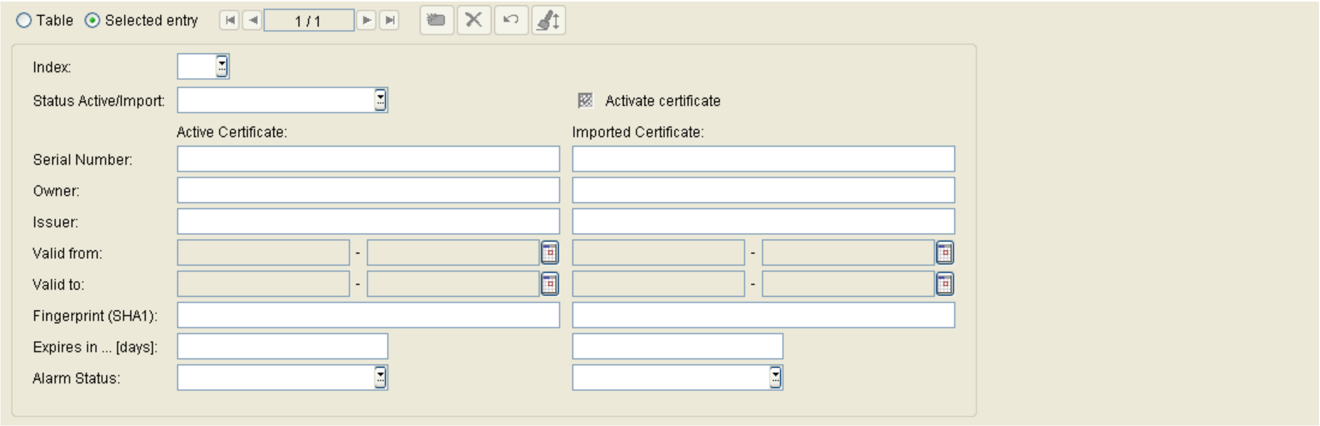
- General Data
- Possible Action Buttons
- "SPE CA Certificates" Tab
- "SIP Settings" Tab
- "HFA Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.12.1 "SPE CA Certificates" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Signaling and Payload Encryption (SPE) > "SPE CA Certificates" Tab



The parameters described below are available once for the currently active certificate and once for the imported certificate.

Index

Index number for the certificate.

Status Active/Import:

Specifies whether a certificate is registered as imported and/or active on the phone. The five statuses listed below are possible.

Possible values:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA 1):

This is the fingerprint extracted from the certificate.

Expires in ... [days]:

Number of days before the certificate expires.

> ⓘ The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Displays the duration of validity for certificates when searching for certificates due to expire.

Possible values:

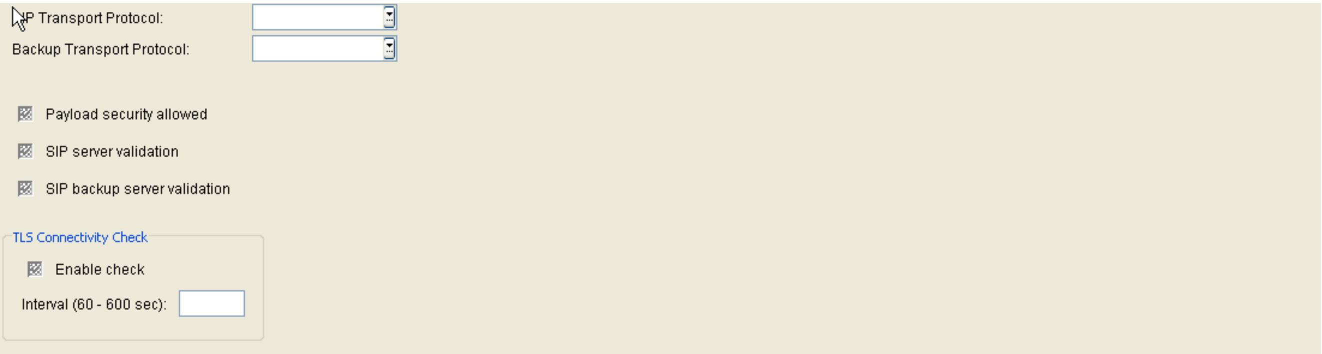
- **valid**
- **soon running out**
- **expired**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted. The active certificate is used to encrypt calls.

7.2.12.2 "SIP Settings" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Signaling and Payload Encryption (SPE) > "SIP Settings" Tab



SIP Transport Protocol:

Backup Transport Protocol:

▨ Payload security allowed

▨ SIP server validation

▨ SIP backup server validation

TLS Connectivity Check

▨ Enable check

Interval (60 - 600 sec):

SIP Transport Protocol:

Transport protocol used for SIP signaling.

Possible options:

- **UDP**
- **TCP**
- **TLS**

Backup Transport Protocol:

Transport protocol used for SIP signaling when the backup SIP server is in use.

Possible options:

- **UDP**
- **TCP**

Payload security allowed

If this checkbox is activated, encryption of voice messages is enabled.

SIP server validation

If this checkbox is activated, the connection to the SIP server is verified.

SIP backup server validation

If this checkbox is activated, the connection to the backup SIP server is verified.

TLS Connectivity Check

Enable check

If checkbox is activated, the TLS connectivity check will be enabled.

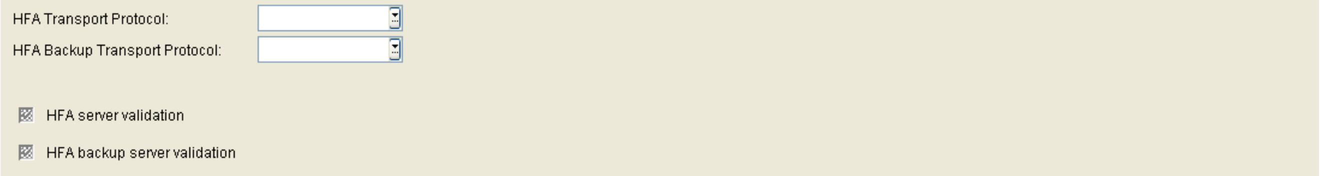
Interval

Time interval in seconds in which the TLS connectivity is checked periodically.

Possible options: **60** - **600**

7.2.12.3 "HFA Settings" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Signaling and Payload Encryption (SPE) > "HFA Settings" Tab



HFA Transport Protocol:

HFA Backup Transport Protocol:

▨ HFA server validation

▨ HFA backup server validation

HFA Transport Protocol:

Transport protocol used for HFA signaling.

Possible options:

- **UDP**
- **TCP**
- **TLS**

HFA Backup Transport Protocol:

Transport protocol used for HFA signaling when the backup HFA server is in use.

Possible options:

- **UDP**
- **TCP**
- **TLS**

HFA server validation

If this checkbox is activated, the connection to the HFA server is verified.

HFA backup server validation

If this checkbox is activated, the connection to the HFA backup server is verified.

7.2.13 VoIP Security V1

This area features the following components:

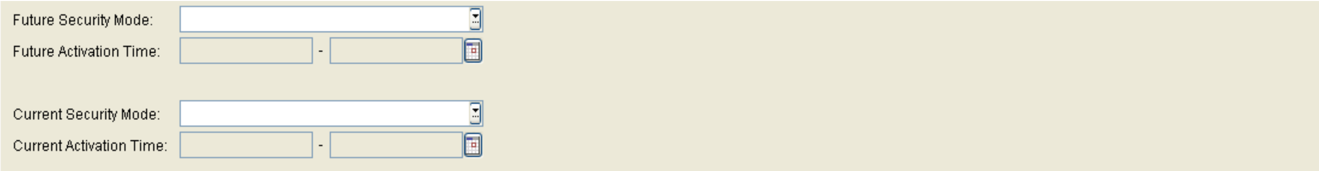
- General Data
- Possible Action Buttons
- "HFA Key Distribution" Tab

7.2.13.1 "HFA Key Distribution" Tab

Call: Main Menu > IP Devices > IP Client Configuration > VoIP Security V1 > "HFA Key Distribution" Tab

In this interface, only the particular status is indicated. The administration of the security mode is done in the Key Distribution ares, see Section 11.1, "Key Distribution".

In Section 16.11.3, "Changing Security Mode", you can find further advice on enabling and disabling the security mode.



Future Security Mode:

Future Activation Time: -

Current Security Mode:

Current Activation Time: -

Future Security Mode:

Mode of the future encryption (read-only).

Possible values:

- **Encryption on**
- **Encryption aus**

Future Activation Time:

Time of the future activation (read-only).

For the selection of a timespan for searching, see Section 5.4.2.4, "Time field with calendar button".

Current Security Mode:

Mode of the current encryption (read-only).

Possible values:

- **Encryption on**
- **Encryption aus**

Current Activation Time:

Time of the current activation (read-only).

For the selection of a timespan for searching, see Section 5.4.2.4, "Time field with calendar button".

In Section 16.11.3, "Changing Security Mode", you can find further advice on enabling and disabling the security mode.

7.2.14 Dialup Site

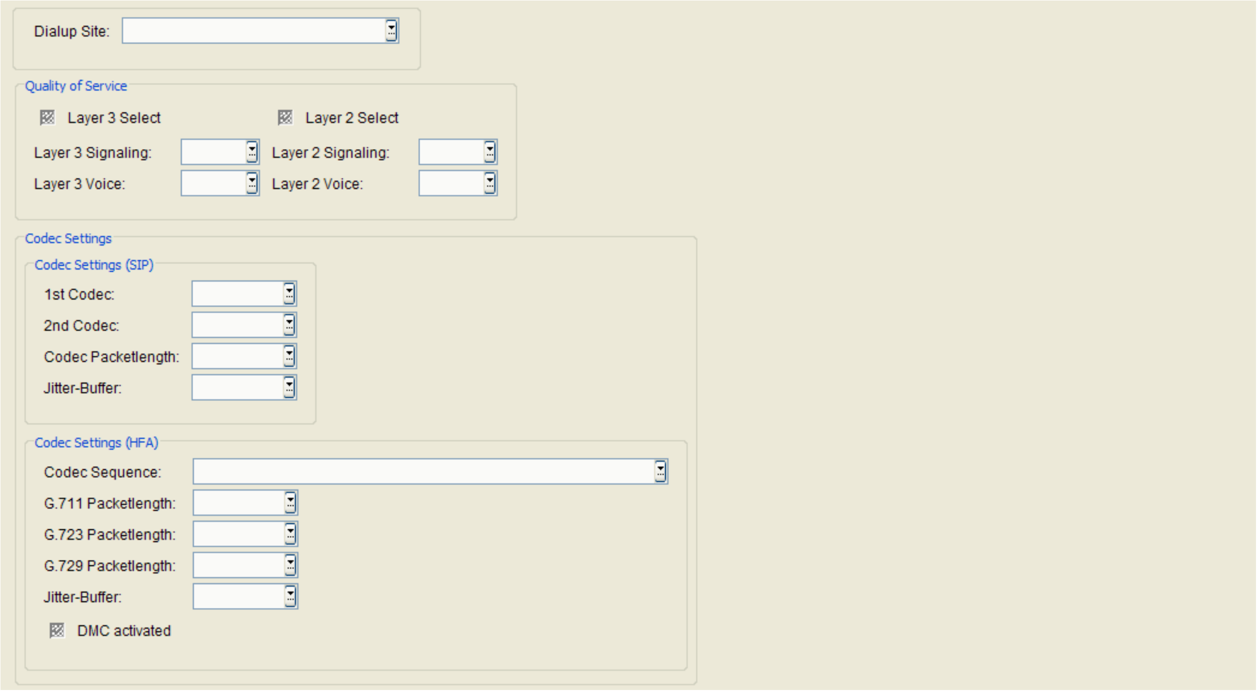
Call: Main Menu > IP Devices > IP Client Configuration > Dialup Site

This area features the following components:

- General Data
- Possible Action Buttons
- "Dialup Site Parameters" Tab

7.2.14.1 "Dialup Site Parameters" Tab

Call: Main Menu > IP Devices > IP Client Configuration > Dialup Site > "Dialup Site Parameters" Tab



Dialup Site

Address of the dialup site.

Quality of Service

Layer 3 Select

Checkbox for activating the QoS configuration on layer 3.

Layer 3 Signaling:

Class of service value for call signaling on layer 3.

Possible options:

- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**

- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CS7**
- **Default**

Layer 3 Voice:

Class of service value for voice on layer 3.

Possible options:

- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CS7**
- **Default**

Layer 2 Select

Checkbox for activating the QoS layer 2 configuration.

Layer 2 Signaling:

Class of Service value for call signaling on layer 2.

Value range: **0** ... **7**

Layer 2 Voice:

Class of Service value for voice on layer 2.

Value range: **0** ... **7**

Codec Settings

Codec Settings (SIP)

1st Codec:

First compression method.

Possible options:

- **G.711**
- **G.729**

2nd Codec:

Second compression method.

Possible options:

- **G.711**
- **G.729**
- **None**

Codec Packetlength:

Possible options:

- **Automatic**
- **10**
- **20**

Jitter-Buffer (ms):

Caching duration:

Possible options (in ms):

Value range: **20** ... **190** milliseconds.

Codec Settings (HFA)

Codec Sequence:

Possible options:

- **not compressing Codecs preferred, besides G.723 preferred**
- **not compressing Codecs preferred, besides G.729 preferred**
- **compressing Codecs preferred, G.723 preferred**
- **compressing Codecs preferred, G.729 preferred**
- **only compressing Codecs, G.723 preferred**

- **only compressing Codecs, G.729 preferred**

G.711 Packetlength:

Possible options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

G.723 Packetlength:

Possible options:

- **30**
- **60**

G.729 Packetlength:

Possible options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

Jitter-Buffer (ms):

Cache size.

Possible options (in ms):

Value range: **20** ... **190** milliseconds.

DMC activated

Checkbox for activating DMC bandwidth.

7.2.15 OpenScape

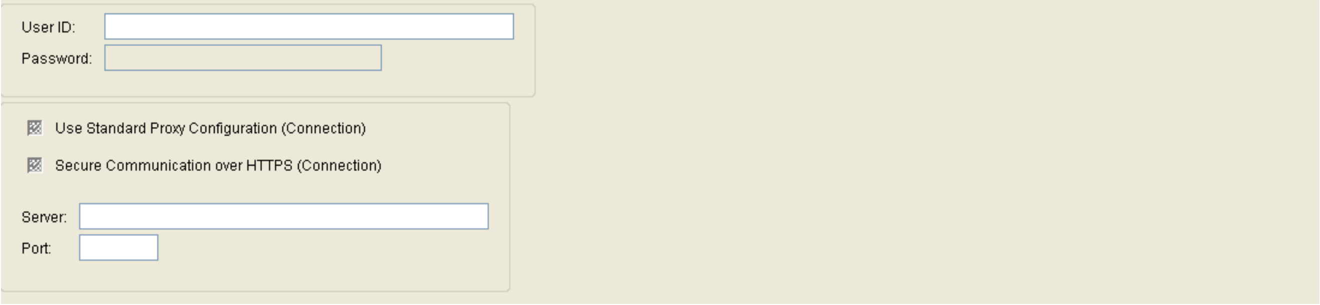
Call: Main Menu > IP Devices > IP Client Configuration > OpenScape

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "Connection" Tab
- "Instant Messaging (XMP)" Tab
- "WEB Access" Tab

7.2.15.1 "Connection" Tab

Call: Main Menu > IP Devices > IP Client Configuration > OpenScape > "Connection" Tab



User ID:

Password:

☒ Use Standard Proxy Configuration (Connection)

☒ Secure Communication over HTTPS (Connection)

Server:

Port:

User ID:

User ID for accessing the OpenScape Connection Server.

Password:

Password for accessing the OpenScape Connection Server.

Use Standard Proxy Configuration:

If this checkbox is activated, the standard proxy is used.

Secure Communication over HTTPS:

If this checkbox is activated, HTTPS is used for secure communication.

Server:

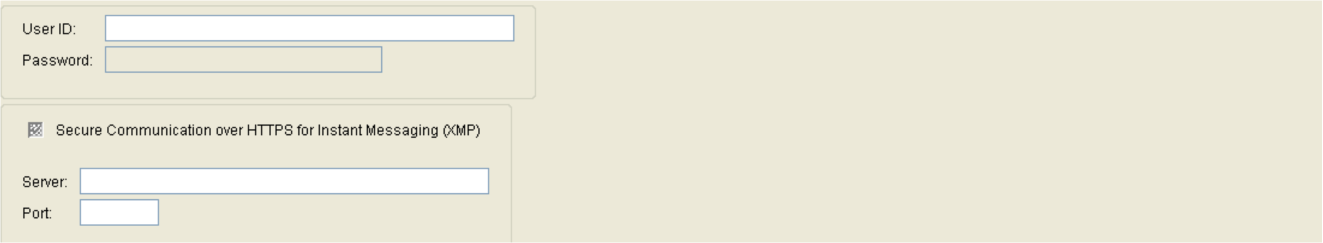
Address of the OpenScape Connection Server.

Port:

Port number of the OpenScape Connection Server.

7.2.15.2 "Instant Messaging (XMP)" Tab

Call: Main Menu > IP Devices > IP Client Configuration > OpenScape > "Instant Messaging (XMP)" Tab



User ID:

Password:

☒ Secure Communication over HTTPS for Instant Messaging (XMP)

Server:

Port:

User ID:

User ID for access to the OpenScape Instant Messaging (XMP) server.

Passwort:

Password for access to the OpenScape Instant Messaging (XMP) server.

Secure Communication over HTTPS for Instant Messaging (XMP)

Checkbox for activating secure communication over HTTPS.

Server:

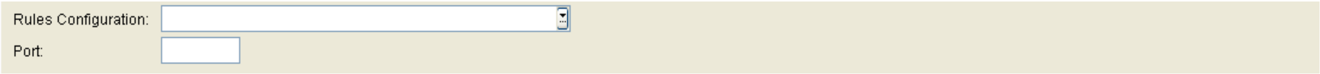
Address of the server for OpenScape Instant Messaging (XMP).

Port:

Port number of the server for OpenScape Instant Messaging (XMP).

7.2.15.3 "WEB Access" Tab

Call: Main Menu > IP Devices > IP Client Configuration > OpenScape > "WEB Access" Tab



Rules Configuration:

Port:

Rules Configuration:

Rules Configuration for access to WEB server.

Port:

Port number for access to the WEB server.

7.3 IP Gateway Configuration

This menu item consists of the following areas:

- QoS Data Collection
- Security Settings
- Signaling and Payload Encryption (SPE)
- IPSec/VPN

7.3.1 QoS Data Collection

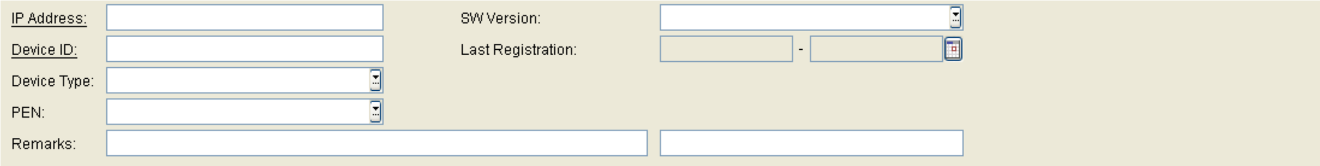
This area features the following components:

- General Data
- Possible Action Buttons
- "Server Data" Tab
- "Report Settings" Tab
- "Threshold Values" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

Call: Main Menu > IP Devices > IP Gateway Configuration > QoS Data Collection > General Data



This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP gateways. The base data associated with the IP gateways found is displayed in **Object** view.

The value displayed in the **Remarks** fields can be changed (all other fields are read-only).

IP Address:

IP address of the IP gateway.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID

ID that uniquely identifies this IP gateway.

Device Type:

IP gateway device type.

You can view all IP devices supported by the DLS in Section 3.4, "Area of Application".

Example: **HG3500**

PEN:

Position of the gateway assembly group (plug-in position).

SW Version:

Software version of the IP gateway.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

Last Registration:

Last time the IP gateway logged on to the DLS.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP gateways that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Get

Loads a template that has already been saved. For more information, see Section 15.4, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.4, "Editing Templates".

Discard

Discards any changes made and new entries.

Read

The parameters displayed on the new mask are read in again by the IP device.

Rename

Changes the name of a saved template. For more information, see Section 15.4, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.4, "Editing Templates".

Import Certificate

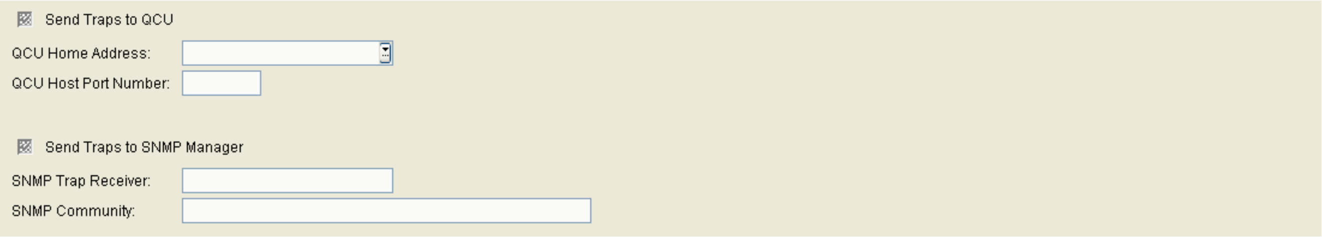
Imports a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.12, "Security: Administering Certificates".

Remove Certificate

Deletes a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.12, "Security: Administering Certificates".

7.3.1.1 "Server Data" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > QoS Data Collection > "Server Data" Tab



☒ Send Traps to QCU

QCU Home Address:

QCU Host Port Number:

☒ Send Traps to SNMP Manager

SNMP Trap Receiver:

SNMP Community:

Send Traps to QCU

If this checkbox is activated, messages are sent to QCU in the event of errors.

QCU Home Address:

IP address or host name of the server that collects the QDC data.

QCU Host Port Number:

Port number for the server that collects the QDC data.

Send Traps to SNMP Manager

If this checkbox is activated, messages are sent to SNMP Manager in the event of errors.

SNMP Community:

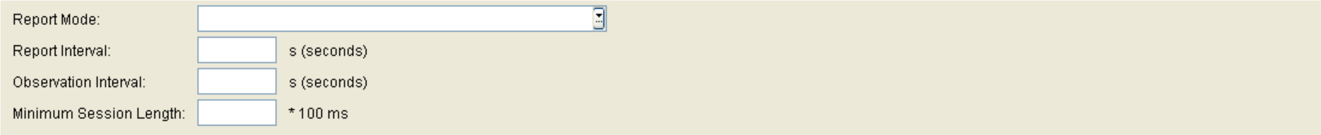
Community string used for authorization on the SNMP server.

SNMP Trap Receiver:

IP address of SNMP Manager.

7.3.1.2 "Report Settings" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > QoS Data Collection > "Report Settings" Tab



Report Mode:

Specifies when a report should be generated.

Possible options:

- **EOS Threshold exceeded**
  At the end of the connection that exceeded the threshold.
- **EOR Threshold exceeded**
  At the end of the reporting interval that exceeded the threshold.
- **EOS (End of Session)**
  At the end of the connection.
- **EOR (End or Report Interval)**
  At the end of the reporting interval.

Report Interval:

Time interval in which a QoS report is sent.

Value range: **0** ... **3600** seconds.

Observation Interval:

Time interval in which threshold violation is checked.

Value range: **0** ... **5000** seconds.

Minimum Session Length:

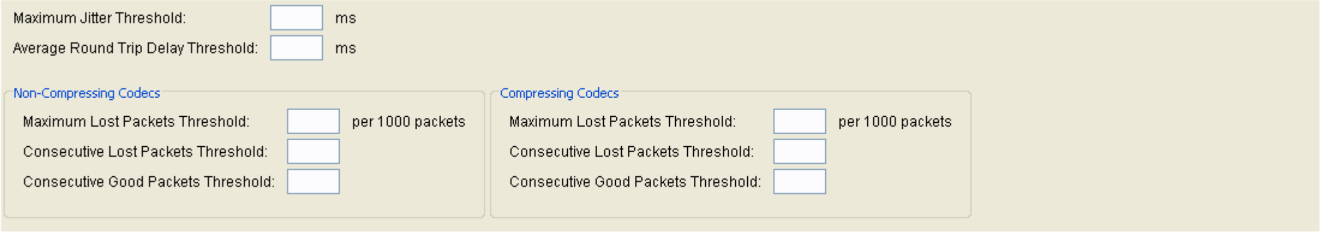
A QoS report is not sent if a session (for example, a call) undershoots this minimum.

Value range: **0** ... **5000** (x 100 ms).

7.3.1.3 "Threshold Values" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > QoS Data Collection > "Threshold Values" Tab

The threshold values that produce a QoS report if exceeded are entered here.



Maximum Jitter Threshold: ms
Average Round Trip Delay Threshold: ms

Non-Compressing Codecs
Maximum Lost Packets Threshold: per 1000 packets
Consecutive Lost Packets Threshold:
Consecutive Good Packets Threshold:

Compressing Codecs
Maximum Lost Packets Threshold: per 1000 packets
Consecutive Lost Packets Threshold:
Consecutive Good Packets Threshold:

Maximum Jitter Threshold:

Maximum threshold in milliseconds for runtime fluctuations during data transmission.

Value range: **0** ... **255**

Default: **15**

Average Round Trip Delay Threshold:

Average response time in milliseconds for signal transmission. A report is issued if this is exceeded.

Default: **100**

Non-Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during uncompressed transmission. The number is specified in 1000-packet increments.

Value range: **0** ... **255**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during uncompressed transmission.

Value range: **0** ... **255**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during uncompressed transmission.

Value range: **0** ... **255**

Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during compressed transmission.

Value range: **0** ... **255**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during compressed transmission.

Value range: **0** ... **255**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during compressed transmission.

Value range: **0** ... **255**

7.3.2 Security Settings

This area features the following components:

- General Data
- Possible Action Buttons
- "Settings" Tab
- "WBM Server Certificates" Tab

7.3.2.1 "Settings" Tab

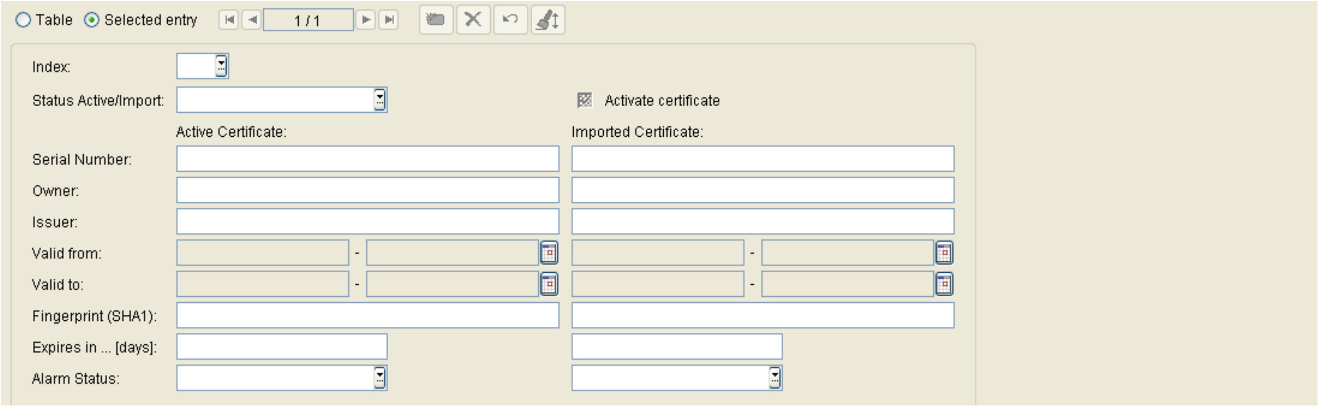
Call: Main Menu > IP Devices > IP Gateway Configuration > Security Settings > "Settings" Tab

No additional data are required for IPSec/VPN Settings

No additional security settings are currently required.

7.3.2.2 "WBM Server Certificates" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > Security Settings > "WBM Server Certificates" Tab



Index

Indec number for the certificate.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm SHA1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".

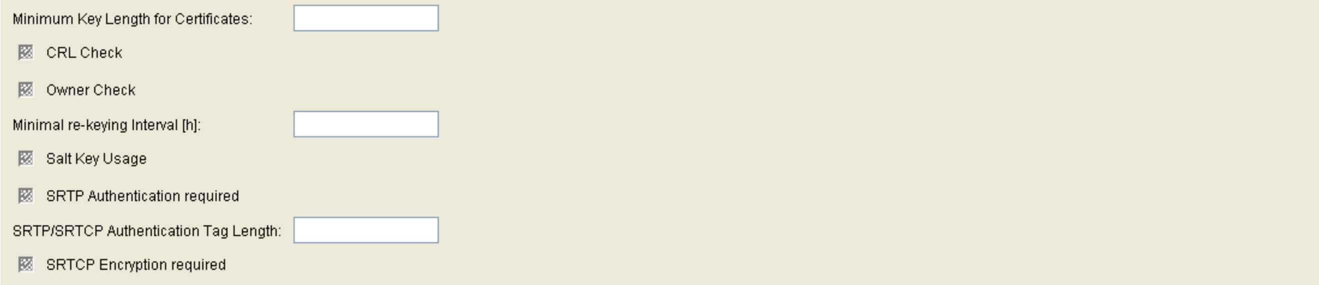
7.3.3 Signaling and Payload Encryption (SPE)

This area features the following components:

- General Data
- Possible Action Buttons
- "Settings" Tab
- "SPE Certificate" Tab
- "SPE CA Certificates" Tab
- "CRL Distribution Points" Tab

7.3.3.1 "Settings" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > Signaling and Payload Encryption (SPE) > "Settings" Tab



Minimum Key Length for Certificates:

▨ CRL Check

▨ Owner Check

Minimal re-keying Interval [h]:

▨ Salt Key Usage

▨ SRTP Authentication required

SRTP/SRTCP Authentication Tag Length:

▨ SRTCP Encryption required

Minimum Key Length for Certificates

Minimum key length for certificates.

CRL Check

If this checkbox is activated, the Certificate Revocation List (CRL) in which invalid certificates can be entered is verified.

Owner Check

If this checkbox is activated, the owner’s name is verified (Subjectname check).

Maximum re-keying Interval

Maximum re-keying interval in hours.

Salt Key Usage

If this checkbox is activated, salt key usage is necessary.

SRTP Authentication required

If this checkbox is activated, secure RTP authentication is necessary.

SRTP/SRTCP Authentication Tag Length

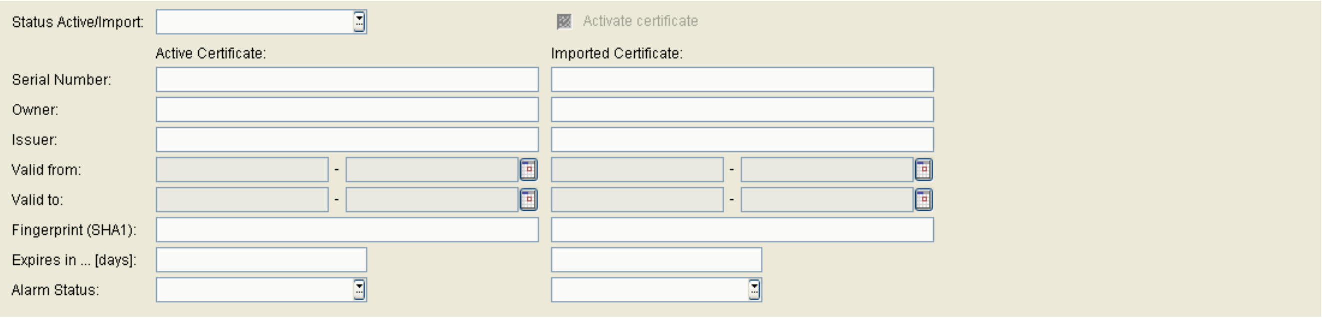
Length of the authentication key.

SRTCP Encryption required

If this checkbox is activated, SRTCP encryption is necessary.

7.3.3.2 "SPE Certificate" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > Signaling and Payload Encryption (SPE) > "SPE Certificate" Tab



Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm SHA1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

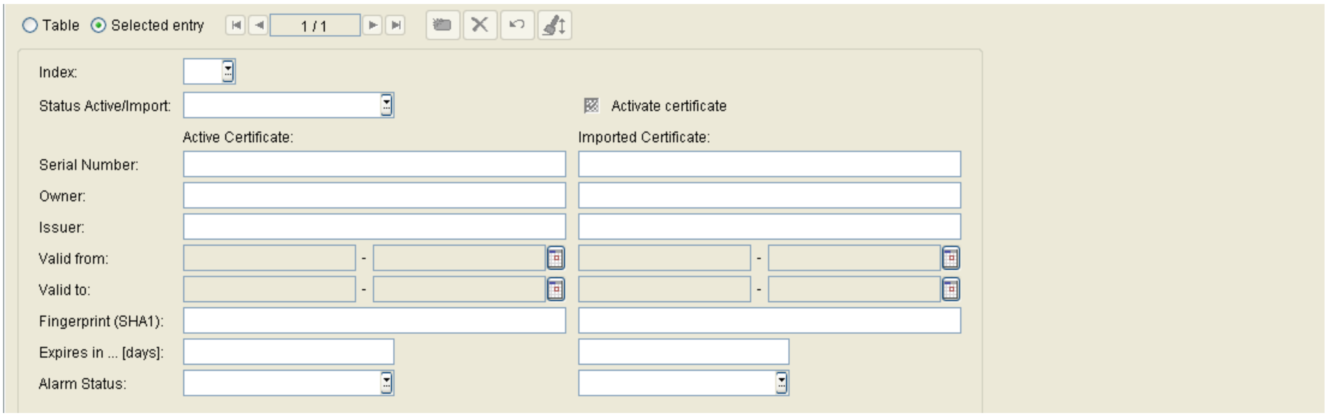
Possible values:

- **valid**
- **soon running out**
- **expired**

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".

7.3.3.3 "SPE CA Certificates" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > Signaling and Payload Encryption (SPE) > "SPE CA Certificates" Tab



Index

Index for identifying the SPE CA certificates.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm SHA1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

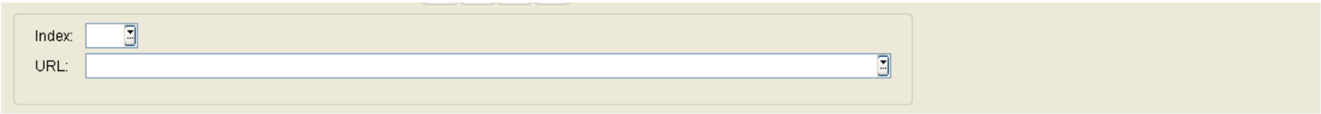
Possible values:

- **valid**
- **soon running out**
- **expired**

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".

7.3.3.4 "CRL Distribution Points" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > Signaling and Payload Encryption (SPE) > "CRL Distribution Points" Tab



Index

Index for identifying the CRL distribution points.

URL

URL of the CRL distribution point, for example, http://.... or ldap://...

7.3.4 IPSec/VPN

This area features the following components:

- General Data
- Possible Action Buttons
- "Settings" Tab
- "Peer Credentials" Tab
- "CA Certificates" Tab
- "CRL Files" Tab

7.3.4.1 "Settings" Tab

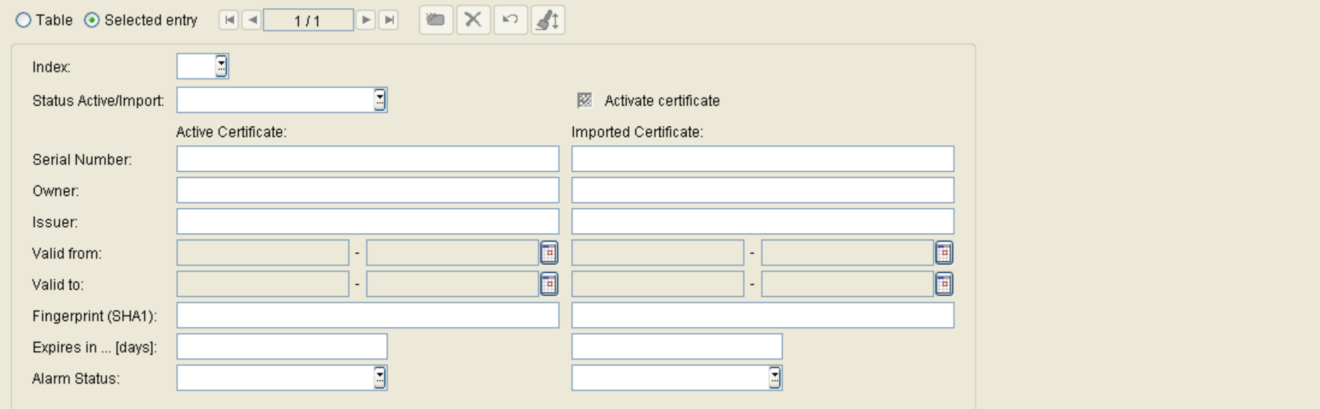
Call: Main Menu > IP Devices > IP Gateway Configuration > IPSec/VPN > "Settings" Tab

No additional data are required for IPSec/VPN Settings

No additional IPSec/VPN settings are currently required.

7.3.4.2 "Peer Credentials" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > IPSec/VPN > "Peer Credentials" Tab



Index

Index number for the certificate.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm SHA1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

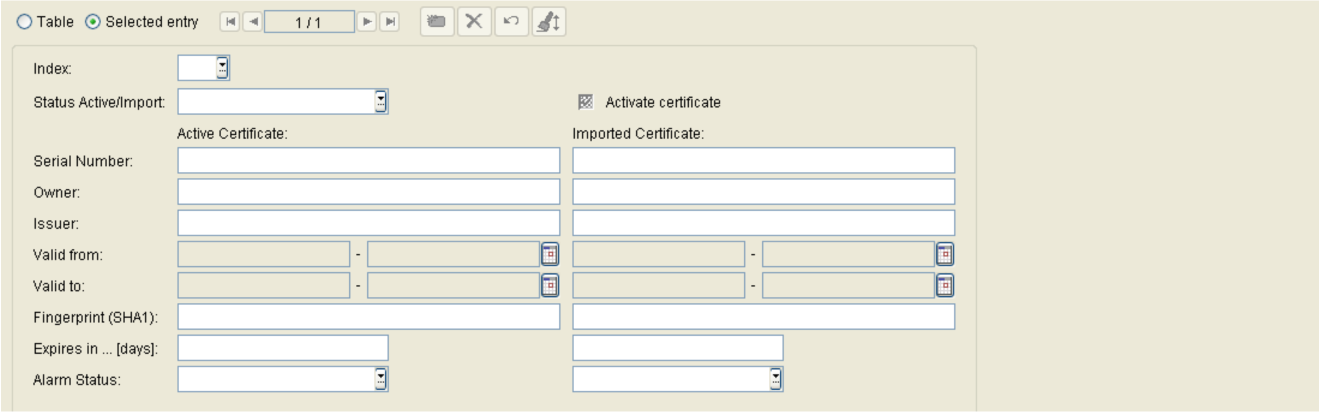
Possible values:

- **valid**
- **soon running out**
- **expired**

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".

7.3.4.3 "CA Certificates" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > IPSec/VPN > "CA Certificates" Tab



Index

Index for identifying the CA certificates.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA1):

Test algorithm SHA1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

> The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

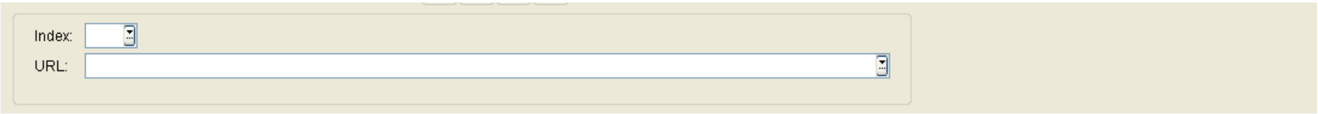
Possible values:

- **valid**
- **soon running out**
- **expired**

> For further information on importing and activating certificates, see Section 16.12, "Security: Administering Certificates".

7.3.4.4 "CRL Files" Tab

Call: Main Menu > IP Devices > IP Gateway Configuration > IPSec/VPN > "CRL Files" Tab



Index

Index for identifying the CRL files.

CRL Files

Directory path for CRL files.

7.4 IP Device Interaction

You can use the **IP Device Interaction** area to transfer data from the IP Device to the DLS and to activate a restart at the IP Devices.

Call: Main Menu > IP Devices > IP Device Interaction

This menu consists of the following submenus:

- Read IP Device Data
- Reset IP Devices
- Ping IP Devices
- Scan IP Devices

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.4.1 Read IP Device Data

Call: Main Menu > IP Devices > IP Device Interaction > Read IP Device Data

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

You can use this function to read out information from the IP Device. Only registered IP Devices will be considered.

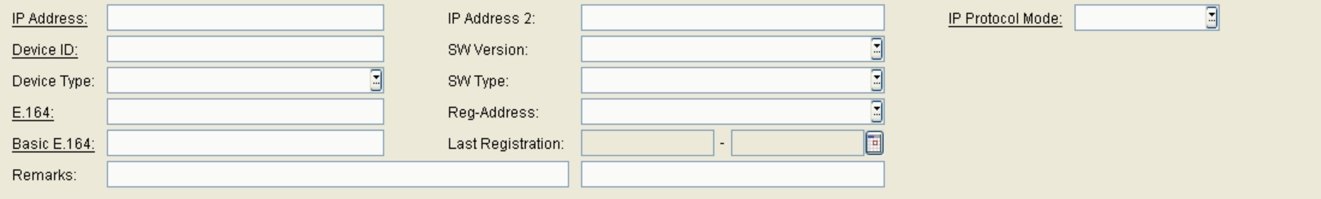
In this case, the data is synchronized between the IP Device and DLS database. The data is read without IP Devices being reset (see Section 7.4.2, "Reset IP Devices"). In other words, no further actions or interventions are performed at the workpoint.

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is identical for the **Read IP Device Data** and **Reset IP Devices** interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP Devices. The base data associated with the IP Devices found is displayed in the **Object** view (no changes possible).



IP Address:		IP Address 2:		IP Protocol Mode:	
Device ID:		SW Version:			
Device Type:		SW Type:			
E.164:		Reg-Address:			
Basic E.164:		Last Registration:	-		
Remarks:					

> You can use the following wildcards in all text and selection list fields in **Search** view:
> - * (asterisk): Stands for any sequence of characters.
> - ? (question mark): Stands for exactly one character.
> - ^ (circumflex): Stands for an empty field.
>
> Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.
>
> All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only those IP Devices that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of the IP Device. For OpenStage, in IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

Workpoint device type.

All workpoint device types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Examples: **optiPoint 410 standard**, **optiClient 130**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version used by the IP Device.

Example for IP phones and IP clients: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

SW Type:

Software type used by the IP Device.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**

Reg-Address:

IP address of the gateway or the gatekeeper where the IP Device must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Remarks:

Fields for general informations.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP Device that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Reset IP Device

Restarts/resets the device.

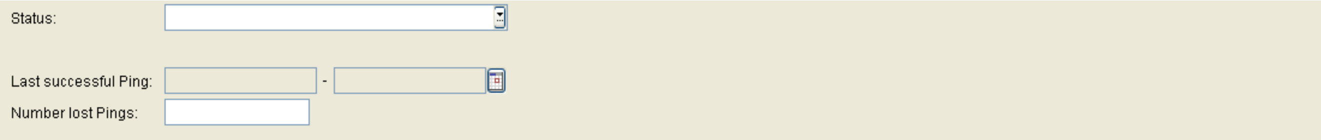
Restore Factory Setting

Restarts/resets the device and restores factory settings. When you press this button, you will be asked to enter the reset password.

Available for OpenStage, optiPoint410, and optiPoint420.

7.4.1.1 "Info" Tab

Call: Main Menu > IP Devices > IP Device Interaction > Read IP Device Data > "Info" Tab



Status:

Possible options:

- **in Service**
  IP phone that is currently in service.
- **license expired**
  IP phone with an expired license.
- **invalid license token**
  Unlicensed IP phone.
- **invalid SW signature**
  IP phone with an invalid software signature.

Last successful Ping

Displays the last successful PING.

The value is read-only.

See also Section 7.4.3, "Ping IP Devices".

Number lost Pings

Total number of unsuccessful PINGs.

The value is read-only.

See also Section 7.4.3, "Ping IP Devices".

7.4.2 Reset IP Devices

Call: Main Menu > IP Devices > IP Device Interaction > Reset IP Devices

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

You can perform a reboot and a factory reset.

For information on general interface operation, see Section 5.4.2, "Work Area".

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Reset IP Device

Restarts/resets the device.

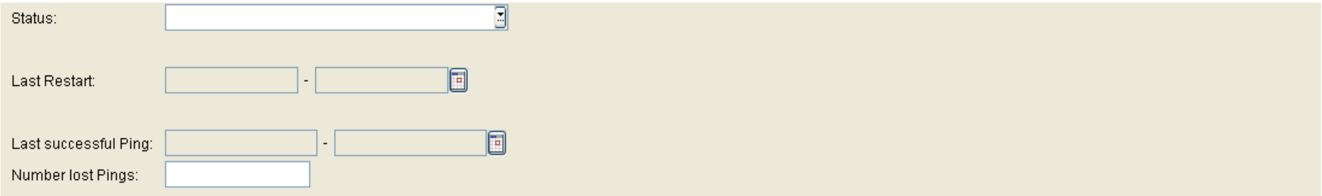
Restore Factory Setting

Restarts/resets the device and restores factory settings. When you press this button, you will be asked to enter the reset password.

Available for OpenStage, optiPoint410, and optiPoint420.

7.4.2.1 "Info" Tab

Call: Main Menu > IP Devices > IP Device Interaction > Reset IP Devices > "Info" Tab



Status:

IP phone status.

Possible options:

- **in Service**
  IP phone that is currently in service.
- **license expired**
  IP phone with an expired license.
- **invalid license token**
  Unlicensed IP phone.
- **invalid SW signature**
  IP phone with an invalid software signature.

Last Restart:

Displays date/time of last restart.

Last successful Ping

Displays the last successful PING.

The value is read-only.

See also Section 7.4.3, "Ping IP Devices".

Number lost Pings

Total number of unsuccessful PINGs.

The value is read-only.

See also Section 7.4.3, "Ping IP Devices".

7.4.3 Ping IP Devices

Call: Main Menu > IP Devices > IP Device Interaction > Ping IP Devices

This area features the following components:

- General Data
- Possible Action Buttons
- "IP Phones" Tab
- "IP Clients" Tab
- "IP Gateways" Tab

This function enables you to use PINGs to check IP Device response, in other words , to check if they are still contactable.

The following DLS areas contain information on successful or unsuccessful pings:

- IP Devices > IP Device Management > Inventory Data > "Pings" Tab
- IP Device Interaction > Read IP Device Data > "Info" Tab
- IP Device Interaction > Reset IP Devices > "Info" Tab

General Data

☑ Enable IP Device Pings

Enable IP Device Pings

Checkbox for activating IP device PING settings.

Possible Action Buttons

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

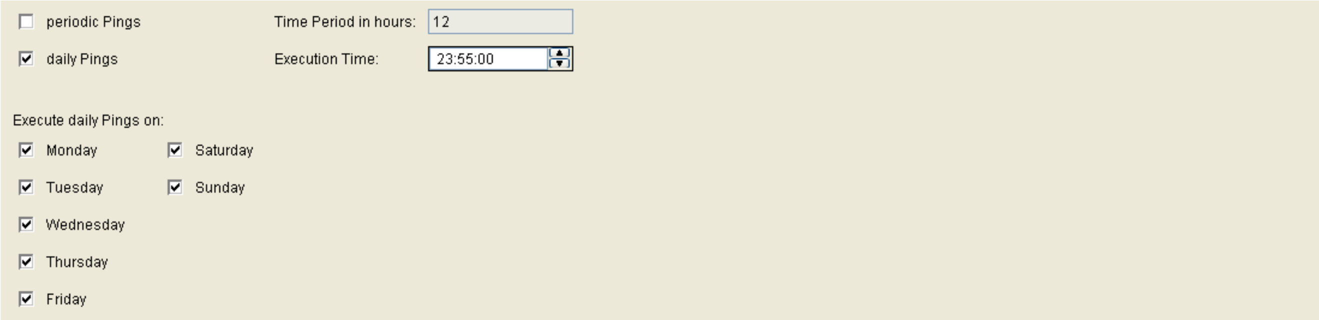
Refresh

Refreshes the content of the relevant page.

7.4.3.1 "IP Phones" Tab

Call: Main Menu > IP Devices > IP Device Interaction > Ping IP Devices > "IP Phones" Tab

You can define the chronological order of PING requests for IP phones in this tab.



□ periodic Pings   Time Period in hours: 12

☑ daily Pings   Execution Time: 23:55:00

Execute daily Pings on:

☑ Monday   ☑ Saturday

☑ Tuesday   ☑ Sunday

☑ Wednesday

☑ Thursday

☑ Friday

periodic Pings

Checkbox for activating periodic PINGs.

Time Period in hours

Time between two periodic pings. Only applies if "periodically Pings" is active.

Value range: **1** ... **23** hours.

daily Pings

Checkbox for activating daily pings.

Execution Time:

Time for daily pings (for a calendar, see Section 5.4.2.4, "Time field with calendar button").

Only applies if "daily Pings" is active.

Execute daily Pings on:

This function enables you to restrict pings to individual weekdays.

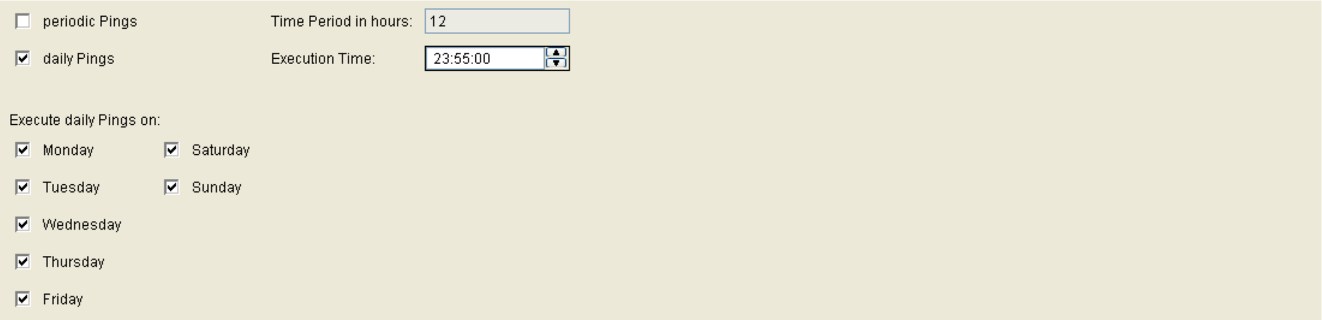
Options available (several options possible):

- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**
- **Sunday**

Only applies if "daily Pings" is active.

7.4.3.2 "IP Clients" Tab

Call: Main Menu > IP Devices > IP Device Interaction > Ping IP Devices > "IP Clients" Tab



□ periodic Pings Time Period in hours: 12

☑ daily Pings Execution Time: 23:55:00

Execute daily Pings on:

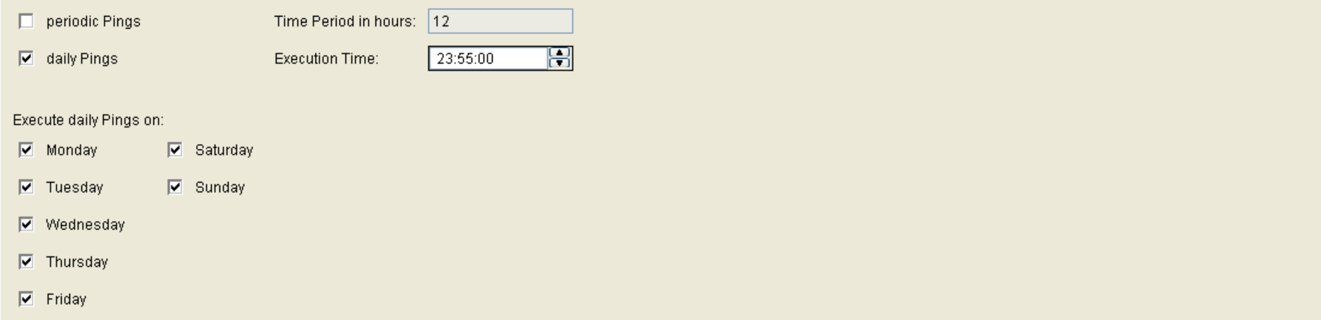
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

You can define the chronological order of PING requests for IP clients in this tab.

For a description of the interface, see Section 7.4.3.1, ""IP Phones" Tab".

7.4.3.3 "IP Gateways" Tab

Call: Main Menu > IP Devices > IP Device Interaction > Ping IP Devices > "IP Gateways" Tab



□ periodic Pings	Time Period in hours: 12
☑ daily Pings	Execution Time: 23:55:00

Execute daily Pings on:

☑ Monday	☑ Saturday
☑ Tuesday	☑ Sunday
☑ Wednesday	
☑ Thursday	
☑ Friday	

You can define the chronological order of PING requests for IP clients in this tab.

For a description of the interface, see Section 7.4.3.1, ""IP Phones" Tab".

7.4.4 Scan IP Devices

Call: Main Menu > IP Devices > IP Device Interaction > Scan IP Devices

This area features the following components:

- General Data
- Possible Action Buttons
- "IP Ranges" Tab
- "Configuration" Tab
- "Scan Results" Tab

This function lets a DLS user with an TAP, for example, create a DLS database of all IP Devices in the network for processing purposes.

During a scan, the DLS sends a ContactMe request consisting of a short HTML message to every IP address in the specified range. The DLS then waits to see if the relevant device sends a callback. If the ICMP ping is activated for the scan (see "Configuration" Tab), an ICMP ping is sent before a ContactMe request to find out if the IP address is assigned to a device.

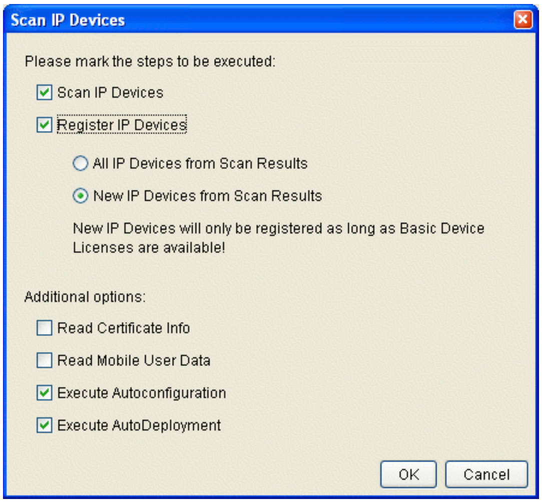
Configuring an IP scanner

If you have not done so already, you must now create an IP scanner, that is, a configuration that indicates the IP areas to be scanned and how the scan should proceed. To do this, proceed as follows:

1. Create a new IP scanner by clicking **New**.
2. Enter a name and a description for the IP scanner in the General Data area.
3. Enter the address range that should be scanned and the port where the devices can be reached for the DLS in the **"IP Ranges" Tab** area.
4. If necessary, specify additional parameters in **"Configuration" Tab**.

Start scanning

A selection window is displayed when you click **Scan IP Devices**:



Please mark the steps to be executed:

☑ Scan IP Devices

☑ Register IP Devices

○ All IP Devices from Scan Results

● New IP Devices from Scan Results

New IP Devices will only be registered as long as Basic Device Licenses are available!

Additional options:

□ Read Certificate Info

□ Read Mobile User Data

☑ Execute Autoconfiguration

☑ Execute AutoDeployment

The administrator can decide whether the workpoint scan should take place first or at the same time as registration:

- **Scan IP Devices**
  The IP devices are scanned.
- **Register IP Devices**
  The IP devices are registered.

Registration is necessary to record the workpoints in the inventory database.

The whole procedure can also take place in two steps, with scanning as the first step and registration as the second. Registration differentiates between the registration of all scanned IP devices and the registration of only those IP devices that are not yet contained in the inventory database:

- **All IP devices from Scan Results**
  This registers all IP Devices contained in the scan results, including those already registered.
- **New IP Devices from Scan Results**
  Only unregistered IP devices are registered.

If the administrator does not wish to allow all IP devices recognized by the scan to be registered, he or she must delete the corresponding entries from the scan results.

> If you are using TAP to scan IP devices for the first time at a customer facility, (for example, to record the inventory), ensure that **Perform AutoDeployment** is deactivated using deployment rules. This prevents unwanted deployment in the customer network during operating hours.

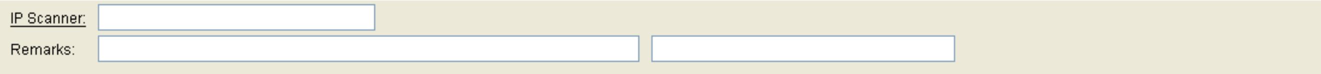
If individual devices are not found during the scan, increase the timeout (see **Timeout (sec)**) and run a new scan.
If some of the workpoints are still not reached during scanning, a second scan operation is started for the affected IP devices. This takes **at least five minutes**. During this time, the

progress bar indicates 99%; the IP devices identified during the first run can now be administered.
An entry is stored in the activity log for every IP device that was not reached during the second scan (see Section 14.1, "Job Control").

> When scanning IP devices, a valid DLS server address is transferred to the scanned IP device so that the device can contact the DLS server independently later.
> This does not happen, however, if the IP device already received a DLS server address from a DHCP server. In this case, the DLS address delivered by the DHCP server is maintained.

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data



IP Scanner:		
Remarks:		

IP Scanner:

Name of the IP scanner.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all scanners that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

New

Creates a new IP scanner.

Delete

Deletes one or more IP scanners (multiple selections possible in table view).

Scan Workpoints

Starts the IP scanner displayed in **Object** view.

Refresh

Refreshes the content of the relevant page.

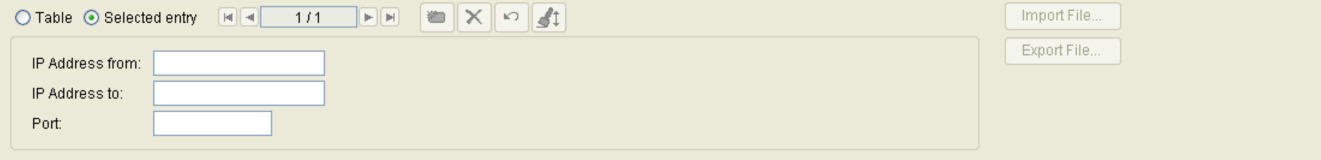
7.4.4.1 "IP Ranges" Tab

Call: Main Menu > IP Devices > IP Device Interaction > Scan IP Devices > "IP Ranges" Tab

Use this tab to specify an IP address range/port number combination for the IP Devices to be scanned. You can add another combination in the **New** and **Object** view with the button and delete it with the ☒ button.

In addition, you can import a CSV file containing IP/port combinations and export this data in CSV format.

> To avoid heavy network load, the IP address range should be selected so that where possible only one workpoint is scanned.
>
> If the IP range specified contains other IP clients (not workpoints), malfunctions can sometimes occur at the devices.



IP Address from

IP address for the lower limit of the IP range to be scanned.

Format: **000.000.000.000**, 000 = value between 000 and 255.

IP Address to

IP address for the upper limit of the IP range to be scanned.

Format: **000.000.000.000**, 000 = value between 000 and 255.

Port

Port number for the IP addresses to be scanned.

The following default ports are used by the various workpoint types and should be entered here:

- IP phone: **8085**
- IP client: **8082**
- WLAN phone: **80**

Format: Up to five digits.

Import File...

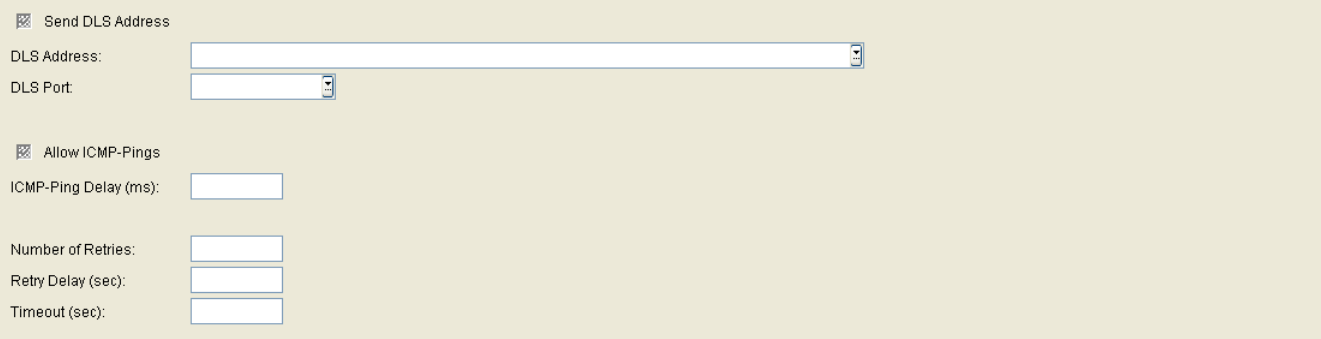
Loads a file in CSV format with existing IP ranges and port numbers into the IP range table.

Export File...

Saves the IP ranges and port numbers from the IP range table to a file in CSV format.

7.4.4.2 "Configuration" Tab

Call: Main Menu > IP Devices > IP Device Interaction > Scan IP Devices > "Configuration" Tab



☒ Send DLS Address

DLS Address:

DLS Port:

☒ Allow ICMP-Pings

ICMP-Ping Delay (ms):

Number of Retries:

Retry Delay (sec):

Timeout (sec):

Send DLS Address

Use the DLS on an TAP to activate the **Send DLS Address** checkbox and identify the DLS address and the DLS port number on the EWS. During scanning, the workpoints are informed of the address data of the DLS that serves them.

> The Send DLS Address option must not be used if there is a permanent DLS server in the network.

DLS Address:S

IP address of the DLS server on the EWS.

Format: **000.000.000.000** (000 = value between 000 and 255).

DLS Port:

Port number of the DLS server on the EWS.

Value range: Up to five digits.

Allow ICMP-Pings:

If the checkbox is activated, ICMP pings are used when scanning. This speeds up IP device scans because ContactMe requests are only sent to IP addresses where the ICMP ping was successful.

> This checkbox must be deactivated if the network does not support ICMP pings as otherwise the IP device scan is unable to deliver a result.

ICMP-Delay (ms):

Interval between ICMP pings to ensure that the ICMP pings are not blocked by the operating system.

Number of Retries:

Maximum number of retries for a scan. The value is evaluated for each IP address.

Default: **1**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries. The value is evaluated for each IP address.

Default: **10**

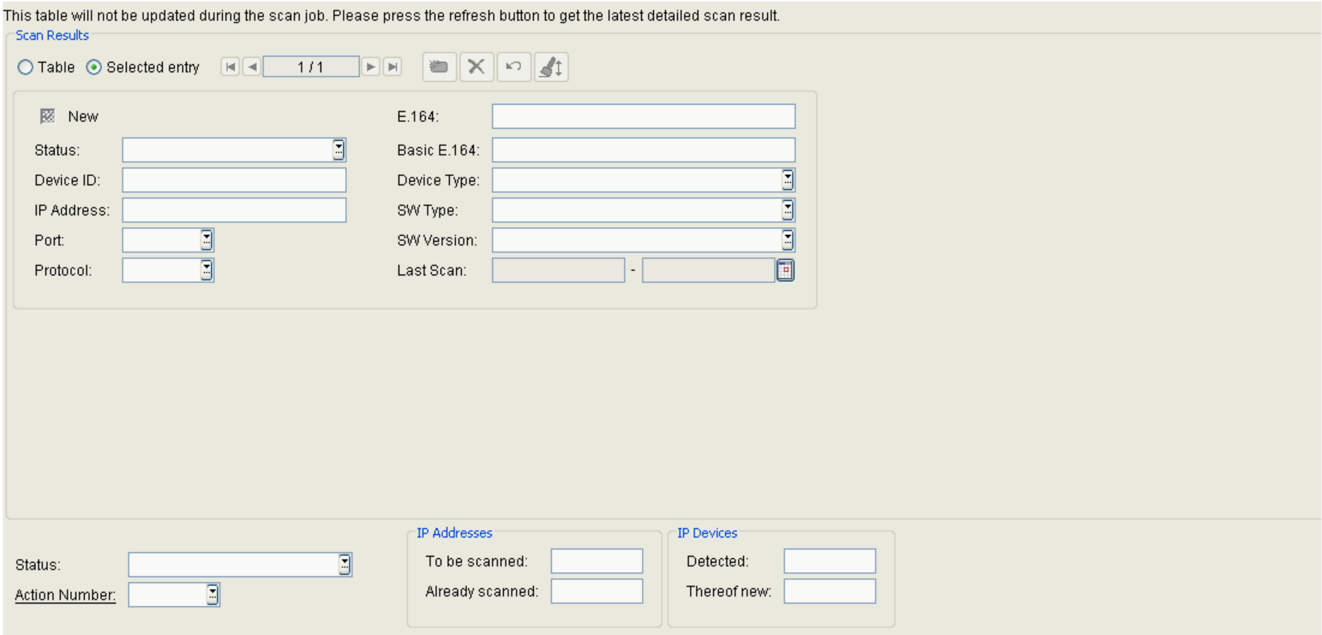
Timeout (sec)

The maximum amount of time that may elapse between a Contact-Me request from the DLS and registration of the IP Devices involved.

Default: **60**

7.4.4.3 "Scan Results" Tab

Call: Main Menu > IP Devices > IP Device Interaction > Scan IP Devices > "Scan Results" Tab



This table will not be updated during the scan job. Please press the refresh button to get the latest detailed scan result.

New

An IP Device that is reregistered during a scan is indicated by a checkmark.

Status

Displays the status of the scan for each individual IP Device.

Possible values:

- **running**
- **confirmed**
- **finished**
- **failed**

Device ID

Displays the device ID of the scanned IP Device. This is used for unique identification of the IP device. In IP phones, this is generally identical to the MAC address.

IP Address

Displays the IP address of the scanned IP Device.

Port

Displays the port that the scanned IP Device uses to communicate with the DLS.

Protocol

Displays the protocol that the scanned IP Device uses to communicate with the DLS.

E.164

Displays the E.164 number of the scanned IP Device.

Basic E.164

Displays the basic E.164 number of the scanned IP Device.

Device Type

Displays the phone type of the scanned IP Device.

Example: **optiPoint 410 advance**

Software Type:

Displays the software type of the scanned IP Device.

Example: **Siemens SIP**, **Siemens HFA**

SW Version

Displays the software version installed on the scanned IP Device.

Example: **6.0.53**

Last Scan

Displays the data and time of the last scan.

Status:

Displays the current scan status.

Example: **running**, **finished**

Action Number:

Displays the action number for the current scan.

IP Addresses

To be scanned:

Displays how many IP addressed within the IP range are yet to be scanned.

Already scanned:

Displays how many IP addressed within the IP range are already scanned.

Workpoints

Detected:

Displays how many workpoints have been found by the scan.

Thereof new:

Displays how many of the workpoints found by the scan are not yet registered.

7.5 IP Device XML Applications

Call: Main Menu > IP Devices > IP Device XML Applications

The DLS can be used not only for installing and configuring XML applications, but also as application server itself.

> ⓘ XML applications are available only for OpenStage 60 and OpenStage80 with firmware versions SIP V1, SIP V2, and HFA V2.

This menu item consists of the following areas:

- MakeCall
- NewsService
- NewsService Archive

7.5.1 MakeCall

Call: Main Menu > IP Devices > IP Device XML Applications > MakeCall

This mask enables the start (=push) of the XML application ’MakeCall’. This application initiates calls from selected end devices to a target end device. After this, it is possible to check in the call log whether all calls have been executed. This check makes sense after a software update, for instance. The application can only be started from the DLS only, not from the end devices.

To start the function, press the **MakeCall** action button. Then, a dialog window will request the target call number.

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

MakeCall

Pushes the XML application ’MakeCall’. A subsequent dialog window asks the **MakeCall Destinationnumber**.

Send Info Alert

Pushes the XML Application ,NewsService'. A subsequent dialog window asks for the **Header** and **Text** of the message.

Send Text-/Picture-File

Pushes the XML Application ’NewsService’. A subsequent dialog window asks for the name of the **Text-/Picture-File**.

Delete

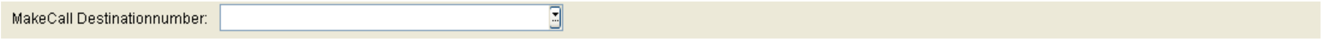
Deletes the saved news.

Refresh

Refreshes the window contents from the database.

7.5.1.1 "Info" Tab

Call: Main Menu > IP Devices > IP Device XML Applications > MakeCall > "Info" Tab



MakeCall Destinationnumber:

MakeCall Destinationnumber

Displays the destination number for the last automatic call initiated by the XML Application 'MakeCall'.

7.5.2 NewsService

Call: Main Menu > IP Devices > IP Device XML Applications > NewsService

This screen enables the start (=push) of the XML application ’NewsService’. This application sends messages to selected end devices. These can be text or picture files. There is a dictinction between an info alert message and a file message. On an info alert, existing calls are disconnected, and the message is displayed on the end device along with an ’INFO’ symbol, until it is confirmed by a button press. File messages are displayed on the end device if it is in idle mode.

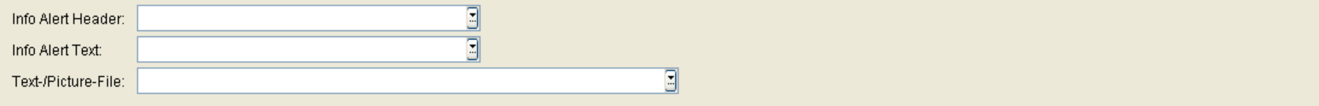
The messages are created and sent by means of the DLS. Stored messages can be read again at the end device. To send a message, press **Send Info Alert** or **Send Text-/Picture File**. Then, a dialog window will ask for the **Header** and **Text** of the message, or for the name of the **Text-/Picture-File**.

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

7.5.2.1 "Info" Tab

Call: Main Menu > IP Devices > IP Device XML Applications > NewsService > "Info" Tab



Info Alert Header:

Info Alert Text:

Text-/Picture-File:

Info Alert Header

Header of the last Info Alert sent to IP Device by means of XML Application 'NewsService'.

Info Alert Text

Text of the last Info Alert sent to IP Device by means of XML Application 'NewsService'.

Text-/Picture File

Name of last Text- (.txt) or Picture-File (.jpg, .bmp, .gif, .png) sent to IP Device by means of XML Application 'NewsService'.

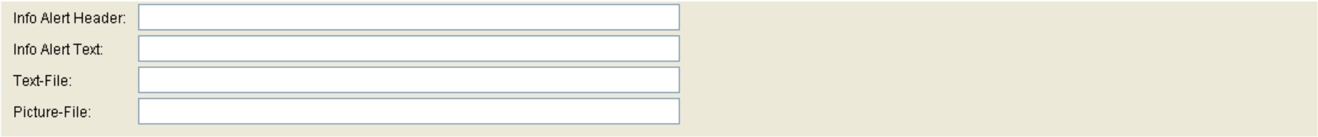
7.5.3 NewsService Archive

Call: Main Menu > IP Devices > IP Device XML Applications > NewsService Archive

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab
- "IP Devices" Tab

General Data



Info Alert Header:	
Info Alert Text:	
Text-File:	
Picture-File:	

NewsService ID

Continuous numbering

NewsServiceType

Type of message.

Possible Values:

- **Info Alert**
- **Picture File**
- **Text File**

Account

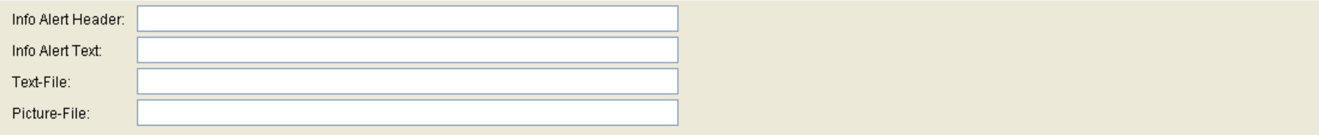
Account name of the user who issued the message.

Execution Time

Execution time of the message sending job.

7.5.3.1 "Info" Tab

Call: Main Menu > IP Devices > IP Device XML Applications > NewsService Archive > "Info" Tab



Info Alert Header:

Info Alert Text:

Text-File:

Picture-File:

Info Alert Header

Header of info alert sent to IP Device.

Info Alert Text

Text of info alert sent to IP Device.

Text File

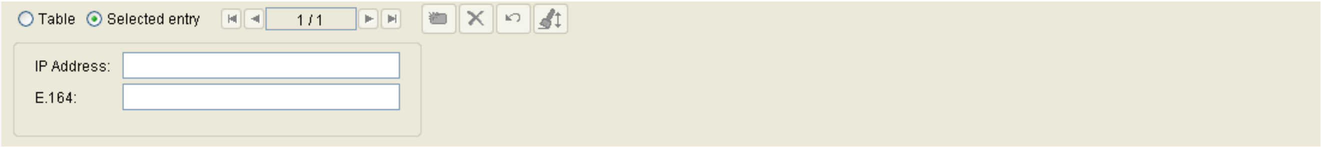
Name of text file sent to IP Device.

Picture File

Name of picture file sent to IP Device.

7.5.3.2 "IP Devices" Tab

Call: Main Menu > IP Devices > IP Device XML Applications > NewsService Archive > "IP Devices" Tab



IP Address:

E.164:

IP Address

IP Address of IP Device the news is sent to.

E.164

Complete E.164 subscriber number of IP Device the news is sent to.

7.6 IP Device Management

Call: Main Menu > IP Devices > IP Device Management

This menu item consists of the following areas:

- Inventory Data
- Trash
- IP Infrastructure
- IP Device Configuration

7.6.1 Inventory Data

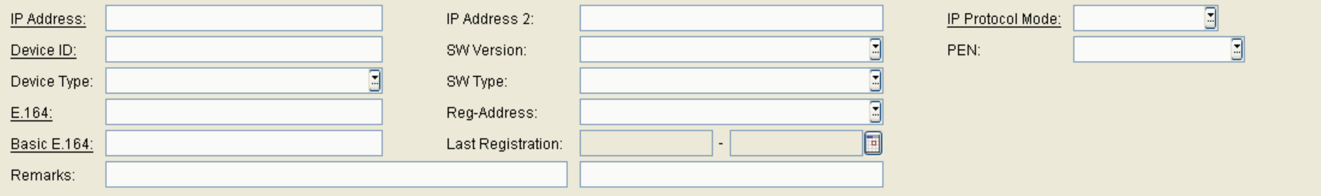
Call: Main Menu > IP Devices > IP Device Management > Inventory Data

This area features the following components:

- General Data
- Possible Action Buttons
- "Inventory Data" Tab
- "Information" Tab
- "Pings" Tab

General Data

This part of the content area is used for entering parameters in **Search** view to find a specific group of workpoints. The base data associated with the workpoints found is displayed in the **Object** view (no changes possible except under **Remarks**).



> You can use the following wildcards in all text and selection list fields in **Search** view:
>
> - * (asterisk): Stands for any sequence of characters.
> - ? (question mark): Stands for exactly one character.
> - ^ (circumflex): Stands for an empty field.
>
> Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.
>
> All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only **those** workpoints that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of the workpoint. For OpenStage, in IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

Workpoint device type.

All workpoint types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **optiPoint 410 standard**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version used by the workpoint.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

SW Type:

Software type used by the workpoint.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**

PEN:

Position of the gateway assembly group (plug-in position).

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last workpoint registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Remarks:

Fields for general information.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Starts a job for distributing the configuration changes. For more information, see Section 15.1, "First Steps: Changing IP Device Parameters".

Discard

The modifications carried out in the mask are discarded.

Export File

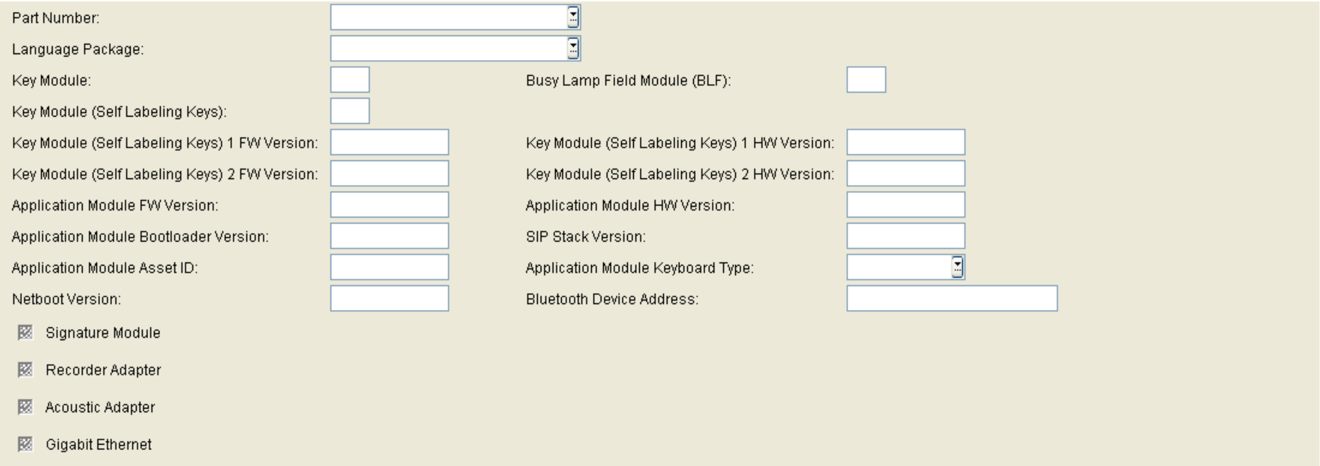
The inventory data are exported into a csv formatted file.

Refresh

Refreshes the window contents from the database.

7.6.1.1 "Inventory Data" Tab

Call: Main Menu > IP Devices > IP Device Management > Inventory Data > "Inventory Data" Tab



Part Number:			
Language Package:			
Key Module:		Busy Lamp Field Module (BLF):	
Key Module (Self Labeling Keys):			
Key Module (Self Labeling Keys) 1 FW Version:		Key Module (Self Labeling Keys) 1 HW Version:	
Key Module (Self Labeling Keys) 2 FW Version:		Key Module (Self Labeling Keys) 2 HW Version:	
Application Module FW Version:		Application Module HW Version:	
Application Module Bootloader Version:		SIP Stack Version:	
Application Module Asset ID:		Application Module Keyboard Type:	
Netboot Version:		Bluetooth Device Address:	

☑ Signature Module

☑ Recorder Adapter

☑ Acoustic Adapter

☑ Gigabit Ethernet

Part Number:

Part number of the workpoint; this number identifies the relevant hardware.

The value is read-only.

Name	Part Number
optiPoint 410 entry arctic	S30817-S7201-A101-*
optiPoint 410 entry manganese	S30817-S7201-A107-*
optiPoint 410 entry arctic (no logo)	S30817-S7201-N101-*
optiPoint 410 entry manganese (no logo)	S30817-S7201-N107-*
optiPoint 410 entry SIP V4.1 arctic	S30817-S7201-L101-*
optiPoint 410 entry SIP V4.1 manganese	S30817-S7201-L107-*
optiPoint 410 entry SIP V5.x arctic	S30817-S7201-M101-*
optiPoint 410 entry SIP V5.x manganese	S30817-S7201-M107-*
optiPoint 410 entry SIP V4.1 arctic (no logo)	S30817-S7201-P101-*
optiPoint 410 entry SIP V4.1 manganese (no logo)	S30817-S7201-P107-*
optiPoint 410 economy arctic	S30817-S7202-A101-*
optiPoint 410 economy manganese	S30817-S7202-A107-*
optiPoint 410 economy arctic (no logo)	S30817-S7202-N101-*
optiPoint 410 economy manganese (no logo)	S30817-S7202-N107-*

Table 7-1

Name	Part Number
optiPoint 410 economy SIP V4.1 arctic	S30817-S7202-L101-*
optiPoint 410 economy SIP V4.1 manganese	S30817-S7202-L107-*
optiPoint 410 economy SIP V5.x arctic	S30817-S7202-M101-*
optiPoint 410 economy SIP V5.x arctic	S30817-S7202-M101-*
optiPoint 410 economy SIP V5.x manganese	S30817-S7202-M107-*
optiPoint 410 economy SIP V4.1 arctic (no logo)	S30817-S7202-P101-*
optiPoint 410 entry SIP V4.1 manganese (no logo)	S30817-S7202-P107-*
optiPoint 410 economy plus arctic	S30817-S7212-A101-*
optiPoint 410 economy plus manganese	S30817-S7212-A107-*
optiPoint 410 economy plus arctic (no logo)	S30817-S7212-N101-*
optiPoint 410 economy plus manganese (no logo)	S30817-S7212-N107-*
optiPoint 410 economy plus SIP V4.1 arctic	S30817-S7212-L101-*
optiPoint 410 economy plus SIP V4.1 manganese	S30817-S7212-L107-*
optiPoint 410 economy plus BIZIP V4.1 arctic	S30817-S7212-L201-*
optiPoint 410 economy plus BIZIP V4.1 manganese	S30817-S7212-L207-*
optiPoint 410 economy plus SIP V5.x arctic	S30817-S7212-M101-*
optiPoint 410 economy plus SIP V5.x manganese	S30817-S7212-M107-*
optiPoint 410 economy plus SIP V4.1 arctic (no logo)	S30817-S7212-P101-*
optiPoint 410 economy plus SIP V4.1 manganese (no logo)	S30817-S7212-P107-*
optiPoint 410 standard arctic	S30817-S7203-A101-*
optiPoint 410 standard manganese	S30817-S7203-A107-*
optiPoint 410 standard arctic (no logo)	S30817-S7203-N101-*
optiPoint 410 standard manganese (no logo)	S30817-S7203-N107-*
optiPoint 410 standard SIP V4.1 arctic	S30817-S7203-L101-*
optiPoint 410 standard SIP V4.1 manganese	S30817-S7203-L107-*
optiPoint 410 standard SIP V5.x arctic	S30817-S7203-M101-*
optiPoint 410 standard SIP V5.x manganese	S30817-S7203-M107-*
optiPoint 410 standard SIP V4.1 arctic (no logo)	S30817-S7203-P101-*
optiPoint 410 standard SIP V4.1 manganese (no logo)	S30817-S7203-P107-*

Table 7-1

Name	Part Number
optiPoint 410 advance arctic	S30817-S7204-A101-*
optiPoint 410 advance manganese	S30817-S7204-A107-*
optiPoint 410 advance arctic (no logo)	S30817-S7204-N101-*
optiPoint 410 advance manganese (no logo)	S30817-S7204-N107-*
optiPoint 410 advance SIP V4.1 arctic	S30817-S7204-L101-*
optiPoint 410 advance SIP V4.1 manganese	S30817-S7204-L107-*
optiPoint 410 advance BIZIP V4.1 arctic	S30817-S7204-L201-*
optiPoint 410 advance BIZIP V4.1 manganese	S30817-S7204-L207-*
optiPoint 410 advance SIP V5.x arctic	S30817-S7204-M101-*
optiPoint 410 advance SIP V5.x manganese	S30817-S7204-M107-*
optiPoint 410 advance SIP V4.1 arctic (no logo)	S30817-S7204-P101-*
optiPoint 420 economy arctic	S30817-S7209-A101-*
optiPoint 420 economy manganese	S30817-S7209-A107-*
optiPoint 420 economy arctic (no logo)	S30817-S7209-N101-*
optiPoint 420 economy manganese (no logo)	S30817-S7209-N107-*
optiPoint 420 economy SIP V4.1 arctic	S30817-S7209-L101-*
optiPoint 420 economy SIP V4.1 manganese	S30817-S7209-L107-*
optiPoint 420 economy SIP V5.x arctic	S30817-S7209-M101-*
optiPoint 420 economy SIP V5.x manganese	S30817-S7209-M107-*
optiPoint 420 economy SIP V4.1 arctic (no logo)	S30817-S7209-P101-*
optiPoint 420 entry SIP V4.1 manganese (no logo)	S30817-S7209-P107-*
optiPoint 420 economy plus arctic	S30817-S7210-A101-*
optiPoint 420 economy plus manganese	S30817-S7210-A107-*
optiPoint 420 economy plus arctic (no logo)	S30817-S7210-N101-*
optiPoint 420 economy plus manganese (no logo)	S30817-S7210-N107-*
optiPoint 420 economy plus SIP V4.1 arctic	S30817-S7210-L101-*
optiPoint 420 economy plus SIP V4.1 manganese	S30817-S7210-L107-*
optiPoint 420 economy plus SIP V5.x arctic	S30817-S7210-M101-*
optiPoint 420 economy plus SIP V5.x manganese	S30817-S7210-M107-*
optiPoint 420 economy plus SIP V4.1 arctic (no logo)	S30817-S7210-P101-*

Table 7-1

Name	Part Number
optiPoint 420 economy plus SIP V4.1 manganese (no logo)	S30817-S7210-P107-*
optiPoint 420 standard arctic	S30817-S7211-A101-*
optiPoint 420 standard manganese	S30817-S7203-A107-*
optiPoint 420 standard arctic (no logo)	S30817-S7203-N101-*
optiPoint 420 standard manganese (no logo)	S30817-S7203-N107-*
optiPoint 420 standard SIP V4.1 arctic	S30817-S7203-L101-*
optiPoint 420 standard SIP V4.1 manganese	S30817-S7203-L107-*
optiPoint 420 standard SIP V5.x arctic	S30817-S7203-M101-*
optiPoint 420 standard SIP V5.x manganese	S30817-S7203-M107-*
optiPoint 420 standard SIP V4.1 arctic (no logo)	S30817-S7203-P101-*
optiPoint 420 standard SIP V4.1 manganese (no logo)	S30817-S7203-P107-*
optiPoint 420 advance arctic	S30817-S7207-A101-*
optiPoint 420 advance manganese	S30817-S7204-A107-*
optiPoint 420 advance arctic (no logo)	S30817-S7204-N101-*
optiPoint 420 advance manganese (no logo)	S30817-S7204-N107-*
optiPoint 420 advance SIP V4.1 arctic	S30817-S7204-L101-*
optiPoint 420 advance SIP V4.1 manganese	S30817-S7204-L107-*
optiPoint 420 advance SIP V5.x arctic	S30817-S7204-M101-*
optiPoint 420 advance SIP V5.x manganese	S30817-S7204-M107-*
optiPoint 420 advance SIP V5.x manganese	S30817-S7204-M107-*
optiPoint 420 advance SIP V4.1 arctic (no logo)	S30817-S7204-P101-*
optiPoint 420 advance SIP V4.1 manganese (no logo)	S30817-S7204-P107-*

Table 7-1

Part numbers for add-on devices (not displayed):

Name	Part Number
optiPoint 420 SLB key module arctic	S30817-S7206-A101-*
optiPoint 420 SLB key module manganese	S30817-S7206-A107-*
optiPoint 420 SLB key module arctic (no logo)	S30817-S7206-N101-*

Table 7-2

Name	Part Number
optiPoint 420 SLB key module manganese (no logo)	S30817-S7206-N107-*
OpenStage 20 SIP 100 ice blue	S30817-S7401-A101
OpenStage 20 SIP 100 lava	S30817-S7401-A103
OpenStage 20 HFA GIG ice blue	S30817-S7401-B101
OpenStage 20 HFA GIG lava	S30817-S7401-B103
OpenStage 20 SIP GIG ice blue	S30817-S7401-C101
OpenStage 20 SIP GIG lava	S30817-S7401-C103
OpenStage 20 HFA 100 ice blue	S30817-S7401-D101
OpenStage 20 HFA 100 lava	S30817-S7401-D103
OpenStage 40 SIP 100 ice blue	S30817-S7402-A101
OpenStage 40 SIP 100 lava	S30817-S7402-A103
OpenStage 40 HFA GIG ice blue	S30817-S7402-B101
OpenStage 40 HFA GIG lava	S30817-S7402-B103
OpenStage 40 SIP GIG ice blue	S30817-S7402-C101
OpenStage 40 SIP GIG lava	S30817-S7402-C103
OpenStage 40 HFA 100 ice blue	S30817-S7402-D101
OpenStage 40 HFA 100 lava	S30817-S7402-D103
OpenStage 60 SIP 100 ice blue	S30817-S7403-A101
OpenStage 60 SIP 100 lava	S30817-S7403-A103
OpenStage 60 HFA GIG ice blue	S30817-S7403-B101
OpenStage 60 HFA GIG lava	S30817-S7403-B103
OpenStage 60 SIP GIG ice blue	S30817-S7403-C101
OpenStage 60 SIP GIG lava	S30817-S7403-C103
OpenStage 60 HFA 100 ice blue	S30817-S7403-D101
OpenStage 60 HFA 100 lava	S30817-S7403-D103
OpenStage 80 SIP GIG ice blue	S30817-S7404-A101
OpenStage 80 SIP GIG lava	S30817-S7404-A103
OpenStage 80 HFA GIG ice blue	S30817-S7404-B101
OpenStage 80 HFA GIG lava	S30817-S7404-B103
OpenStage 80 HFA 100 ice blue	S30817-S7404-D101

Table 7-2

Name	Part Number
OpenStage 80 HFA 100 lava	S30817-S7404-D103
OpenStage 80 SIP 100 ice blue	S30817-S7404-E101
OpenStage 80 SIP 100 lava	S30817-S7404-E103

Table 7-2

Language Package:

Name of installed Language Package.

The value is read-only.

Key Module:

Number of Self Labeling Keys Modules connected.

The value is read-only.

Key Module (Self Labeling Keys):

Number of Self Labeling Keys Modules connected.

The value is read-only.

Key Module (Self Labeling Keys) 1 FW Version:

Firmware version of the first Self Labeling Keys Module.

The value is read-only.

Key Module (Self Labeling Keys) 2 FW Version:

Firmware version of the second Self Labeling Keys Module.

The value is read-only.

Application Module FW Version:

Firmware version of the optiPoint Application Module.

The value is read-only.

Application Module Bootloader Version:

Bootloader version of the optiPoint Application Module.

The value is read-only.

Application Module Asset ID:

You can use the asset ID for the unique identification of an optiPoint Application Module.

Coding:

Byte 1	Byte 2	Byte 3	Byte 4
yyyywwww	wwdddlll	aassssss	sssssttt

Definition:

Section	Length	Meaning	Example
yyyy	4 bits	Last digit of the year	0001 = 2001
w...w	6 bits	Calendar week	000001 = Week 1
ddd	3 bits	Day	001 = Monday, 111 = Sunday
lll	3 bits	Design Line	000 = Siemens, else : reserved
aa	2 bits	Tester Group	0 - 3, factory setting
s...s	11 bits	Serial Number	0 ... 2047
ttt	3 bits	Tester Number	0.1 ... 6.7

The value is read-only.

Netboot Version:

Version of Netboot.

The value is read-only.

Signature module

Active when an optiPoint signature module is connected.

The value is read-only.

Recorder Adapter

Active when an optiPoint recorder module is connected.

The value is read-only.

Acoustic Adapter

Active when an optiPoint acoustic module is connected.

The value is read-only.

Gigabit Ethernet

Indicates whether the device has a gigabit LAN interface.

Busy Lamp Field Module (BLF):

Display showing the BLFs connected.

The value is read-only.

OpenStage 15 Key Module:

Hardware version of the OpenStage 15 Key Module.

Key Module 1 HW Version:

Hardware version of the first Self Labeling Key module.

The value is read-only.

Key Module 2 HW Version:

Hardware version of the second Self Labeling Key module.

The value is read-only.

Application Module HW Version:

Hardware version of the optiPoint Application Module.

The value is read-only.

SIP Stack Version:

Version of the SIP stack.

The value is read-only.

Application Module Keyboard Type:

Keyboard layout of the optiPoint application module connected.

Possible options:

- **QWERTZ**
  (German layout)
- **QWERTY**
  (American layout)

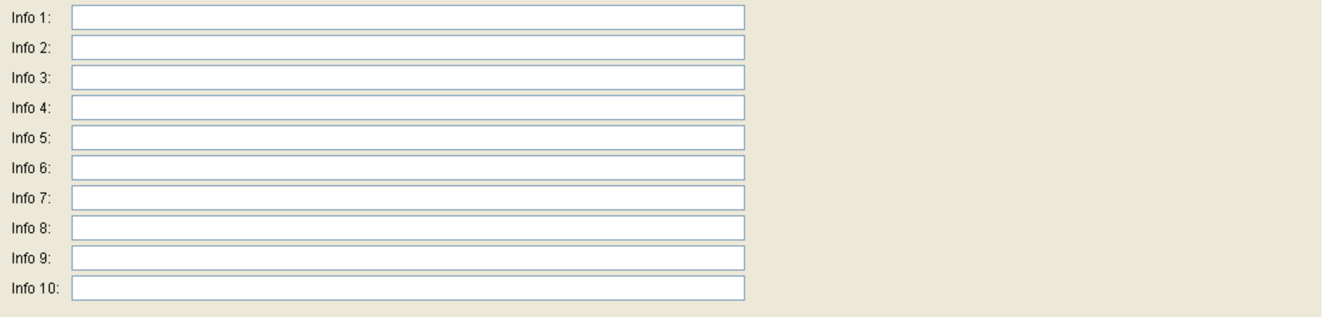
The value is read-only.

Bluetooth Device Address

Bluetooth address of the device.

7.6.1.2 "Information" Tab

Call: Main Menu > IP Devices > IP Device Management > Inventory Data > "Information" Tab



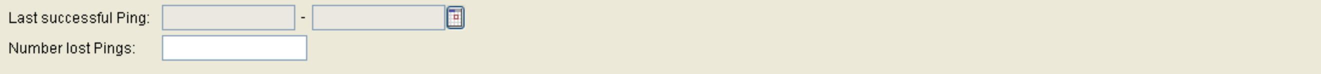
Info 1:
Info 2:
Info 3:
Info 4:
Info 5:
Info 6:
Info 7:
Info 8:
Info 9:
Info 10:

Info 1 ... Info 10:

Additional information on the workpoint, such as, billing data, etc., can be saved in these fields. This information is only stored in the DLS database. Administration is not performed at the workpoint.

7.6.1.3 "Pings" Tab

Call: Main Menu > IP Devices > IP Device Management > Inventory Data > "Pings" Tab



Last successful Ping:	-
Number lost Pings:	

For information on PING, see Section 7.4.3, "Ping IP Devices".

Last successful Ping

Displays the last successful PING.

The value is read-only.

Number lost Pings

Total number of unsuccessful PINGs.

The value is read-only.

7.6.2 Trash

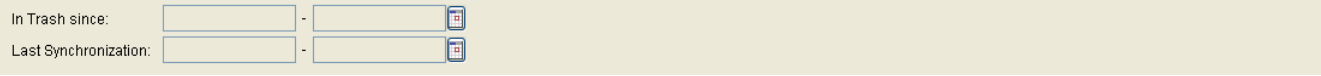
Call: Main Menu > IP Devices > IP Device Management > Trash

This area features the following components:

- General Data
- Possible Action Buttons
- "Information" Tab

7.6.2.1 "Information" Tab

Call: Main Menu > IP Devices > IP Device Management > Trash > "Information" Tab



In Trash since:		-	
Last Synchronization:		-	

In Trash since:

Date at which the IP Device has been put into trash.

Last Synchronization:

Date of last element manager synchronization for this E.164 number.

7.6.3 IP Infrastructure

Call: Main Menu > IP Devices > IP Device Management > IP Infrastructure

In this screen, the administrator can view the IP infrastructure data sent by an application to the DLS. The infrastructure policy is used for automatic adaptation: A default device profile is searched to which that location is assigned for which this infrastructure policy is defined. This profile will be applied to the IP Phone.

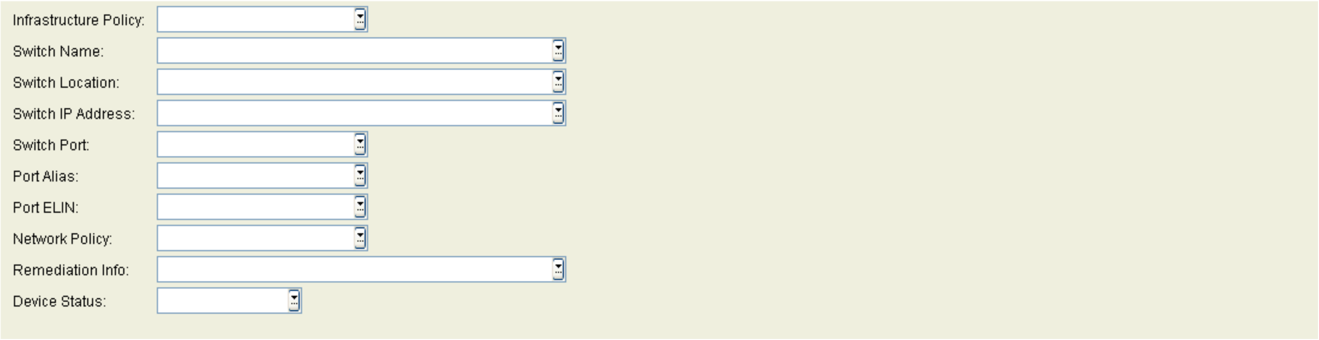
The infrastructure policy is not part of the API interface, though it will be mapped from the switch IP address, the switch port and the Network Policy. The mapping has to be configured by the administrator in the screen **Administration** > **Server Configuration** > **Infrastructure Policy**.

This area features the following components:

- General Data
- Possible Action Buttons
- "IP Switch Data" Tab

7.6.3.1 "IP Switch Data" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Infrastructure > "IP Switch Data" Tab



Infrastructure Policy:

Currently enabled policy, mapped from **Switch IP Address**, **Switch Port** and **Network Policy**.

Switch Name

Name of the edge switch device is currently plugged in.

Switch Location

Location of the edge switch device is currently plugged in.

Switch IP Address

IP address of the edge switch device is currently plugged in

Switch Port

Port of the edge switch device is currently plugged in.

Port Alias

Port Alias

Port ELIN

Port ELIN

Network Policy

Currently enabled network policy for this device.

Remediation Info

Long description of Network Policy.

Device Status

Connection status of device

Possible options:

- **plugged in**
- **plugged off**
- **unknown**

7.6.4 IP Device Configuration

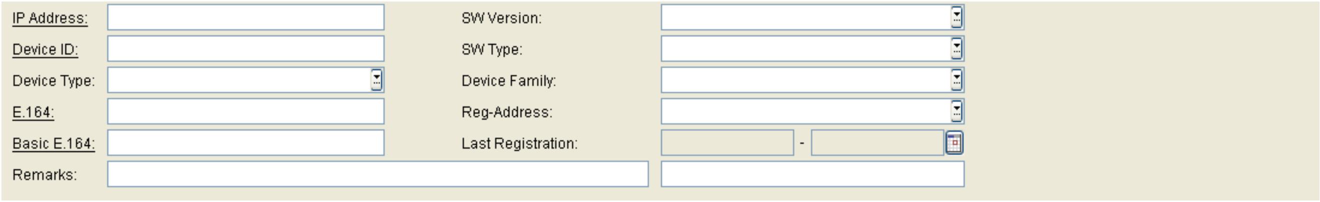
Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "General" Tab
- "EM Synchronization" Tab
- "Profile" Tab
- "DLS Connectivity" Tab
- "Security State Protocol" Tab
- "DCMP" Tab
- "Autoconfig. IP Phone" Tab
- "Autoconfig. IP Client" Tab
- "Autoconfig. IP Gateway" Tab
- "Archives Data" Tab

General Data

This part of the content area is used for entering parameters in **Search** view to find a specific group of IP Devices. The base data associated with the IP Devices found is displayed in the **Object** view (no changes possible except under **Remarks**).



IP Address:		SW Version:	
Device ID:		SW Type:	
Device Type:		Device Family:	
E.164:		Reg-Address:	
Basic E.164:		Last Registration:	-
Remarks:			

You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.

All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only those IP Devices that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of the IP Device.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

IP Device type.

All IP Device types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **optiPoint 410 standard**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

SW Version:

Software version used by the IP Device.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

SW Type:

Software type used by the IP Devices.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**

Device Family:

Type of device: IP Phone, IP Client, or IP Gateway.

Reg-Address:

IP address of the gateway or the gatekeeper where the IP Device must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last IP Device registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP Devices that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Starts a job for distributing the configuration changes. For more information, see Section 15.1, "First Steps: Changing IP Device Parameters".

Discard

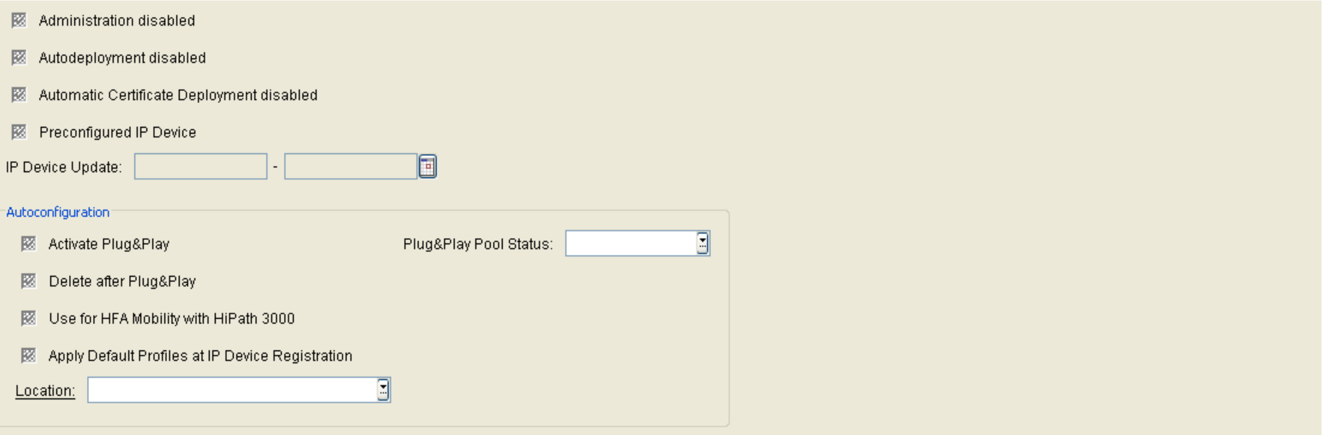
The modifications carried out in the mask are discarded.

Refresh

Refreshes the window contents from the database.

7.6.4.1 "General" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "General" Tab



☒ Administration disabled

☒ Autodeployment disabled

☒ Automatic Certificate Deployment disabled

☒ Preconfigured IP Device

IP Device Update: [ ] - [ ]

Autoconfiguration

☒ Activate Plug&Play — Plug&Play Pool Status: [ ]

☒ Delete after Plug&Play

☒ Use for HFA Mobility with HiPath 3000

☒ Apply Default Profiles at IP Device Registration

Location: [ ]

Administration disabled

If this checkbox is activated, IP Device administration via DLS is disabled. This temporary block prevents accidental changes on the IP Device.

Autodeployment disabled

If this checkbox is activated, autodeployment (see Section 15.6.2, "Automatic Deployment") is disabled for the IP Device.

Automatic Certificate Deployment disabled

If this checkbox is activated, automatic deployment of certificates (see Section 6.10, "Automatic Certificate Deployment") is disabled for this IP Device.

Preconfigured IP Device

If this checkbox is automatically activated, the IP device is preconfigured.

IP Device Update:

Specifies when the last IP Device update was performed.

Autoconfiguration

Activate Plug&Play

If this checkbox is activated, all data in this data record is assigned to the IP Device at the next registration.

Delete after Plug&Play

If this checkbox is activated, the virtual device changes to the real, registered device. The virtual device no longer exists after plug&play. Otherwise, the data record is copied and the virtual device remains.

Apply Default Profiles at IP Device Registration

If this checkbox is activated, the default profile defined in **Profile Management** > **Device Profile** for a particular location is identified and used for each registration. (For meaning and configuration of the location, see Section 6.2.2, "Location".)

Use for HFA Mobility with HiPath 3000

If active, this data record will be used in order to provide gateway registration data for HFA mobility with HiPath 3000.

Location

Current location of the IP Device. The value is set during registration and is displayed only herein. (For meaning and configuration of the location, see Section 6.2.2, "Location".)

Plug&Play Pool Status

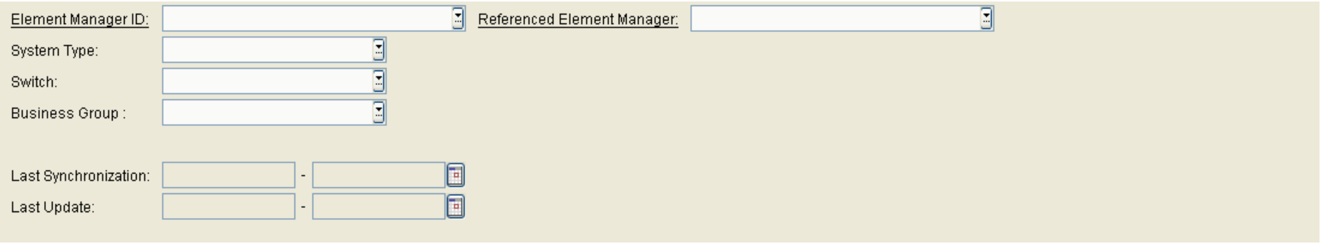
Indicates whether this dataset is used for automatic number assignment with Plug&Play.

Possible options:

- **none**
- **free**
- **in use**
- **multiple use**

7.6.4.2 "EM Synchronization" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "EM Synchronization" Tab



Element Manager ID:		Referenced Element Manager:	
System Type:			
Switch:			
Business Group :			
Last Synchronization:	-		
Last Update:	-		

Element Manager ID:

ID of the Element Manager assigned to the IP Device.

System Type:

Type of Element Manager assigned to the IP Device.

Possible values:

- **HiPath 4000**
- **HiPath DXWeb Pro**
- **HiPath 3000/5000**
- **Other**
- **OpenScape Voice**
- **Imported**
- **OpenOffice EE**
- **OpenScape Office MX/LX**

Switch:

Switch Name (For OpenScape Voice Assistant with Multiple Switch Support only).

Business Group:

Business Group Name (For OpenScape Voice Assistant).

Referenced Element Manager

If an Element Manager is entered here, the data record is only changed at EM synchronization if the data comes from the Element Manager specified here. For more information, see Section 15.2, "Changing the Element Manager Configuration and Creating Jobs".

Last Synchronization:

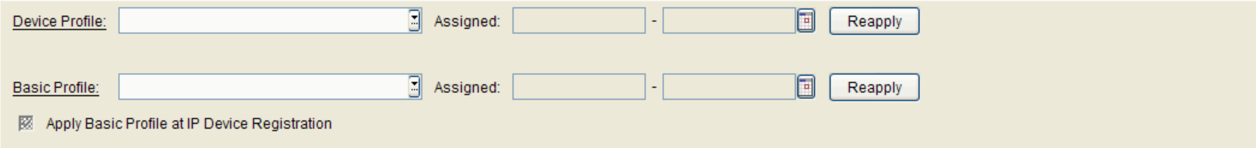
Time of the last synchronization with the system.

Last Update:

Time of the last change to these settings.

7.6.4.3 "Profile" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "Profile" Tab



Device Profile:

Selection of standard device configurations defined in **Profile Management > Device Profile** to be sent to the IP Device. This sets all existing parameters in the profile and any values previously set are overwritten. The parameters that are not replaced by the profile retain their values.

Assigned:

Time and date when the device profile was last assigned to the IP Device.

Reapply:

Apply the **Device Profile** to the IP Device again.

Basic Profile:

Selection of a standard user configuration defined in **Profile Management > User Data Profile** to be sent to the IP Device. This resets all parameters. The parameters that are not set by the profile are assigned default values.

Assigned:

Time when the user profile was last assigned to the IP Device.

Reapply:

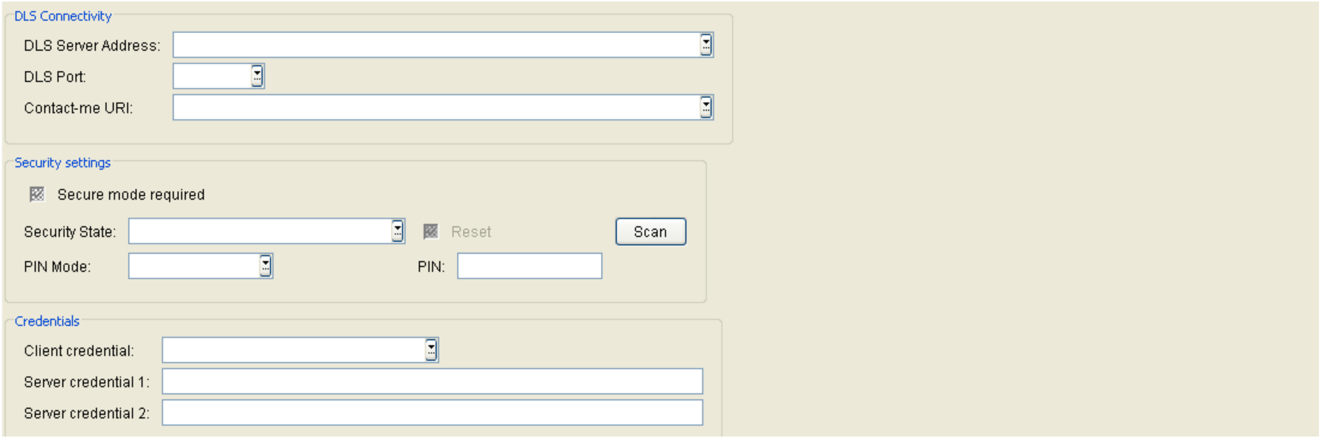
Apply the **Basic Profile** to the IP Device again.

Apply Basic Profile at IP Device Registration

If this checkbox is active, the IP Device is assigned the selected basic user profile at registration.

7.6.4.4 "DLS Connectivity" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity" Tab



DLS Connectivity

DLS Server Address:

IP address or host name of the DLS server. This value is automatically entered in the IP Device if a DHCP server is available and appropriately configured (see Section 4.10.4.3, "Configuring the DHCP Server for DLS").

DLS Port:

Port number of the DLS server. This value is automatically entered in the IP Device if a DHCP server is available and appropriately configured (see Section 4.10.4.3, "Configuring the DHCP Server for DLS").

Default: **18443**

Contact-me URI:

This field is for display purposes and contains the complete URL used by the IP Device to set up a connection to the DLS.

Security Settings

Secure mode required

If this checkbox is activated, mutual authentication is enabled for the DLS and the IP Device. The authentication process (bootstrap) begins the next time the IP Device registers at the DLS or is scanned.

Security Status:

Display the security mode for communication between the DLS and the IP Device.

Possible options:

- **Standard**
  In this mode, the DLS is authenticated using a standard certificate which is the same for all DLS installations.
- **Insecure**
  The previous "Default" mode is considered unsecure once the checkbox "Secure mode required" is activated.
- **Secure**
  This status is displayed once mutual authentication has been carried out between the DLS and the IP Device.
- **Pending**
  The credentials have been transferred to the device, the device has responded but a secure connection between the DLS and the device is not yet complete.
- **Credential transmitted**
  The credentials have been transferred to the device but the device has not yet responded.
- **Credential refused**
  The device rejects secure authentication (for example, because it is not technically ready).
- **Tan failed**
  In standard or individual PIN mode, both the device and the DLS must verify part of the PIN. If the number of failed verification attempts on the DLS side exceeds the threshold set, the security status is set to "Tan failed".
- **Blocked**
  This security status is not currently in use.
- **Go to Default**
  This security state is displayed when the security mode has been changed, but the IP Device does not respond.

PIN Mode:

Possible options:

- **No PIN**
  Access data is sent unencrypted to the IP Device.
- **Default PIN**
  A standard PIN is used for several IP Devices. This is generated automatically by the DLS (see Section 6.8.1, ""Secure mode" Tab").
- **Individual PIN**
  An individual PIN is created for the selected IP Device.

- **Unknown**
  This PIN mode is only available when the DLS interface is in **Search** mode. When moving the DLS to another server, the PIN mode cannot be retrieved. Therefore, the PIN mode is set to "unknown". This has no influence on the functionality.

Reset

If this checkbox is activated, the security mode can be reset to "Insecure" by clicking **Save**. The DLS must then send a new security configuration to the IP Device, that is, the bootstrap operation must be repeated (see also **Secure mode required**).

PIN:

This is entered locally at the IP Device and used to encrypt access data that was sent by the DLS and is required for the transfer to secure mode. The device generally prompts you to enter the PIN. Alternatively, the PIN may be preconfigured in the local administration menu.

Scan

Starts the scan for IP Gateways. In the process of scanning, the IP Gateway switches to secure mode, that is, the communication between gateway and DLS is secured.

Credentials

Client Credential

The device uses these credentials to authenticate itself at the DLS.

Possible options:

- **Active**
  The device last authenticated itself using the active client credentials.
- **Old**
  The device last authenticated itself using old client credentials.
- **Unknown**
  In the DLS, it is currently unknown whether the device possesses active, old or invalid client credentials (for example, when new client credentials have been created or client credentials have been imported).
- **Rejected**
  The device last attempted to authenticate itself using invalid client credentials.

Server Credential 1

Server Credential 1 was successfully sent to the device.

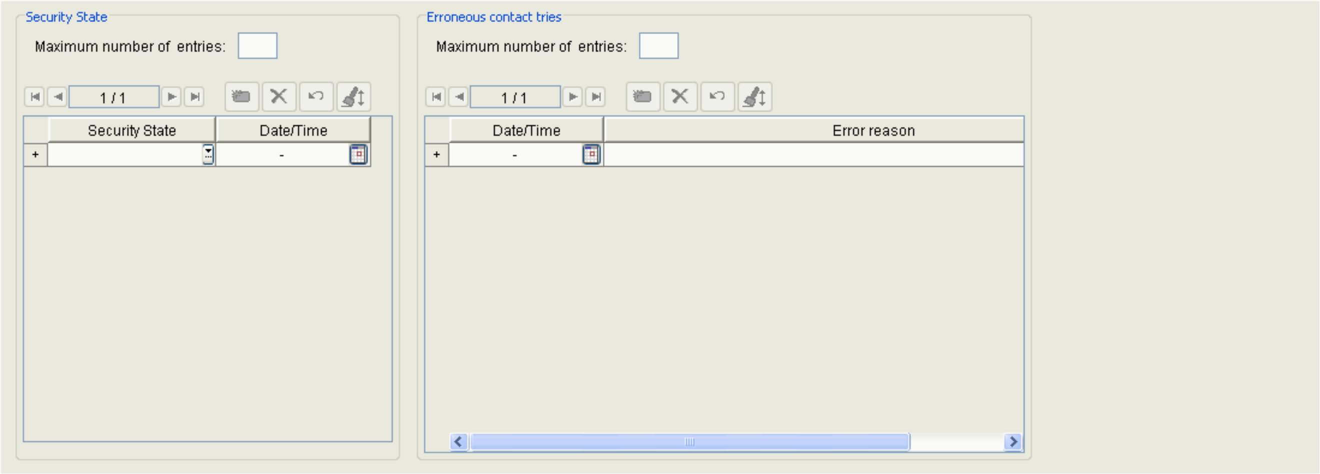
Server Credential 2

Server Credential 2 was successfully sent to the device.

7.6.4.5 "Security State Protocol" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "Security State Protocol" Tab

Changes to the security mode are logged here for the selected IP Devices.



Security State

Maximum number of entries:

Maximum number of security log entries to be displayed.

Security State

Shows the security state of the IP Device at a given time.

Date/Time

Displays the time at which the IP Device had a particular security state.

Erroneous contact tries

Maximum number of entries:

Maximum number of security log entries to be displayed.

Value range: **0** - **100** for devices in default mode, **1** - **100** for devices in secure mode.

Date/Time

Displays the time of the contact try.

Error reason

Error message.

Possible messages:

Error Message	Description
DLS internal authentication failure (no transition)	During the bootstrapping process, the DLS recognized an unknown sequence of messages (e. g. an unexpected message, deviating from the expected one) and cancelled the contact attempt for security reasons.
Workpoint with given id could not be found.	The IP device is not known to the DLS. Possibly an internal DLS error (database or configuration problem).
Encountered invalid PIN	The bootstrapping PIN contains illegal characters or exceeds the defined length.
TAN Verification can only be performed if TAN is required.	The IP Device has sent a TAN, but the current configuration does not require one, thus the TAN cannot be verified.
Verification of DlsObjWorkpointBase failed.	Internal DLS error.
Error while updating DlsObjWorkpointBase.	Internal DLS error.
Invalid security state.	The message traffic does not conform to the current DLS security state (e. g. wrong sequence of messages, modified configuration or error).
Invalid security transition.	The message traffic does not conform to the current DLS security state (e. g. wrong sequence of messages, modified configuration or error).
Error while generating new client certificate.	Internal DLS error during the creation and distribution of e new client certificate.
Fatal server error. See log file for additional information.	Fatal internal DLS error. **Troubleshooting:** For further information, see `..\DeploymentService\Tomcat5\webapps\DeploymentService\log\dlslog.txt`
An active dls server ca could not be found.	Internal DLS error because of a missing CA certificate.
Active server ca is corrupt.	Internal DLS error because of a wrong or corrput CA certificate.

Error Message	Description
An additional dls server ca could not be found.	Internal DLS error because of a missing second CA certificate.
An additional dls server ca already exists.	Internal DLS configuration error.
Additional server ca is corrupt.	Internal DLS error because of a wrong or corrupt second CA certificate.
An item with name mac-addr is missing in item list.	IP Device message contains no device ID (attribute name: mac-addr).
AES encoding failed due to an internal error.	Evaluation of the message by AES failed due to a DLS internal error.
Client must provide a certificate.	The IP Device must provide a client certificate.
Client certificate with invalid signature.	The IP Device has sent an invalid or corrupt certificate.
Client certificate invalid.	The IP Device certificate is invalid due to unknown causes (e. g. expired etc.).
Client ca not found or corrupt.	Internal DLS error because of a missing or corrupt client CA certificate.
DLS internal authentication failure.	Internal DLS error due to problems with the authentification (e. g. invalid or corrupt certificate key, internal certificate problems).
Export of CAs could not be performed.	Internal DLS configuration error: export of the CA certificate could not be executed.
Import of CAs could not be performed.	Internal DLS configuration error: import of the CA certificate could not be executed.
Client cert state is invalid.	Internal DLS configuration error: client certificate status is invalid.
String is not a X509 PEM.	Internal DLS configuration error: characters do not comply to the X509 rules.
DCMP URI is not valid.	Internal DLS configuration error: DCMP URI is invalid.
Invalid dcmp state.	Internal DLS configuration error: DCMP state is invalid.
Invalid dcmp transition.	Internal DLS configuration error: DCMP transition is invalid.
client certificate not accepted by device	The IP Device has not accepted the new client certificate sent by the DLS.

Error Message	Description
device is blocked	Any communication with this IP Device is blocked for security reasons.
device must use secure port	The IP Device must use the secure port (e. g. 18444) instead of the standard port (e. g. 18443.
wrong TAN from device	A TAN has been requested from the IP Device once or multiple times, but even after a defined number of repetitions no valid TAN has been sent. For security reasons, the IP Device is blocked.
No DLS license	No DLS license exists.
licenses exceeded	The number of DLS licenses is exceeded.
unexpected solicited message from workpoint	An (accidental) request message has been sent from the IP Device to the DLS, but was not expected there (no preceding contact-me from the DLS).
empty items list but items expected	The message list is empty, though the DLS expects multiple items.
timeout during read items	Timeout during reading data from a IP Device.
synchronisation exception	Internal DLS synchronisation error.
missing e164	The E.164 has been expected by the DLS, but the IP Device has not sent it.
missing items	The expected items are not contained in the message list.
try later	HFA mobility logoff.
mobility save disabled	HFA mobility.

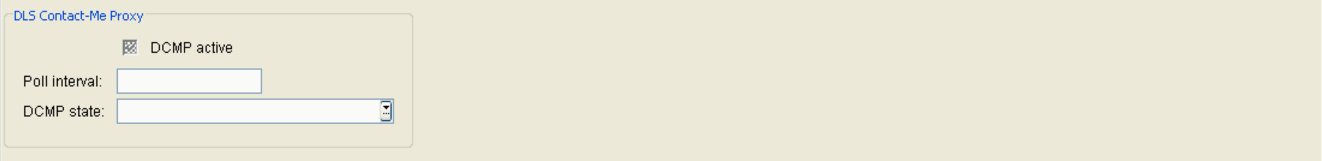
7.6.4.6 "DCMP" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "DCMP" Tab

The DLS Contact-Me Proxy (DCMP) can communicate with the DLS over a firewall or NAT (Network Address Translation) and, if necessary, can perform routing between devices and a DLS in front of the firewall. The devices poll the DCMP regularly. If there are messages on the DLS, the DCMP creates a connection between the device and the DLS.

A DCMP proxy can be assigned as specific location and, therefore, a specific IP address range; see Section 6.8.2, ""DCMP" Tab".

The values in this mask are for display only and cannot be modified.



DLS Contact-Me Proxy

DCMP active

If this checkbox is activated, the device uses the DCMP to communicate with the DLS and polls it regularly. This requires global DCMP activation, see **Administration** > **Workpoint Interface Configuration** > **"DCMP" Tab**.

Poll Interval:

Specifies the intervals at which the device polls the DCMP.

DCMP state:

Provides information about the communication between the device and the DCMP.

Possible values:

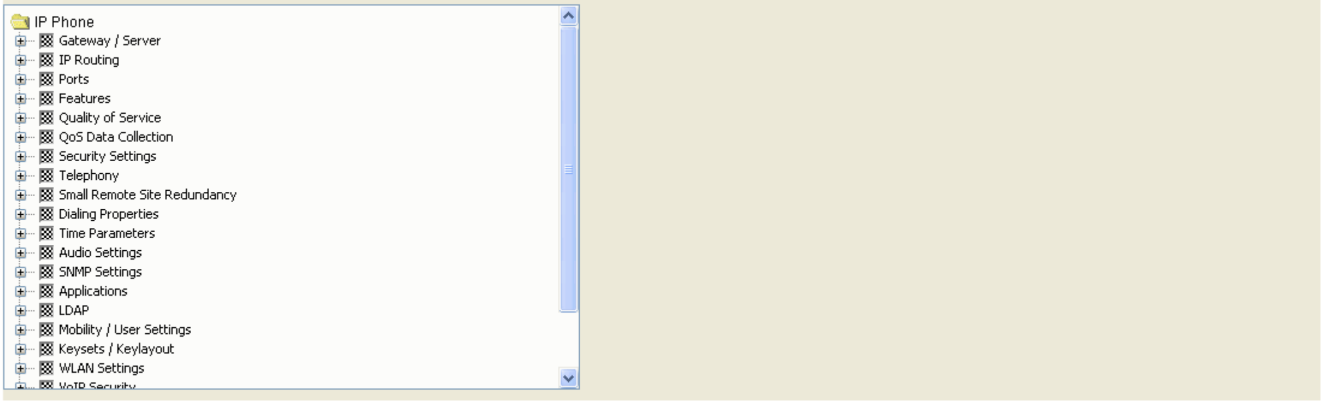
- **Enabled**
  The device is in DCMP mode, that is, the DLS contacts the device via the DCMP server.
- **Disabled**
  The device is not in DCMP mode, that is, the DLS contacts the device directly.
- **Refused**
  The device denies DCMP mode (for example, when it is technically unable to operate in DCMP mode).
- **Outdated**
  DCMP data on the DLS has changed and must be communicated to the device.

- **Disable in progress**
  DCMP for this device is deactivated in the DLS and the modified configuration must be communicated to the device.

7.6.4.7 "Autoconfig. IP Phone" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "Autoconfig. IP Phone" Tab

This displays the attributes that must be sent to the IP Device for autoconfiguration (Plug&Play) on devices not yet connected (= virtual devices). The individual checkmarks are automatically set once an attribute is configured and/or a profile is entered. But also possible the administrator can check individual checkmarks; if so, default values for the checked parameters are sent to the IP Device.



- IP Phone
  - ▨ Gateway / Server
  - ▨ IP Routing
  - ▨ Ports
  - ▨ Features
  - ▨ Quality of Service
  - ▨ QoS Data Collection
  - ▨ Security Settings
  - ▨ Telephony
  - ▨ Small Remote Site Redundancy
  - ▨ Dialing Properties
  - ▨ Time Parameters
  - ▨ Audio Settings
  - ▨ SNMP Settings
  - ▨ Applications
  - ▨ LDAP
  - ▨ Mobility / User Settings
  - ▨ Keysets / Keylayout
  - ▨ WLAN Settings
  - ▨ VoIP Security

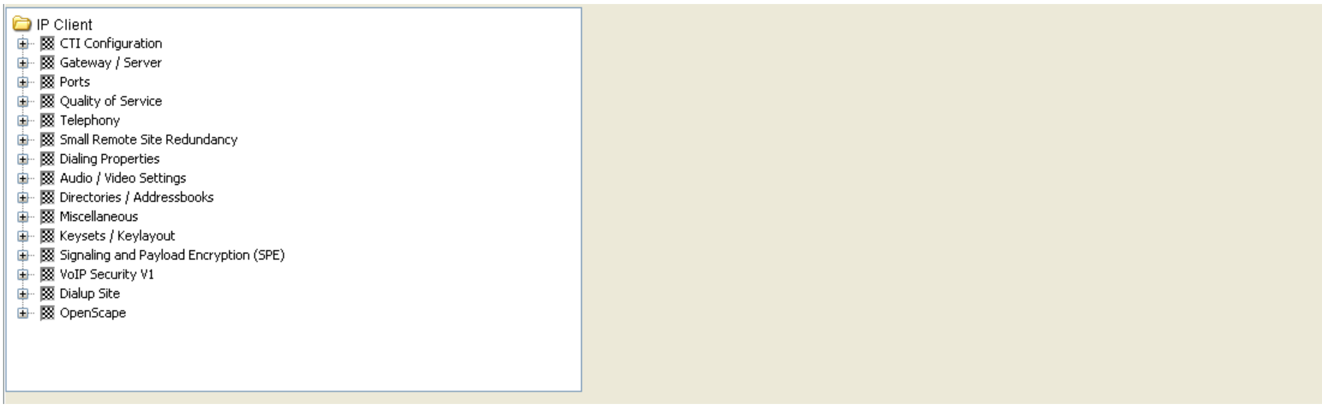
Reset

Resets all fields to inactive.

7.6.4.8 "Autoconfig. IP Client" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "Autoconfig. IP Client" Tab

This displays the attributes that must be sent to the IP Device for autoconfiguration (Plug&Play) on IP clients not yet connected (= virtual devices). The individual checkmarks are automatically set once an attribute is configured and/or a profile is entered. But also possible the administrator can check individual checkmarks; if so, default values for the checked parameters are sent to the IP Device.



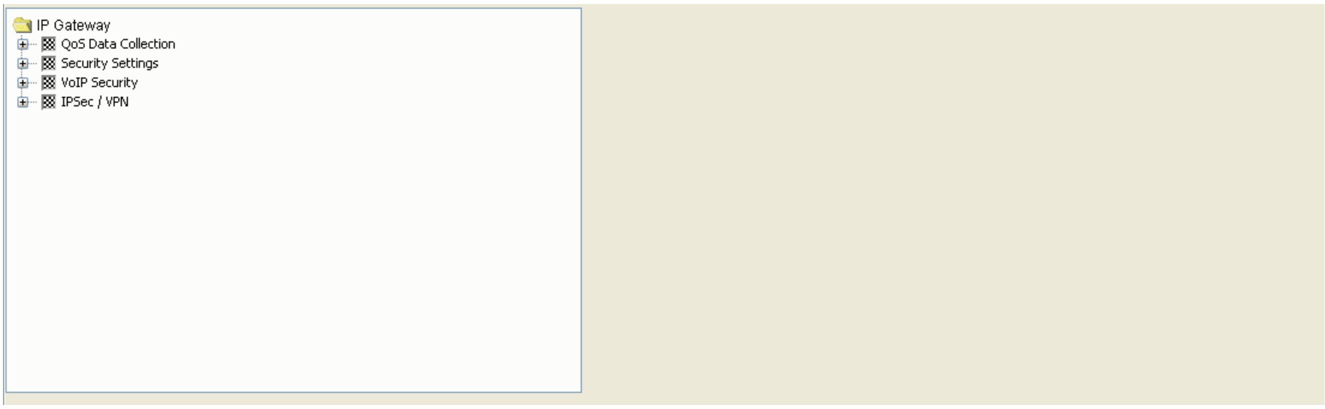
Reset

Resets all fields to inactive.

7.6.4.9 "Autoconfig. IP Gateway" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "Autoconfig. IP Gateway" Tab

This displays the attributes that must be sent to the IP device for autoconfiguration (Plug&Play) on IP gateways not yet connected (= virtual devices). The individual checkmarks are automatically set once an attribute is configured and/or a profile is entered. But also possible the administrator can check individual checkmarks; if so, default values for the checked parameters are sent to the IP Device.

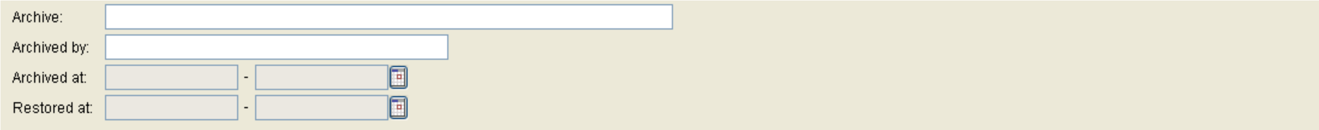


Reset

Resets all fields to inactive.

7.6.4.10 "Archives Data" Tab

Call: Main Menu > IP Devices > IP Device Management > IP Device Configuration > "Archives Data" Tab



Archive:	
Archived by:	
Archived at:	-
Restored at:	-

Archive:

Path for the ZIP archive file on the DLS system.

Archived by

Name of the DLS user who created the archive.

Archived at

Date and time of the archive.

Restored at

Date and time of the archive restore.

8 Mobile Users

Call: Main Menu > Mobile Users

This menu item consists of the following areas:

- SIP Mobile User Configuration
- SIP Mobile User Interaction
- User Data Administration
- Mobility Statistics
- Mobility Statistics Configuration

The **Mobile Users** area is for displaying and modifying Mobile User parameters. For an introduction to mobility, see Section 3.7, "DLS Mobility - General Information".

> ⚠ Changes to data in workpoint configuration masks created with templates are not automatically applied to these templates.
> These changes must be manually saved to the template (Section 15.4, "Editing Templates").

> ℹ A workpoint can only be configured after successful registration at the DLS. The workpoint must be aware of the corresponding DLS IP address for registration. Registration at the DLS is achieved by:
>
> - reading out workpoint data via the DLS, see Section 7.4.4, "Scan IP Devices" and by
> - plugging the LAN connector or power supply into the workpoint.

8.1 SIP Mobile User Configuration

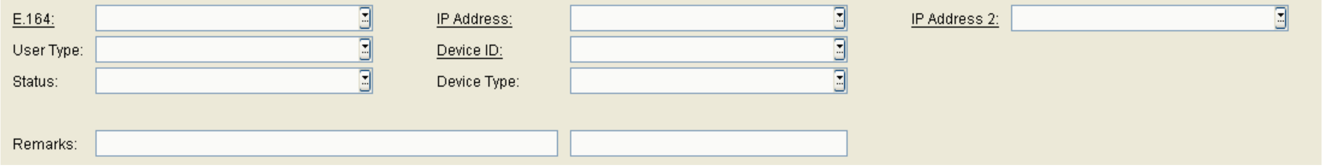
Call: Main Menu > Mobile Users > SIP Mobile User Configuration

This menu consists of the following submenus:

- Gateway/Server
- IP Routing
- Features
- Quality of Service
- Security Settings
- Telephony
- Dialing Properties
- Time Parameters
- Audio Settings
- Applications
- LDAP
- User Settings
- SIP Mobility
- Keysets/Keylayout
- Signaling and Payload Encryption (SPE)
- Miscellaneous

General Data

This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP phones. The base data associated with the IP phones found is displayed in **Object** view (no changes possible except under **Remarks**).



You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.

All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only **those** IP phones that correspond to the specified device type and that also belong to the specified IP address range are selected.

E.164:

Complete E.164 phone number (Mobility ID or basic user phone number).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

User Type:

Displays the type of data used.

Possible options:

- **Mobility enabled Device**
  Mobility Phone data.
- **Mobile User**
  Mobile User data.

For more information on mobility, see Section 3.7, "DLS Mobility - General Information".

Status:

Displays mobility status.

Possible options:

- **Mobile User logged on**
 Mobile User data: a Mobile User is logged on.
- **Mobile User logged off**
 Mobile User data: no Mobile User is logged on.
- **Device available for Mobile User**
 data: no Mobility Phone Mobile User is logged on to the Mobility Phone.
- **Device used by Mobile User**
 data: a Mobility Phone Mobile User is logged on to the Mobility Phone.

For more information on mobility, see Section 3.7, "DLS Mobility - General Information".

IP Address:

IP address of the IP phone.

Example: **192.117.1.193**

The value is read-only at this location.

Device ID:

Physical MAC address of the IP phone.

Example: **00:0E:A6:85:71:80**

Device Type:

Device type of the IP phone.

You can view all IP phone types supported by the DLS in Section 3.4, "IP Devices / versions supported".

Example: **optiPoint 410 standard**

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

This is a read only value.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP phones that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Starts a job for transmitting configuration changes to the selected object. For more information, see Section 15.1, "First Steps: Changing IP Device Parameters". In Templates view, parameters are saved in the selected templates. For more information, see Section 15.4, "Editing Templates".

Discard

The modifications made are not transmitted to the selected object and are deleted from the input mask.

Refresh

The parameters are reloaded from the database.

Get

Loads a template that has already been saved. For more information, see Section 15.4, "Editing Templates".

Rename

Changes the name of a saved template. For more information, see Section 15.4, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.4, "Editing Templates".

8.1.1 Gateway/Server

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server

This area features the following components:

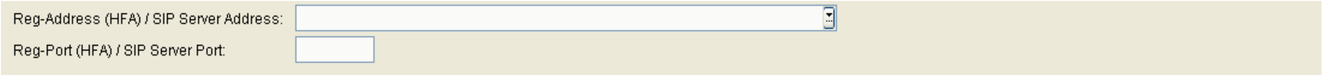
- General Data
- Possible Action Buttons
- "Gateway (HFA) / SIP Server" Tab
- "SIP Terminal Settings" Tab
- "SIP Registering 1" Tab
- "SIP Registering 2" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.1.1 "Gateway (HFA) / SIP Server" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server > "Gateway (HFA) / SIP Server" Tab



Reg-Address (HFA) / SIP Server Address:

Reg-Port (HFA) / SIP Server Port:

Reg-Address (HFA) / SIP Server Address:

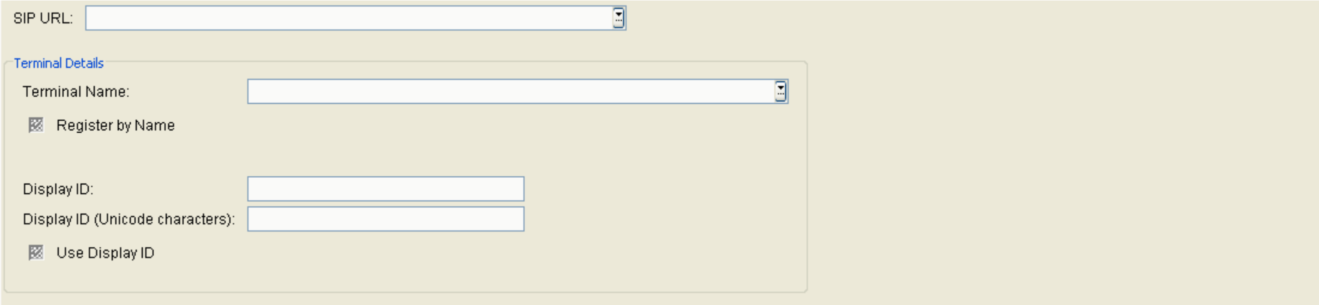
IP address or host name of the PBX, gateway or SIP server used for operating the workpoint.

Reg-Port (HFA) / SIP Server Port:

Port number of the PBX, gateway or SIP server used for operating the workpoint.

8.1.1.2 "SIP Terminal Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server > "SIP Terminal Settings" Tab



SIP URL:

Terminal Details

Terminal Name:

☒ Register by Name

Display ID:

Display ID (Unicode characters):

☒ Use Display ID

SIP URL:

SIP address of the IP phone.

Format: **<SIP user ID>@<Domain>**.

Terminal Details

Terminal Name:

Name of the IP phone used as a synonym for the phone number during registration.

Only necessary if the **Register by Name** check box is selected and the registrar server is appropriately configured.

Register by Name

Check box for activating the function that sends the contents of the **Terminal Name** field as part of registration.

If the check box is not active, the contents of the **E.164 number** field are also sent in the course of registration.

Display ID:

Name of the IP phone as shown on the workpoint display.

Value range: max. 24 alphanumeric characters.

Display ID (Unicode characters):

Name of the IP phone in unicode characters as shown on the workpoint display.

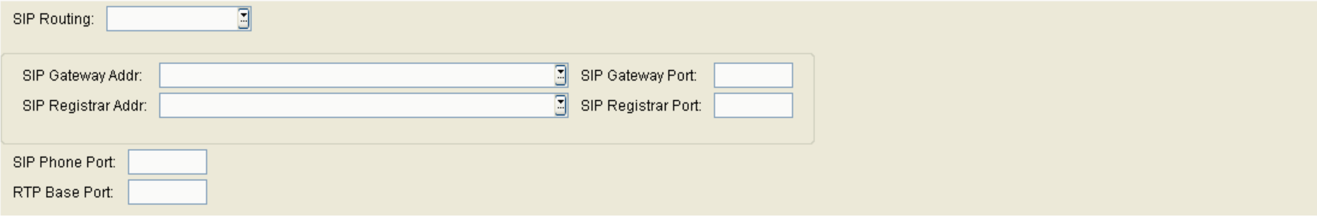
This option is only supported by OpenStage devices.

Use Display ID

If this check box is activated, the Display ID is shown on the workpoint.

8.1.1.3 "SIP Registering 1" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server > "SIP Registering 1" Tab



SIP Routing:

Possible options:

- **Gateway**
  A gateway is used for SIP routing.
- **Server**
  An SIP proxy is used for SIP routing.
- **Direct**

If **Direct** or **Gateway** is selected, no registration messages are sent. Registration messages are sent to the registrar server for the **Server** routing mode.

SIP Gateway Addr.

IP address of the gateway. This parameter is used when the **Gateway** mode is selected for SIP routing.

SIP Gateway Port:

Port number of the gateway. This parameter is used when the **Gateway** mode is selected for SIP routing.

SIP Registrar Addr:

IP address of the SIP registrar.

SIP Registrar Port:

Port number of the SIP Registrar.

SIP Phone Port:

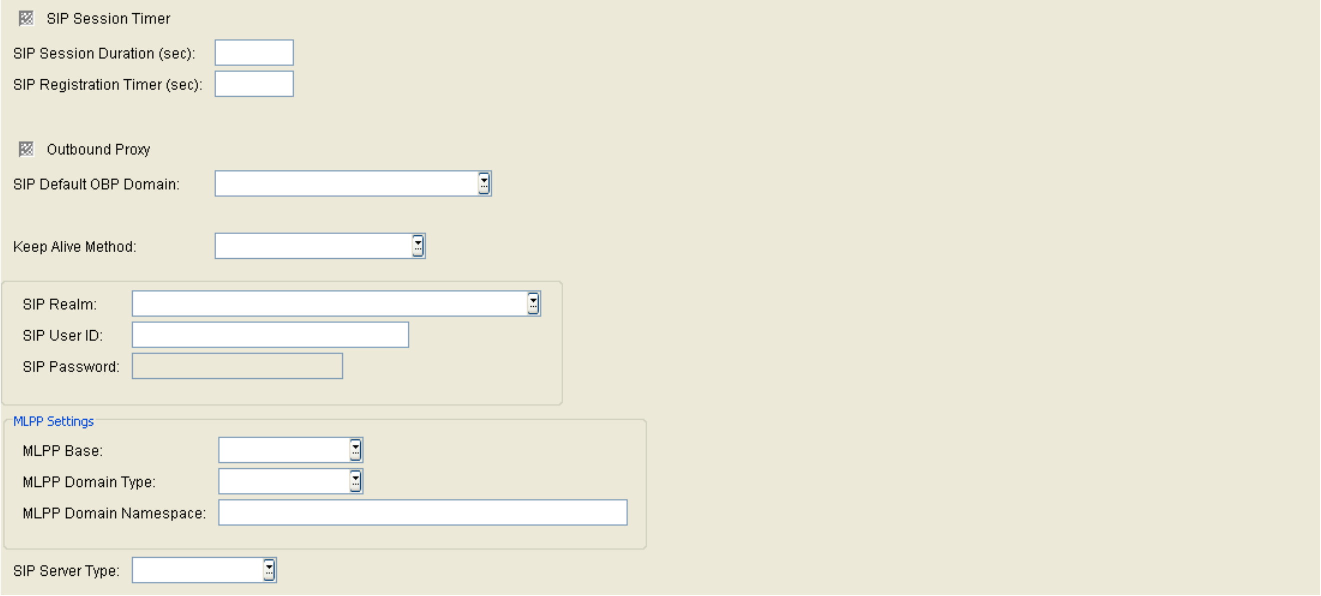
Port number of the IP phone.

RTP Base Port:

Base port number for RTP transport.

8.1.1.4 "SIP Registering 2" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server > "SIP Registering 2" Tab



SIP Session Timer

Check box for activating the SIP session timer. The timer is used to monitor the duration of an SIP session.

SIP Session Duration:

Highest duration in seconds for an SIP session.

Value range: **0** ... **3600** seconds.

SIP Registration Timer:

Time period for re-registration at the SIP server. Re-registration ensures that the SIP telephone remains logged on to the SIP server. It can also detect server connectivity problems.

Value range: **0** ... **4320** seconds.

Default: **0**

Outbound Proxy

Check box for activating an SIP proxy for outbound calls.

Together with **SIP Default OBP Domain** this check box controls outbound call routing on the basis of the number dialed or the user ID.

For more information, see Chapter 17, "Outbound Proxy".

SIP Default OBP Domain:

Together with **Outbound Proxy** this entry controls outbound call routing on the basis of the number dialed or the user ID.

For more information, see Chapter 17, "Outbound Proxy".

Keep Alive Method:

Possible options:

- **Sequence**
- **CRLF**

SIP Realm:

SIP range in which the workpoint is operated. SIP realm is used to identify the telephone at the SIP server.

SIP User ID:

The user ID is the first part of the SIP URL.

SIP Password:

Password required for accessing the SIP server.

MLPP Settings

MLPP Base

Possible options:

- **Local**
- **Server**

MLPP Domain Type

Specifies which resource priority namespace will be accepted from a fixed list.

Possible options:

- **dsn**
  dsn-000000
- **uc**
  uc-000000
- **dsn+uc**
- **Other domain**

MLPP Domain Namespace

Specifies an ASCII string for a single resource priority namespace which will be accepted.

Alphanumerical characters and the following special charakters are allowed: -!%*_+` "~

A "." is not allowed.

SIP Server Type:

Possible options:

- **Broadsoft**
- **OpenScape Voice**
- **Sylantro**
- **other**
- **HiQ8000**
- **Genesys**

8.1.2 IP Routing

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > IP Routing

This area features the following components:

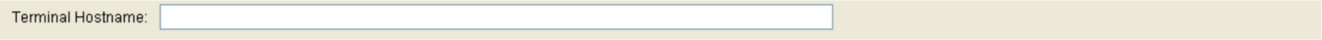
- General Data
- Possible Action Buttons
- "DNS Server" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.2.1 "DNS Server" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > IP Routing > "DNS Server" Tab



Terminal Hostname:

Terminal Hostname:

Host name of the terminal.

Permitted characters: letters, digits, hyphens, underscores, and periods; case-sensitive; maximum length: 63 characters.

The value is read-only if it was dynamically assigned with DHCP.

8.1.3 Features

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features

This area features the following components:

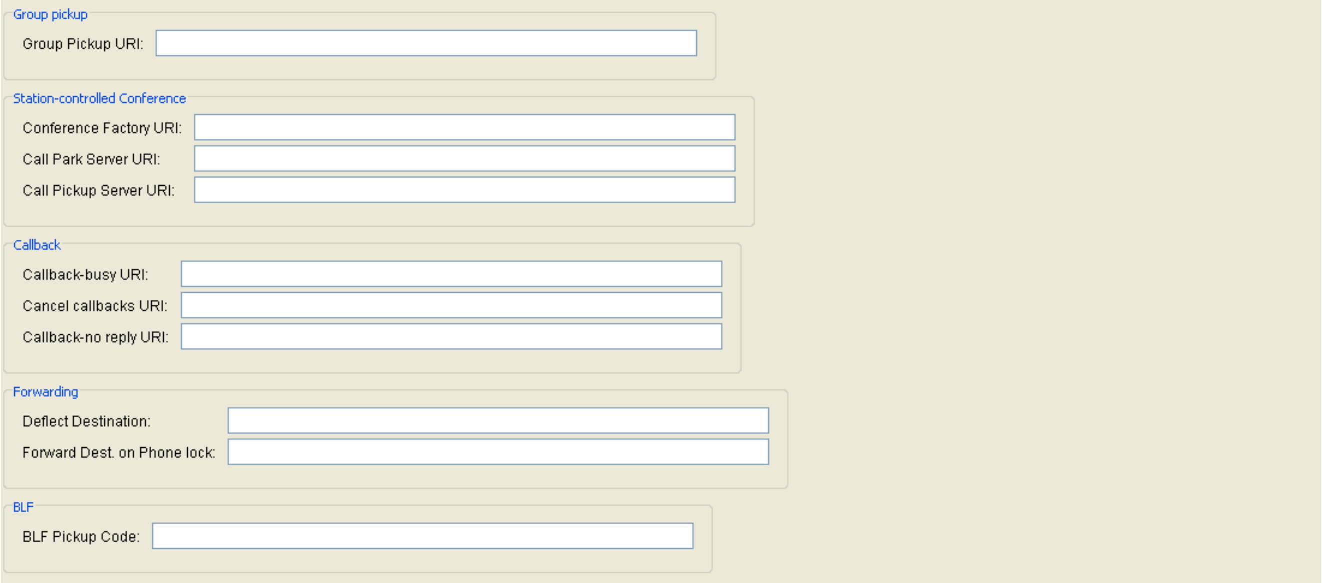
- General Data
- Possible Action Buttons
- "Feature Settings 1" Tab
- "Feature Settings 2" Tab
- "Call related User Settings" Tab
- "Availability" Tab
- "Server based Features" Tab
- "Dialplan" Tab
- "Ringer Melody / Tone" Tab
- "Call Forwarding" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.3.1 "Feature Settings 1" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Feature Settings 1" Tab



Group pick-up

Group Pickup URI:

URI of the group pickup.

Only available in SIP workpoints.

Station-controlled Conference

Conference Factory URI:

URI for setting up conference calls.

Only available in SIP workpoints.

Call Park Server URI:

URI of the server for parking calls.

Only available in SIP workpoints.

Call Pickup Server URI:

URI of the server for group pickup.

Only available in SIP workpoints.

Callback

Callback-busy

URI of the server that controls the "Callback-busy" feature.

Cancel callbacks URI:

URI of the server that controls the "Cancel callbacks" feature.

Callback-no reply URI

URI of the server that controls the "Callback-no reply" feature.

Deflection

Deflect Destination:

Destination number for call forwarding.

Only available in SIP workpoints.

Forward Dest. on Phone lock:

Destination number for forwarding in the case of a call to a locked workpoint.

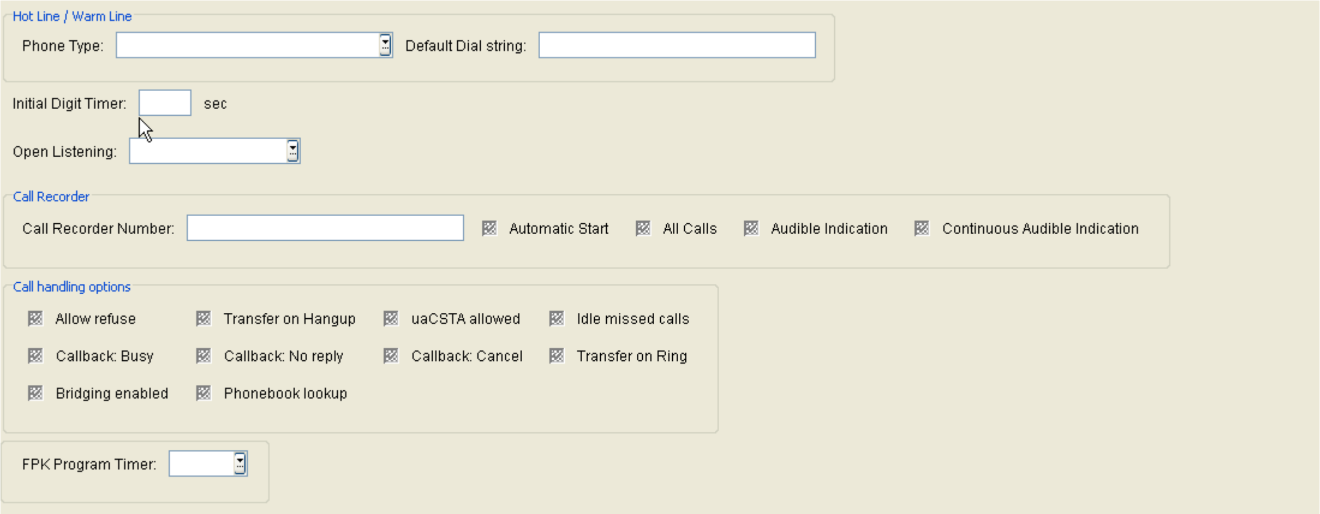
BLF

BLF Pickup Code:

BLF Pickup Code.

8.1.3.2 "Feature Settings 2" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Feature Settings 2" Tab



Hot Line / Warm Line

Phone Type: Default Dial string:

Initial Digit Timer: sec

Open Listening:

Call Recorder

Call Recorder Number: ▨ Automatic Start ▨ All Calls ▨ Audible Indication ▨ Continuous Audible Indication

Call handling options

▨ Allow refuse ▨ Transfer on Hangup ▨ uaCSTA allowed ▨ Idle missed calls

▨ Callback: Busy ▨ Callback: No reply ▨ Callback: Cancel ▨ Transfer on Ring

▨ Bridging enabled ▨ Phonebook lookup

FPK Program Timer:

Hot Line/Warm Line

Phone Type:

Time delay for the functions "Hotline" and "Warmline"

Possible options:

- **Ordinary**
- **Hot Line**
- **Warm Line**

Only available in SIP workpoints.

Default Dial String:

Destination number for the functions "Hotline" and "Warmline".

Only available in SIP workpoints.

Initial Digit Timer:

Waiting time in seconds for a dialed digit after the dial tone starts.

Only available in SIP workpoints.

Open Listening

Open Listening settings.

Possible options:

- **Standard Mode**
  To switch to Open Listening mode, the user must press and hold the Open Listening key while returning the handset to the cradle.
- **US Mode**
  To switch to Open Listening mode, the user must first press the Open Listening key and then return the handset to the cradle.

Call Recorder

Recording Mode

Determines the behaviour of the call recording.

Possible options:
- **Manual**
- **Auto Start**
- **All Calls**

Audible Notification

Select the tone for audible notification.

Possible options:
- **Off**
- **On / Single Shot**
- **Continuous**

Call Recorder Number:

Phone number of the call recorder.

Automatic Start

When activated, call recording is started automatically, with incoming calls and outgoing calls. The user can switch the recording on or off during a conversation.

The checkbox is effective only if voice recording is activated on the phone.

All Calls

When activated, call recording is started automatically, with incoming calls and outgoing calls. The user can not control the recording.

The checkbox is effective only if voice recording is activated on the phone.

Audible Indication

A beep signals to the called party that the phone call is being recorded.

Continuous Audible Indication

A continuous audible indication signals to the called party that the phone call is being recorded.

The checkbox is effective only when **Audible Indication** is activated.

Call handling options

Allow refuse

If this check box is active, the user can reject an incoming call.

Only available in SIP workpoints.

Transfer on Hangup

If this check box is active, the user can transfer a call between an active participant and a participant that is on hold.

Only available in SIP workpoints.

uaCSTA allowed

If this check box is active, telephony applications which support the uaCSTA standard can access the phone.

Idle missed calls

If this check box is active, an indication for missed calls will be shown on the display.

Callback: Busy

If this check box is active, the user can register a callback request when the call target is busy.

Only available in SIP workpoints.

Callback: No reply

If this check box is active, the user can register a callback request when the callee does not respond.

Only available in SIP workpoints.

Callback: Cancel

If this check box is active, the user can cancel callback requests.

Transfer on Ring

If this check box is active, the user can transfer a call to a third participant before he responds.

Only available in SIP workpoints.

Bridging enabled

Enables or disables bridging.

Only available in SIP workpoints.

Phonebook lookup

Checkbox for activating the "Phonebook lookup" feature.

FPK Program Timer

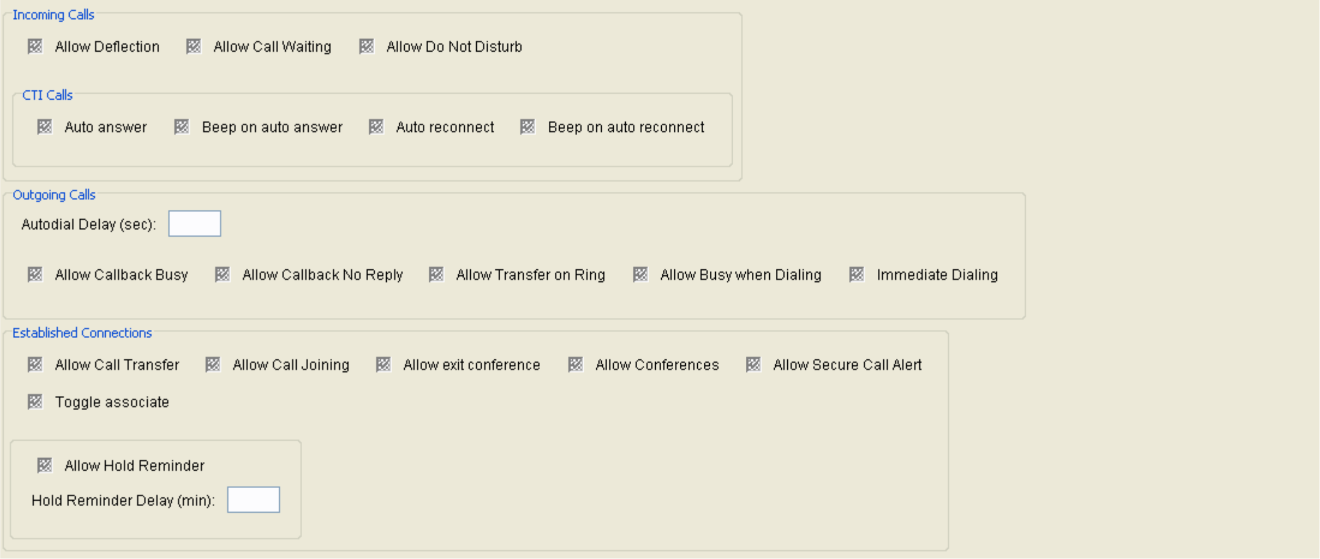
When "Off" is selected, the free programmable keys (FPKs) will not change to programming mode on long press.

Possible options:

- **On**
- **Off**

8.1.3.3 "Call related User Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Call related User Settings" Tab



Incoming Calls

▨ Allow Deflection ▨ Allow Call Waiting ▨ Allow Do Not Disturb

CTI Calls

▨ Auto answer ▨ Beep on auto answer ▨ Auto reconnect ▨ Beep on auto reconnect

Outgoing Calls

Autodial Delay (sec):

▨ Allow Callback Busy ▨ Allow Callback No Reply ▨ Allow Transfer on Ring ▨ Allow Busy when Dialing ▨ Immediate Dialing

Established Connections

▨ Allow Call Transfer ▨ Allow Call Joining ▨ Allow exit conference ▨ Allow Conferences ▨ Allow Secure Call Alert

▨ Toggle associate

▨ Allow Hold Reminder

Hold Reminder Delay (min):

Incoming calls

Allow Deflection

Check box for activating Call Deflection.

Allow Call Waiting

Check box for activating Call Waiting.

Allow Do Not Disturb

Check box for activating Do Not Disturb.

CTI Calls

Auto answer

Check box for activating Auto Answer.

Only available in SIP workpoints.

Beep on auto answer

Check box for activating a confirmation beep on Auto Answer.

Only available in SIP workpoints.

Auto reconnect

Check box for activating automatic reconnection of a parked call.

Only available in SIP workpoints.

Beep on auto reconnect

Check box for activating a confirmation beep on reconnection of a parked call.

Only available in SIP workpoints.

Immediate Dialing

If this check box is active, immediate dialing is executed as soon as the entered string matches a dial plan entry.

Only available in SIP workpoints.

Outgoing calls

Autodialing delay (sec):

Delay for Automatic Dialing in seconds.

Allow Callback Busy

Check box for activating Callback on Busy.

Allow Callback No Reply

Check box for activating Callback on No Reply.

Allow Transfer on Ring

Check box for activating Transfer on Ring.

Allow Busy when Dialing

Check box for activating Busy when Dialing.

Allow Immediate Dialing

Check box for activating the **Hot Keypad Dialing** feature.

Established Connections

Allow Call Transfer

Check box for activating Call Transfer.

Allow Call Joining

Check box for activating Call Joining.

Allow exit conference

Check box for activating Exit Conference.

Allow Conferences

Check box for activating Conferences.

Allow Secure Call Alert

If the handling of secure calls is enabled on the phone and this check box is activated, a popup window and an alert tone will notify the user when an insecure (unencrypted) call comes in.

Toggle associate

Checkbox for activating associated toggle.

Allow Hold Reminder

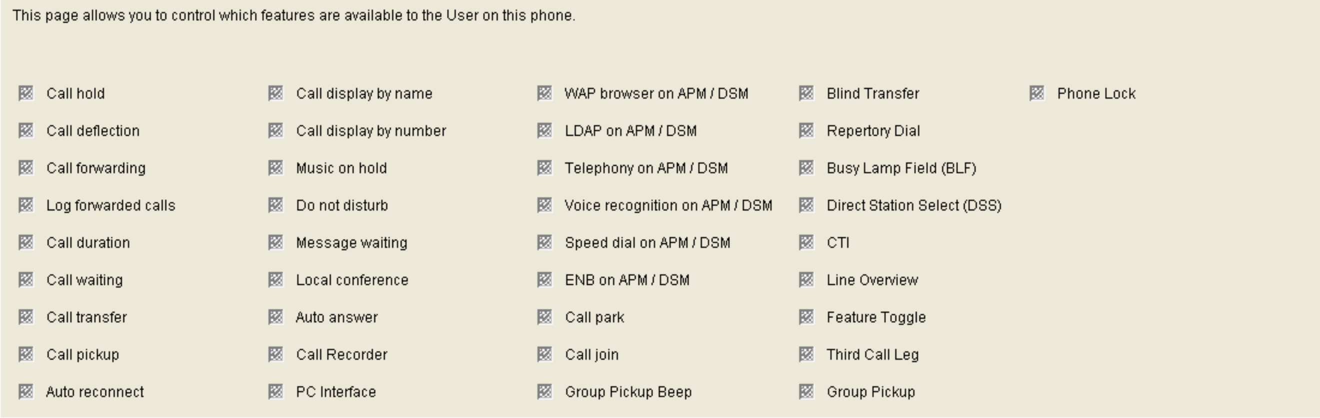
Check box for activating the Hold Reminder.

Hold Reminder Delay (min):

Delay for the Hold Reminder in minutes.

8.1.3.4 "Availability" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Availability" Tab



This page allows you to control which features are available to the User on this phone.

- ☑ Call hold
- ☑ Call deflection
- ☑ Call forwarding
- ☑ Log forwarded calls
- ☑ Call duration
- ☑ Call waiting
- ☑ Call transfer
- ☑ Call pickup
- ☑ Auto reconnect
- ☑ Call display by name
- ☑ Call display by number
- ☑ Music on hold
- ☑ Do not disturb
- ☑ Message waiting
- ☑ Local conference
- ☑ Auto answer
- ☑ Call Recorder
- ☑ PC Interface
- ☑ WAP browser on APM / DSM
- ☑ LDAP on APM / DSM
- ☑ Telephony on APM / DSM
- ☑ Voice recognition on APM / DSM
- ☑ Speed dial on APM / DSM
- ☑ ENB on APM / DSM
- ☑ Call park
- ☑ Call join
- ☑ Group Pickup Beep
- ☑ Blind Transfer
- ☑ Repertory Dial
- ☑ Busy Lamp Field (BLF)
- ☑ Direct Station Select (DSS)
- ☑ CTI
- ☑ Line Overview
- ☑ Feature Toggle
- ☑ Third Call Leg
- ☑ Group Pickup
- ☑ Phone Lock

Call Hold

Check box for activating the function for placing calls on hold.

Area of validity: Only applies to SIP workpoints.

Call deflection

Check box for activating manual forwarding for incoming calls (CD).

Only available in SIP workpoints.

Call forwarding

Check box for activating automatic call forwarding (CF).

Only available in SIP workpoints.

Log forwarded calls

Check box for activating logging for forwarded calls.

Only available in SIP workpoints.

Call duration

Check box for activating the function for displaying the call duration.

Only available in SIP workpoints.

Call waiting

Check box for activating visual and/or acoustic alerting for waiting calls (CW).

Only available in SIP workpoints.

Call transfer

Check box for activating the function for transferring calls (ECT).

Only available in SIP workpoints.

Call pickup

Check box for activating the function for picking up parked calls.

Only available in SIP workpoints.

Auto reconnect

Check box for activating the auto reconnect feature.

Only available in SIP workpoints.

Call display by number

Switch for activating call number display at the workpoint.

Only available in SIP workpoints.

Call display by name

Switch for activating caller name display at the workpoint.

Only available in SIP workpoints.

Music on hold

Check box for activating music on hold for held and parked calls.

Only available in SIP workpoints.

Do not disturb

Check box for activating the do-not-disturb function (optical alerting and ring only).

Only available in SIP workpoints.

Message waiting

Check box for activating alerting for waiting messages (MWI).

Only available in SIP workpoints.

Local conference

Check box for activating the function for setting up a local conference.

Only available in SIP workpoints.

Auto answer

Check box for activating auto answer.

Only available in SIP workpoints.

Call recording

Check box for activating call recording.

PC Interface

Check box for activating the PC interface.

WAP browser on APM/DSM

Check box for activating the WAP browser on the optiPoint application module/display module.

Only available in SIP workpoints.

LDAP on APM/DSM

Check box for activating the LDAP function on the optiPoint application module/display module.

Only available in SIP workpoints.

Telephony on APM/DSM

Check box for activating the telephony function on the optiPoint application module/display module.

Only available in SIP workpoints.

Voice recognition on APM/DSM

Check box for activating the voice recognition function (voice dialing) on the optiPoint application module/display module.

Only available in SIP workpoints.

Speed dial on APM/DSM

Check box for activating the speed-dialing function on the optiPoint application module/display module with a Java midlet.

Only available in SIP workpoints.

ENB on APM/DSM

Check box for activating the electronic notebook on the optiPoint application module/display module.

Only available in SIP workpoints.

Call park

Check box for activating the function for parking calls.

Only available in SIP workpoints.

Call join

Check box for activating the function for joining calls.

Only available in SIP workpoints.

Group Pickup Beep

Check box for activating the "Group Pickup Beep" feature.

Blind Transfer

Checkbox for activating the feature "Blind Transfer".

Repertory Dial

Checkbox for activating the feature "Repertory Dial".

Busy Lamp Flag (BLF)

Checkbox for activating the Busy Lamp Field (BLF).

Direct Station Select (DSS)

Checkbox for activating Direct Station Select (DSS).

CTI

Checkbox for activating CTI.

Line Overview

Checkbox for activating the "Line Overview"

Feature Toggle

Checkbox for activating the feature "Feature Toggle".

Third Call Leg

Checkbox for activating the feature "Third Call Leg".

Group Pickup

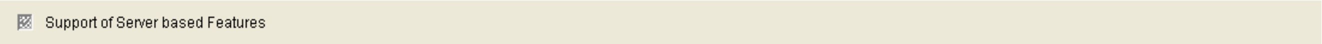
Checkbox for activating the feature "Group Pickup".

Phone Lock

Checkbox for activating the feature "Phone Lock".

8.1.3.5 "Server based Features" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Server based Features" Tab



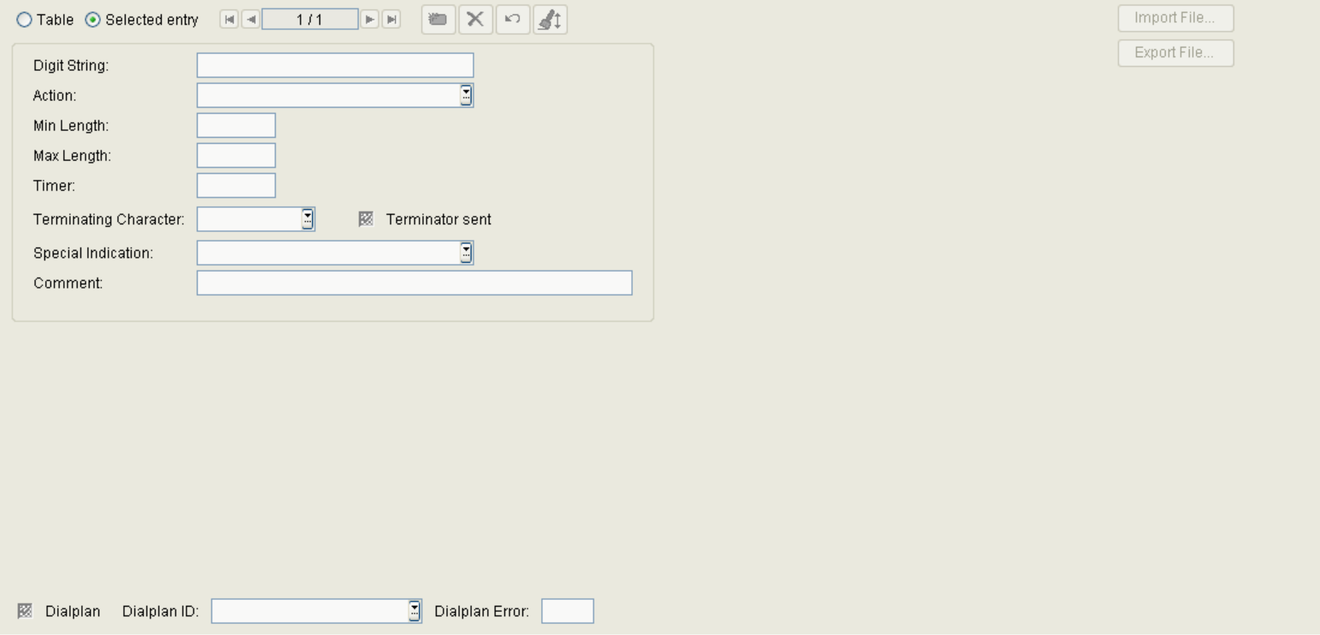
☒ Support of Server based Features

Support of Server based Features

If this check box is activated, server-based features on the device are enabled for the user.

8.1.3.6 "Dialplan" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Dialplan" Tab



Digit String:
Action:
Min Length:
Max Length:
Timer:
Terminating Character:
☒ Terminator sent
Special Indication:
Comment:

☒ Dialplan Dialplan ID: Dialplan Error:

Digit String

Digit String Digit string for executing this action.

Only available in SIP workpoints.

Action

Action executed for this digit string.

Possible options:

- **-C- Action for digits**
- **-CD1- Action for digits, dial tone**
- **-D1- Dial tone**
- **-S- Send digits**
- **SD1- Send digits, dial tone**

Only available in SIP workpoints.

Min Length

Minimum digit string length for digit string interpretation.

Only available in SIP workpoints.

Max Length

Maximum digit string length for digit string interpretation.

Only available in SIP workpoints.

Timer

Delay before the action is performed.

Value range: 1 ... 9 seconds.

Only available in SIP workpoints.

Terminating Character

Character that ends the digit string entered.

Possible options:

- **#**
- *****

Only available in SIP workpoints.

Special Indication

Possible options:

- **-E- emergency call**
- **-b- bypass**

Only available in SIP workpoints.

Terminator sent

Displays whether the terminating character is included in the digit string.

Dial Plan

Check box for activating the dial plan. The entries in the "Dialplan" Tab are interpreted if this check box is active.

Only available in SIP workpoints.

Dial Plan ID:

Name of the dial plan - must begin with a "!".

Value range: max. 14 alphanumeric characters.

Only available in SIP workpoints.

Dial Plan Error:

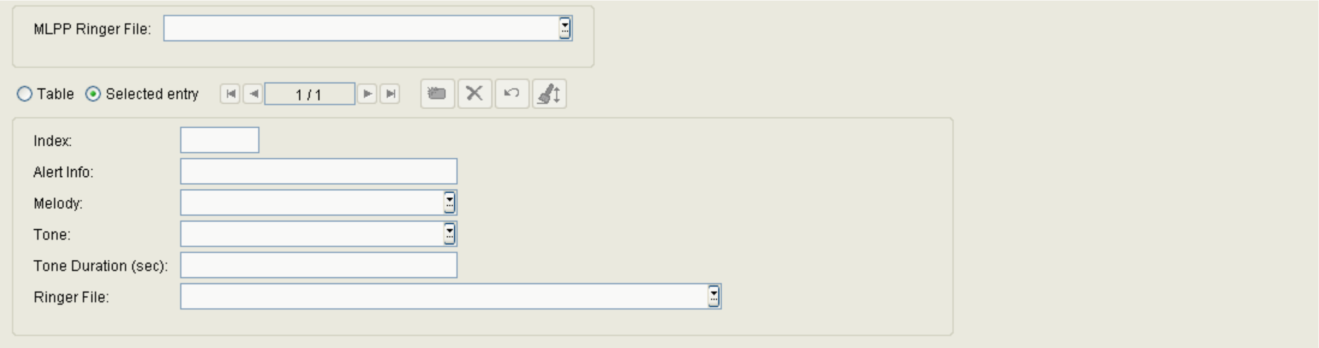
Specifies the dial plan entry that is faulty in the event of an error.

Value range: **1** ... **48**

Only available in SIP workpoints.

8.1.3.7 "Ringer Melody / Tone" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Ringer Melody / Tone" Tab



A template for **Ringer Melody / Tone** can be created by searching for an IP Device with entries in **Ringer Melody / Tone** (empty entries are allowed as well). Use the action **Copy to Template** to create a template. There must be 15 entries, which may be empty.
This template can be modified, saved, and applied.

MLPP Ringer File

Precedence ringer for priority calls.

Index

Specifies the sequence of the signaling entries.

This is automatically set. The field is provided for display only.

Alert Info

If the string specified here is identical with a special string which is sent to the phone in the SIP alert info header, the corresponding ringtone is used

Only available in SIP workpoints.

Melody

Type of ring melody.

Possible options: **Melody 1** ... **8**, **Melody off**.

Only available in SIP workpoints.

Tone

Ringtone sequence.

Possible options:

- **1**
  = 1 sec ON, 4 sec OFF
- **2**
  = 1 sec ON, 2 sec OFF
- **3**
  = 0,7 sec ON, 0,7 sec OFF, 0,7 sec ON, 3 sec OFF

Only available in SIP workpoints.

Tone Duration

Duration of the ringtone.

Value range: **1** ... **300** seconds.

Default: **60** seconds.

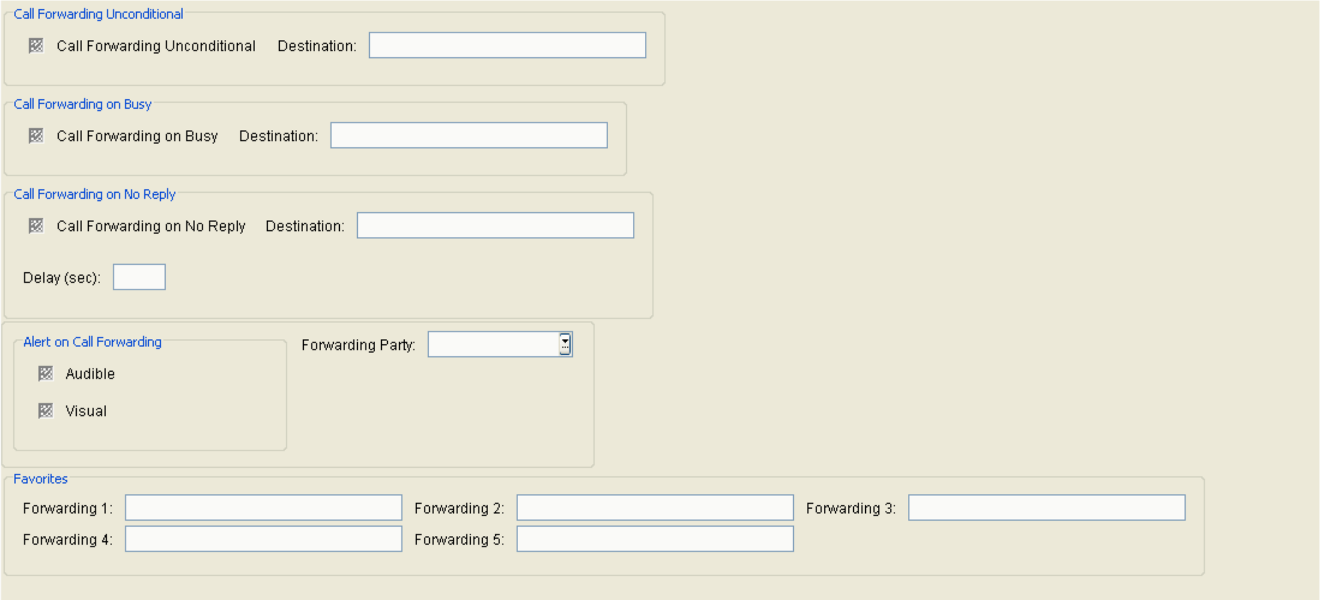
Only available in SIP workpoints.

Ringer File

Name of the audio file containing the ringtone.

8.1.3.8 "Call Forwarding" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Call Forwarding" Tab



Call Forwarding Unconditional

Call Forwarding Unconditional

Check box for activating Unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Call Forwarding on Busy

Call Forwarding on Busy

Check box for activating Call Forwarding n Busy.

Destination:

Call number of the Call Forwarding destination.

Call Forwarding on No Reply

Call Forwarding on No Reply:

Check box for activating Call Forwarding on No Reply.

Destination:

Call number of the Call Forwarding destination.

Delay (sec):

As soon as this time span has expired without the call being accepted, the call is forwarded.

Alert on Call Forwarding

Audible

Check box for activating an audible alert on the forwarding phone.

Visual

Check box for activating a visible alert on the forwarding phone.

Forwarding Party:

Select which forwarding party will be displayed when multiple forwarding is active.

Possible options:

- **Display first**
- **Display last**

Favorites

Forwarding 1:

Forwarding 2:

Forwarding 3:

Forwarding 4:

Forwarding 5:

8.1.4 Quality of Service

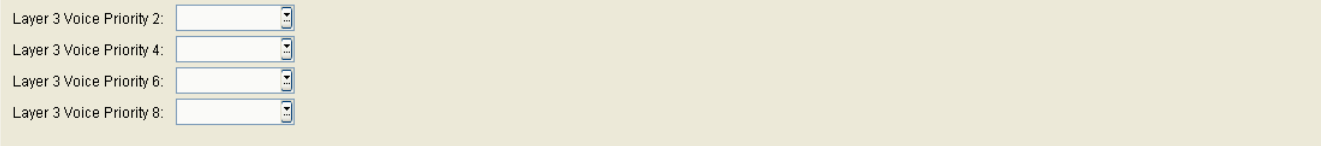
Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Quality of Service

This area features the following components:

- General Data
- Possible Action Buttons
- "QoS Parameter" Tab

8.1.4.1 "QoS Parameter" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Quality of Service > "QoS Parameter" Tab



Layer 3 Voice Priority 2:

Layer 3 Voice Priority 4:

Layer 3 Voice Priority 6:

Layer 3 Voice Priority 8:

Layer 3 Voice Priority 2

Layer 3 value for voice priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 4

Layer 3 value for voice priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 6

Layer 3 value for voice priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 8

Layer 3 value for voice priority calls.

Value range: **DSCP00** ... **DSCP63**

8.1.5 Security Settings

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Security Settings

This area features the following components:

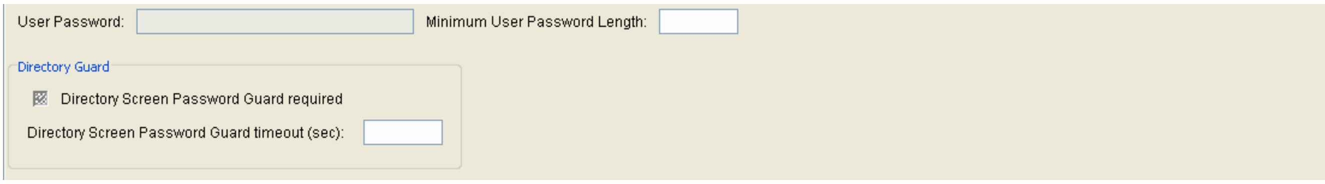
- General Data
- Possible Action Buttons
- "Passwords" Tab
- "Enabled Services (NW Stack)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.5.1 "Passwords" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Security Settings > "Passwords" Tab



User Password:
Minimum User Password Length:

Directory Guard

☒ Directory Screen Password Guard required

Directory Screen Password Guard timeout (sec):

User Password:

Password for access to the workpoint’s user area.

Minimum User Password Length:

Minimum number of characters that a password must contain.

Directory Guard

Directory Screen Password Guard required

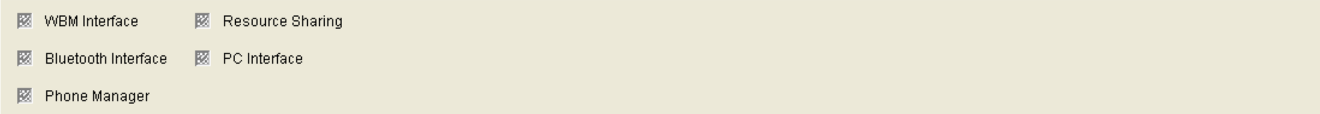
This check box activates password protection on the directory screen. To use the screen, you must enter the standard user password.

Directory Screen Password Guard timeout (sec)

Password protection is activated when the length of time specified here expires. After this time, you must enter the password to continue using the directory screen.

8.1.5.2 "Enabled Services (NW Stack)" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Security Settings > "Enabled Services (NW Stack)" Tab



☒ WBM Interface ☒ Resource Sharing

☒ Bluetooth Interface ☒ PC Interface

☒ Phone Manager

WBM Interface

Check box for activating the WBM interface.

Resource Sharing

Check box for activating resource sharing (shared use of mouse and keyboard).

Bluetooth Interface

Check box for activating the Bluetooth interface.

Phone Manager

Check box for activating the Phone Manager.

PC Interface

Check box for activating the interface between the PC and the device.

8.1.6 Telephony

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Telephony

This area features the following components:

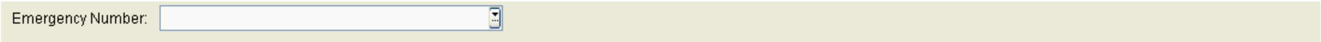
- General Data
- Possible Action Buttons
- "Telephony" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.6.1 "Telephony" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Telephony > "Telephony" Tab



Emergency Number:

Emergency Number:

Contains the phone number that can be dialed in an emergency.

8.1.7 Dialing Properties

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Dialing Properties

This area features the following components:

- General Data
- Possible Action Buttons
- "Dialing Properties" Tab
- "Canonical Dial Lookup" Tab

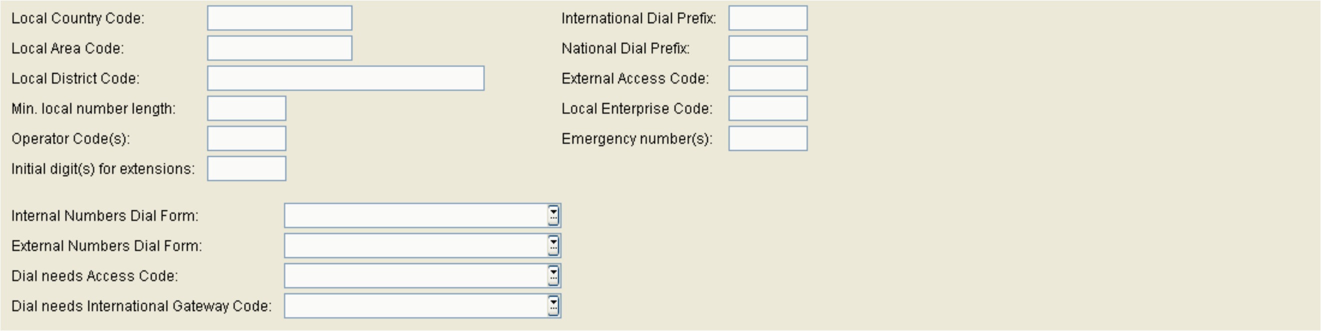
For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.7.1 "Dialing Properties" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Dialing Properties > "Dialing Properties" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").



Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

Local District Code:

Phone number of the company network.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **722** for Siemens Munich Hofmannstraße.

Only available for devices in the optiPoint family.

Min. local number length

Minimum length of the local number.

Operator Code(s)

The operator number. You may enter multiple numbers separated by commas.

Initial digit(s) for extensions

List of initial digits of all possible extensions in the local enterprise network. When a call number could not be matched as a public network number, the phone checks if it is part of the local enterprise network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly.

Example: If, the extensions 3000-5999 are configured in OpenScape Voice, each number will start with 3, 4, or 5. Therefore, the digits to be entered are **3, 4, 5**.

International Dial Prefix:

National prefix.

Format: Up to four digits.

Example: **00** in Germany.

National Dial Prefix:

International prefix.

Format: Up to five digits.

Example: **0** in Germany.

External Access Code:

Number for trunk seizure for an outgoing external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Local Enterprise Node:

Call number of the company network.

Example: **722** for Siemens Munich Hofmannstraße.

Only available for devices in the OpenStage family.

Emergency number(s)

You may enter multiple emergency numbers separated by commas.

Internal Numbers Dial Form

Possible options:

- **Local Company Format**
- **Always Add Node**

- **Use External Number**

External Numbers Dial Form

Possible options:

- **Local Public Format**
- **National Public Format**
- **International Public Format**

Dial needs Access Code

Possible options:

- **Not used**
- **For External Number**

Dial needs International Gateway Code

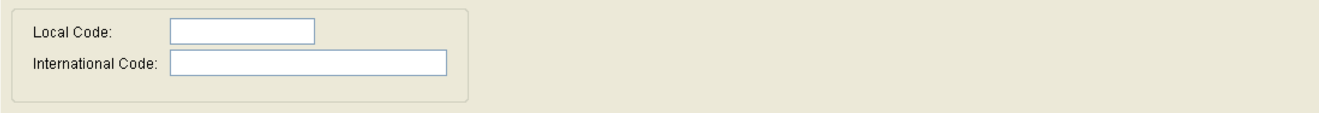
Possible options:

- **Use National Code**
- **Unchanged**

8.1.7.2 "Canonical Dial Lookup" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Dialing Properties > "Canonical Dial Lookup" Tab

This function transforms the entries in the first field ("Local Area Code") on the basis of a particular digit string as specified in the second field ("International Dial Code"). This digit string can be a national or international dial prefix, for example. This allows you to dial frequently used prefixes by entering just one digit.



Local Code

Digit or short digit string which can be used for dialing a particular prefix, for example.

International Code

Digit string, such as, a prefix, that is dialed at the beginning of the dialing operation using a particular digit.

8.1.8 Time Parameters

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Time Parameters

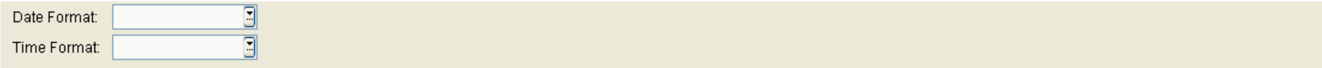
This area features the following components:

- General Data
- Possible Action Buttons
- "Time" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

8.1.8.1 "Time" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Time Parameters > "Time" Tab



Date Format:

Time Format:

Date format:

Format for date entry. Manual entry is only necessary if this information is not automatically transmitted (for example, PBX or DHCP server).

Possible options:

- **YY-MM-DD**
  Example: 04-10-05 for 5.10.2004
- **MM/DD/YY**
  Example: 10/05/04 for 5.10.2004
- **DD.MM.YY**
  Example: 05.10.04 for 5.10.2004

Time Format:

Time format.

Possible options:

- **12 hour**
- **24 hour**

8.1.9 Audio Settings

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Audio Settings

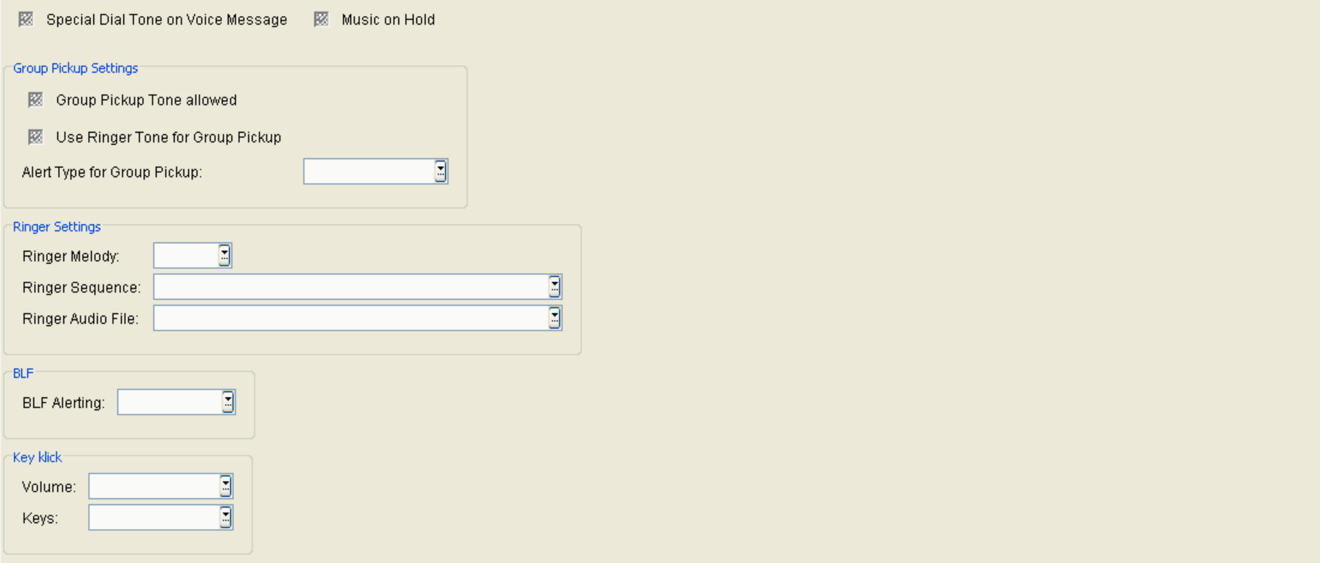
This area features the following components:

- General Data
- Possible Action Buttons
- "Audio Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

8.1.9.1 "Audio Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Audio Settings > "Audio Settings" Tab



Special Dial Tone on Voice Message

Check box for activating a special dial tone if a voice message is received.

Music on Hold

If this checkbox is activated, the phone will play music to a caller when he is put on hold.

Group Pickup Settings

Group Pickup Tone allowed

Activates or deactivates the generation of an acoustic signal for incoming pickup group calls.

Use Ringer Tone for Group Pickup

If this is checked, a pickup group call will be signaled by a short standard ringtone. If unchecked, a pickup group call will be signaled by an alert tone.

Alert type for Group Pickup:

Sets the type of visual alert on the phone GUI.

Possible Options:

- **Prompt**
  An incoming pickup call is signaled by an alert on the phone GUI. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured.

- **Notify**
  An incoming pickup call is signaled by an alert on the phone GUI. To accept the call, the user must confirm the alert or press the corresponding function key, if configured.

Ringer Settings

Ringer Melody:

Possible Options see Section 7.1.12.3, "Ringer Melody:"

Ringer Sequence:

Possible Options:

- **1 sec ON, 4 sec OFF**
- **1 sec ON, 2 sec OFF**
- **0.7 sec ON, 0.7 sec OFF, 0.7 sec OFF, 3 sec OFF**

Ringer Audio File

Name of the file that contains the ringtone.

Key klick

Volume

Defines the volume of key clicks.

Possible Values:

- **Off**
- **Low**
- **Medium**
- **High**

Keys

Defines which keys shall have audible clicks.

Possible Values:

- **Keypad only**
- **All keys**

8.1.10 Applications

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications

This area features the following components:

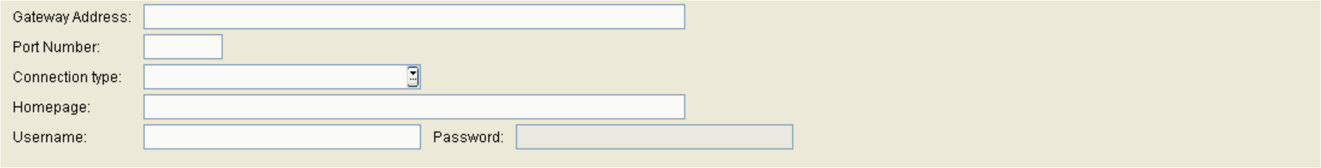
- General Data
- Possible Action Buttons
- "WAP" Tab
- "Java" Tab
- "XML Applications" Tab
- "Application List" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.10.1 "WAP" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications > "WAP" Tab



Gateway Address:

IP address or host name of the WAP server.

Port Number:

Port number of the WAP server.

Connection type:

Protocol type for connection to the WAP server.

Possible options:

- **HTTP**
- **WSP**

Homepage:

URL of the welcome page where the WAP homepage is located.

Username

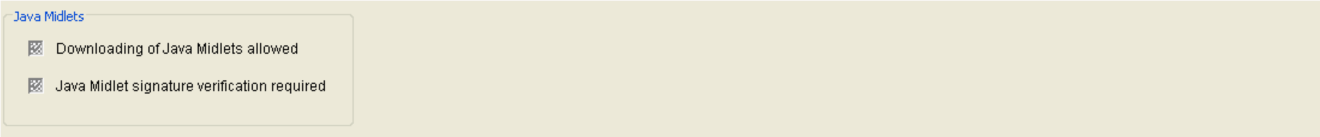
User ID for identification at the WAP server.

Password:

Password for the user ID.

8.1.10.2 "Java" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications > "Java" Tab



Java Midlets

☑ Downloading of Java Midlets allowed

☑ Java Midlet signature verification required

Java Midlets

Downloading of Java Midlets allowed

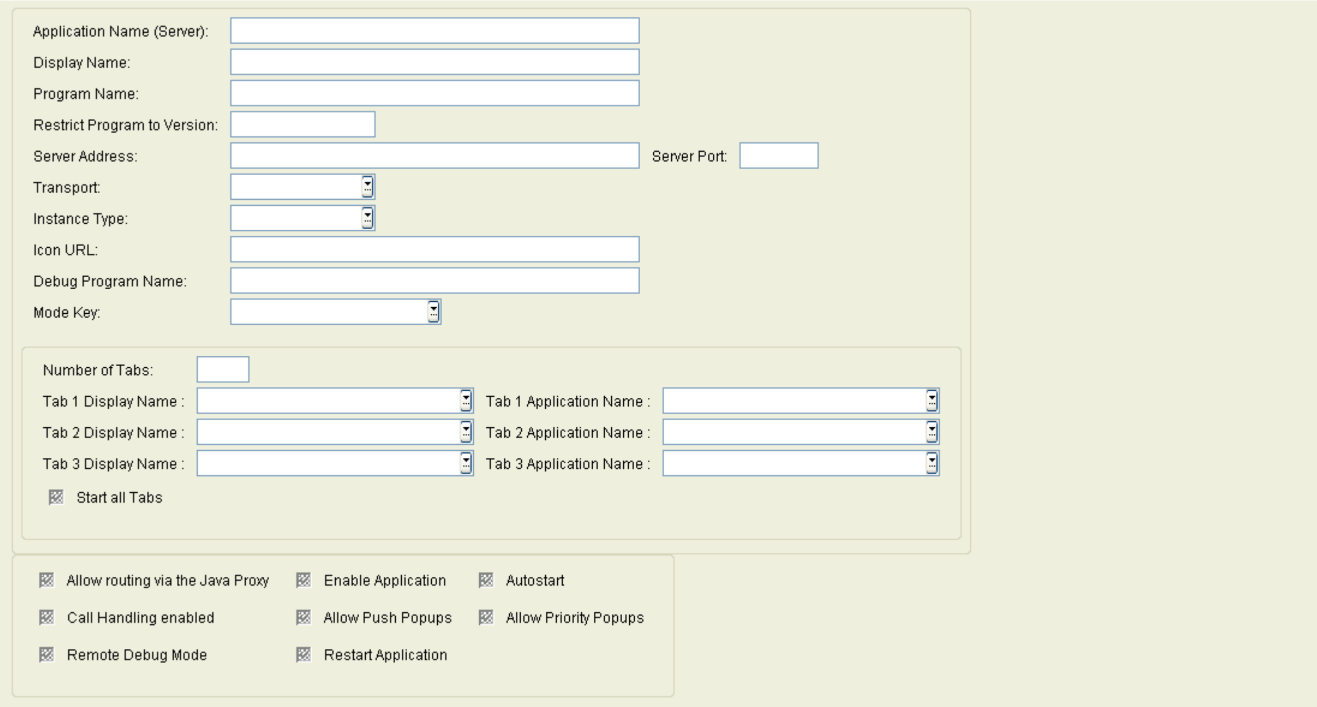
If this check box is activated, you can download Java midlets to the workpoint.

Java Midlet signature verification required

If this check box is activated, Java midlets must be verified using a signature.

8.1.10.3 "XML Applications" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications > "XML Applications" Tab



For information on XML applications, please refer to Section 7.1.14.4, ""XML Applications" Tab"

XML Applications

Application Name (Server):

This name is used internally by the workpoint software to identify the application.

Display Name:

This name is used for listing the application on the workpoint menu.

Program Name:

Path of the start file of the server-side program, relativ to the server address.

Restrict Program to Version:

Server Address:

IP address of the server, on which the program is running.

Example: **192.168.1.150**

Server Port:

Port used by the server-side program for receiving data from the workpoint.

Examples: **80** (Apache default port); **8080** (Tomcat default port).

Transport:

Transport protocol used for transmitting XML data.

Possible options:

- **HTTP**
- **HTTPS**

Instance Type:

Selection of the type of instance.

Possible options:

- **Normal**
- **Xpressions**
- **Phonebook**

Icon URL:

URL of the application icon (not yet implemented).

Debug Program Name:

Name and, where applicable, directory path of the program on the server that receives error messages from the terminal’s *.XML application platform.

Mode Key:

Select a mode key to start the application.

Possible options:

- **No Mode Key**
- **Phonebook Mode Key**
- **CallLog Mode Key**
- **Messages Mode Key**
- **Help Mode Key**

Number of Tabs:

The number of embedded tabs within the XML application to be shown on phone display.

Value range: **0** ... **3**

> For an XML-application with a number of Tabs > 0, one of the entries between **Tab 1 Application Name** and **Tab 3 Application Name** must be set to the same value as the **Application Name (Server)** that it is associated with. When the XML application is started, the tab which has the same name as the XML application is the tab that initially gets focus.

Tab 1 Display Name:

Labeling displayed on the 1st tab header.

Tab 2 Display Name:

Labeling displayed on the 2nd tab header.

Tab 3 Display Name:

Labeling displayed on the 3rd tab header.

Tab 1 Application Name:

The name used by the XML application to identify the application running under the 1st tab. The name must be unique over all XML-applications.

Tab 2 Application Name:

The name used by the XML application to identify the application running under the 2nd tab. The name must be unique over all XML-applications.

Tab 3 Application Name:

The name used by the XML application to identify the application running under the 3rd tab. The name must be unique over all XML-applications.

Start all Tabs

On application start, all tabs will be opened.

Allow routing via the Java Proxy

Enable Application

Autostart

Call Handling enabled

Allow Push Popups

Allow Priority Popups

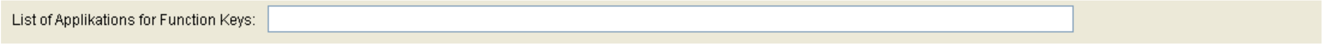
Remote Debug Mode

Restart Application

Restart Application, if it is already running.

8.1.10.4 "Application List" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications > "Application List" Tab


List of Applikations for Function Keys:

List of Applications for Function Keys

Comma-separated list of names for applications, which can be started by means of Function Keys.

8.1.11 LDAP

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > LDAP

This area features the following components:

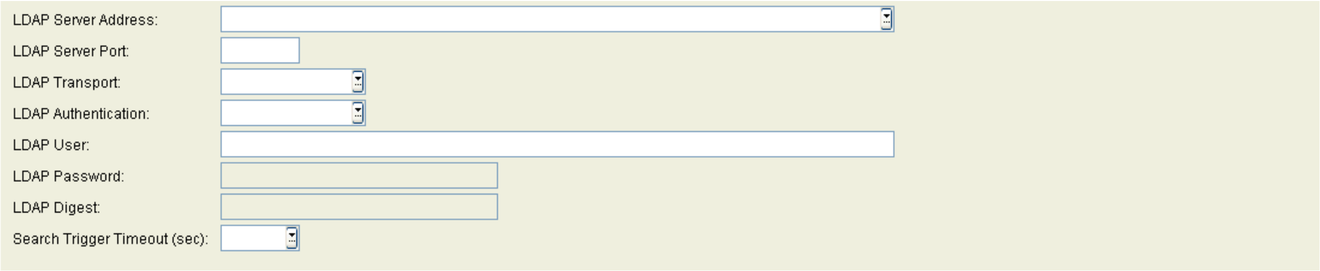
- General Data
- Possible Action Buttons
- "LDAP Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination"

8.1.11.1 "LDAP Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > LDAP > "LDAP Settings" Tab



LDAP Server Address:

IP address or host name of the LDAP server.

LDAP Server Port:

Port number of the LDAP server.

LDAP Transport:

Transport protocol used to transmit LDAP data.

Possible options:

- **TCP**

LDAP Authentication:

Option for selecting the LDAP access.

Possible options:

- **Anonymous**
- **Simple**

LDAP User:

User name for authenticated LDAP access.

LDAP Password:

Password for authenticated LDAP access.

LDAP Digest:

Search Trigger Timeout (sec):

Search Trigger Timeout for LDAP simple search.

Possible options:

- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**
- **60**

8.1.12 User Settings

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > User Settings

This area features the following components:

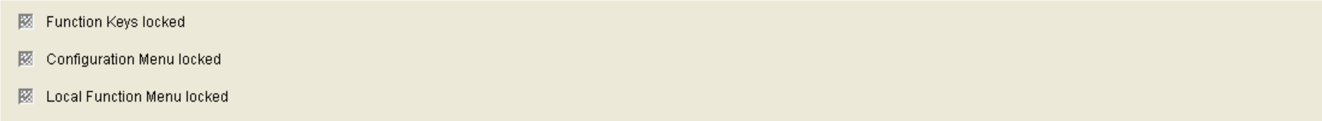
- General Data
- Possible Action Buttons
- "Locks" Tab
- "Locked Configuration Menus" Tab
- "Locked Local Functions" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.12.1 "Locks" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > User Settings > "Locks" Tab



☒ Function Keys locked

☒ Configuration Menu locked

☒ Local Function Menu locked

Function Keys locked

Check box for locking function keys on the Mobility Phone for a Mobile User.

Configuration Menus locked

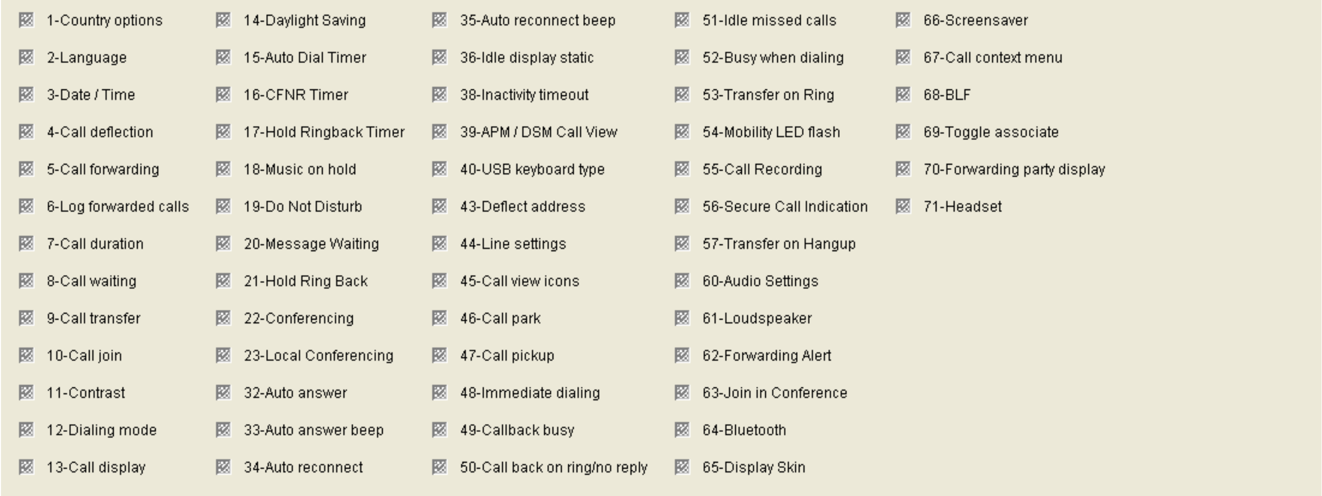
Check box for locking configuration menus on the Mobility Phone for a Mobile User.

Local Function Menus locked

Check box for locking local function menus on the Mobility Phone for a Mobile User.

8.1.12.2 "Locked Configuration Menus" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > User Settings > "Locked Configuration Menus" Tab



☑ 1-Country options
☑ 2-Language
☑ 3-Date / Time
☑ 4-Call deflection
☑ 5-Call forwarding
☑ 6-Log forwarded calls
☑ 7-Call duration
☑ 8-Call waiting
☑ 9-Call transfer
☑ 10-Call join
☑ 11-Contrast
☑ 12-Dialing mode
☑ 13-Call display
☑ 14-Daylight Saving
☑ 15-Auto Dial Timer
☑ 16-CFNR Timer
☑ 17-Hold Ringback Timer
☑ 18-Music on hold
☑ 19-Do Not Disturb
☑ 20-Message Waiting
☑ 21-Hold Ring Back
☑ 22-Conferencing
☑ 23-Local Conferencing
☑ 32-Auto answer
☑ 33-Auto answer beep
☑ 34-Auto reconnect
☑ 35-Auto reconnect beep
☑ 36-Idle display static
☑ 38-Inactivity timeout
☑ 39-APM / DSM Call View
☑ 40-USB keyboard type
☑ 43-Deflect address
☑ 44-Line settings
☑ 45-Call view icons
☑ 46-Call park
☑ 47-Call pickup
☑ 48-Immediate dialing
☑ 49-Callback busy
☑ 50-Call back on ring/no reply
☑ 51-Idle missed calls
☑ 52-Busy when dialing
☑ 53-Transfer on Ring
☑ 54-Mobility LED flash
☑ 55-Call Recording
☑ 56-Secure Call Indication
☑ 57-Transfer on Hangup
☑ 60-Audio Settings
☑ 61-Loudspeaker
☑ 62-Forwarding Alert
☑ 63-Join in Conference
☑ 64-Bluetooth
☑ 65-Display Skin
☑ 66-Screensaver
☑ 67-Call context menu
☑ 68-BLF
☑ 69-Toggle associate
☑ 70-Forwarding party display
☑ 71-Headset

The following functions can be locked for the Mobile User in the configuration menus by activating the relevant check box:

1-Country options

The user can select a country from a list to adapt the phone to country specific conditions.

2-Language

The user can set the language for the administration and user menu.

3-Date / Time

The user can set the local time, the current date, and the daylight saving time.

4-Call deflection

The user can activate or deactivate call deflection.

5-Call forwarding

The user can activate or deactivate call forwarding.

6-Log forwarded calls

The user can activate or deactivate the logging of forwarded calls.

7-Call duration

The user can determine whether the call duration is indicated on the display.

Only available in optiPoint workpoints.

8-Call waiting

The user can determine whether a second call is allowed during a connected call. If not, the caller hears the busy tone.

9-Call transfer

The user can allow call transfer.

10-Transfer call

The user can enable or disable the posibility to interlink an active and a held call.

11-Contrast

The user can set the contrast for the display.

12-Dialing mode

The user can determine whether a number only or, alternatively, a name can be used for dialing.

Only available in optiPoint workpoints.

13-Call display

The user defines which information about the caller is displayed on an incoming call.

Only available in optiPoint workpoints.

14-Daylight Saving

The user can set the daylight saving time.

15-Auto dial timer

The delay time between the entry of the last call number digit and the start of the dialing process can be set by the user.

16-CFNR timer

The user can set the delay time that passes before a call is forwarded, if Call Forwarding on No Reply is activated.

17-Hold ringback timer

The user can set the time delay, after which the workpoints indicates that there us a held call.

18-Music on hold

The user can determine whether the music on hold stored in the phone is used. If music on hold is activated, it is played as soon as the phone is put to hold.

19-Do not disturb

The user can determine whether Do Not Disturb is available on the phone. If Do Not Disturb is active, the phone will not ring on an incoming call, and the caller will hear the busy tone.

20-Message waiting

The user can determine whether new messaes in the mailbox are signaled by a LED.

Only available in optiPoint workpoints.

21-Hold ring back

If this function is active and a participant has been put to hold, a signal sounds after a configurable time to remind that a call is on hold. The user can allow this function and set the delay time for the acoustic signal.

22-Conference

The user can allow system based conferences.

Only available in optPoint workpoints.

23-Local conference

The user can allow local 3-party conferences.

32-Auto answer

The user can determine whether incoming calls are accepted automatically by the CTI application which is connected to the phone.

33-Auto answer beep

The user can determine whether a signal will sound when a call that is accepted automatically by the CTI application connected to the phone.

34-Auto reconnect

The user can determine whether a held call can be reconnected automatically by the CTI application.

35-Auto reconnect beep

The user can determine whether a signal will sound when a held call is reconnected by the CTI application.

36-Idle display static

The user can configure the indication of system messages in idle state.

Only available in optiPoint workpoints.

38-Inactivity timeout

The user can set the delay time between the last entry and the return to the idle state.

39-APM / DSM Call View

The user can activate or deactivate the call view on the optiPoint application module.

40-USB keyboard type

The user can modify the language of the USB keyboard connected to an optiPoint phone.

Only available in optiPoint workpoints.

43-Deflect address

The user can enter resp. modify the target number for call deflection.

44-Line settings

The user can modify the settings of a line key.

45-Call view icons

The user can determine whether messages on the optiPoint display module, like, for instance, the list of missed calls, are displayed as text or symbols.

46-Call park

The user can allow call parking.

47-Call pickup

The user can allow pickup of a parked call.

48-Immediate dialing

49-Callback busy

The user can activate the transmission of a callback request to the system in case the phone is busy.

50-Call back on ring/no reply

The user can activate the transmission of a callback request to the system in case a call is not replied.

Only available in OpenStage workpoints.

51-Idle missed calls

The user can activate missed calls notifications on the display.

Only available on optiPoint workpoints.

52-Busy when dialing

Der Benutzer kann bestimmen, ob ein Abruf abgewiesen wird, der während der Eingabe einer Rufnummer eingeht.

The user can determine whether incoming calls are refused while a call number is entered.

53-Transfer on Ring

The user can determine whether a call is transferred as soon as the third participant’s phone rings, even if the transferring participant has not hung up.

54-Mobility LED flash

The user can determine whether the mobility key LED flashes during data exchange between phone and DLS, like, for instance, while mobility logon and logoff.

Only available in optiPoint workpoints.

55-Call Recording

The user can activate call recording.

Only available in optiPoint workpoints.

56-Secure Call Indication

The user can determine whether an alert tone shall indicate an insecure speech connection.

57-Transfer on Hangup

The user can determine whether, when one call is active and another call is on hold, the user can connect these calls by hanging up.

60-Audio Settings

The user can modify settings like ringtones and room character.

Only available in OpenStage workpoints.

61-Loudspeaker

The user can activate or deactivate handsfree talking.

Only available in OpenStage workpoints.

62-Forwarding Alert

63-Join in Conference

The user can determine whether visual or acoustical warning notifications indicate an incoming call while call forwarding is active.

Only available in OpenStage workpoints.

64-Bluetooth

The user can activate or deactivate bluetooth connectivity.

65-Display Skin

The user can choose the display theme.

Only available in OpenStage 60/80 workpoints.

66-Screensaver

The user can activate the phones's screensaver and set the delay time for starting the screensaver.

Only available in OpenStage 60/80 workpoints.

67-Call context menu

The user can define the displayed menu.

Only available in OpenStage 60/80 workpoints.

68-BLF

The user can define how an incoming call for the phone supervised by the BLF key shall be displayed.

69-Toggle associate

The user can enable or disable the connecting of a first call and a second call by going on-hook. When "Toggle associate" is activated, the following procedure will ensue: The user has accepted a second call, whereby the first call is put to hold. As soon as the user has alternated back to the first call, and then again to the second call, he/she can connect both calling parties by going on-hook.

Available in all OpenStage workpoints.

70- Forwarding party display

For multiple forwarding, the user can determine whether the first forwarding party or the last forwarding party is displayed.

Available in all OpenStage SIP workpoints.

71- Headset

The user can define the type of headset connected to the phone.

Available for OpenStage 40/60/80 SIP/HFA.

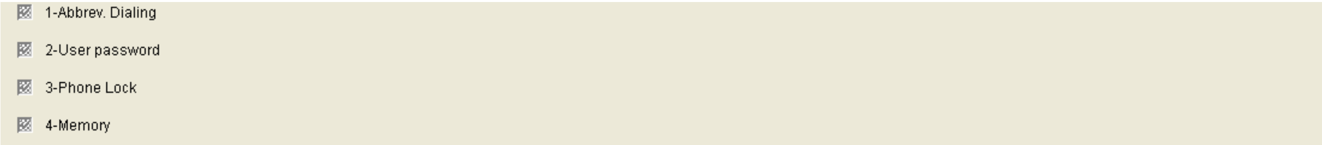
72- Key klick

The user can define the mode of key klick on the phone.

Available for OpenStage 40/60/80 SIP/HFA.

8.1.12.3 "Locked Local Functions" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > User Settings > "Locked Local Functions" Tab



☒ 1-Abbrev. Dialing

☒ 2-User password

☒ 3-Phone Lock

☒ 4-Memory

The following functions can be locked for the Mobile User in the configuration menus by activating the relevant checkbox:

1-Abbreviated dialing

The user can set up abbreviated dialing numbers.

Only available in optiPoint workpoints.

2-User password

The user can change his password.

3-Phone lock

The user can lock the phone. If the phone is locked, no unauthorized person can call from this phone in a regular manner or modify any settings. Only emergency numbers and pre-defined numbers from the dial plan can be dialed.

4-Memory

The user can delete all abbreviated dialing numbers and restore the factory settings.

Only available in optiPoint workpoints.

8.1.13 SIP Mobility

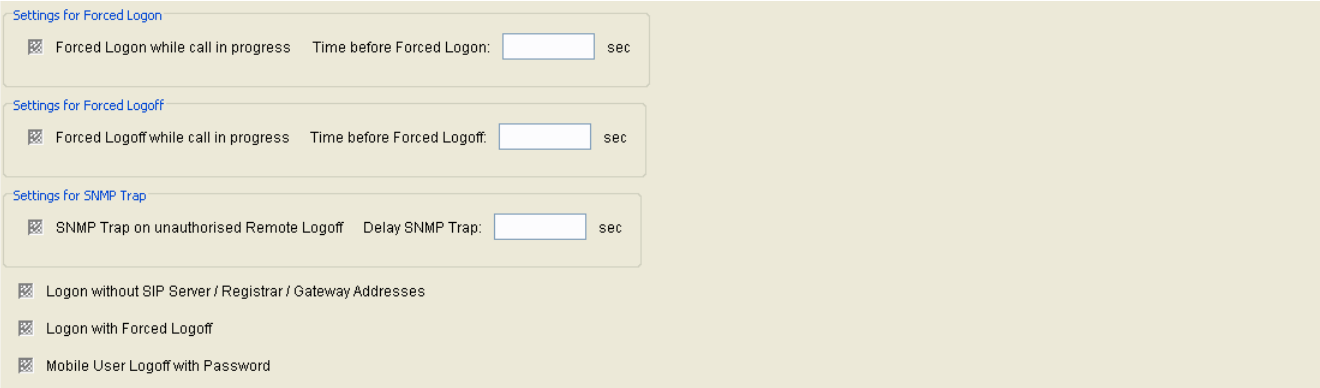
Call: Main Menu > Mobile Users > SIP Mobile User Configuration > SIP Mobility

This area features the following components:

- General Data
- Possible Action Buttons
- "Mobility Logon/Logoff" Tab
- "Mobility Data" Tab

8.1.13.1 "Mobility Logon/Logoff" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > SIP Mobility > "Mobility Logon/Logoff" Tab



Settings for Forced Logon

☒ Forced Logon while call in progress Time before Forced Logon: sec

Settings for Forced Logoff

☒ Forced Logoff while call in progress Time before Forced Logoff: sec

Settings for SNMP Trap

☒ SNMP Trap on unauthorised Remote Logoff Delay SNMP Trap: sec

☒ Logon without SIP Server / Registrar / Gateway Addresses

☒ Logon with Forced Logoff

☒ Mobile User Logoff with Password

Settings for Forced Logon

If the check box is active, the mobile user can be logged on to the device during the call. Logon is performed once the time entered in the field **Time before Forced Logon** has expired. If the check box is not active, attempted logon during the call is not forced even when the call has been completed. Forced logon must then be restarted.

Settings for Forced Logoff

If the check box is active, the Mobile User can be logged off from the device during the call. Logoff is performed once the time specified in the field **Time before Forced Logoff** has elapsed. If the check box is not active, attempted logoff during the call is not forced even when the call has been completed. Forced logoff must then be restarted.

Settings for SNMP Trap

If the check box is active, a message is sent to the SNMP server each time an unauthorized remote logoff is attempted. For information on entering SNMP server data, see Section 7.1.13.1, ""SNMP" Tab".

Logon without SIP Server / Registrar / Gateway Addresses

If this check box is active, the following data is not sent to the device when a mobile user logs on: SIP server address/port, SIP registrar address/port, SIP gateway address/port.

Logon with Forced Logoff

If this check box is active, Mobile User logoff is forced as soon as another user logs on to the device.

Mobile User Logoff with Password

If the check box is active, Mobile User logoff is only possible when the password of the currently logged-on Mobile User is entered.

Time before Forced Logon

Time in seconds until forced logon takes place. This information is only relevant if the option **Forced Logon while call in progress** is activated. A value from 0 to 180 can be entered.

Time before Forced Logoff

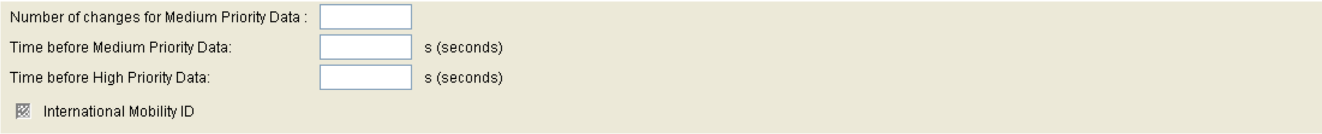
Time in seconds until forced logoff takes place. This information is only relevant if the option "Forced Logoff while call in progress" is activated. A value from 0 to 180 can be entered.

Delay SNMP Trap

Time in seconds until the SNMP trap is sent. For information on entering SNMP server data, see Section 7.1.13.1, ""SNMP" Tab".

8.1.13.2 "Mobility Data" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > SIP Mobility > "Mobility Data" Tab



Number of changes for Medium Priority Data : □

Time before Medium Priority Data: □ s (seconds)

Time before High Priority Data: □ s (seconds)

☑ International Mobility ID

Number of changes for Medium Priority Data:

Defines how many changes to medium priority data may take place in the workpoint before this data is sent to the DLS.

Time before Medium Priority Data:

Defines the interval after which medium priority data that has been changed in the workpoint is sent to the DLS.

Time before High Priority Data:

Defines the interval after which high priority data that has been changed in the workpoint is sent to the DLS.

International Mobility ID

If this check box is activated, the device automatically adds the local country code to the extension, in addition to the trunk number and local area code when a mobile user logs on. The international code is configured under **Mobile Users** > **SIP Mobile User Configuration** > **Dialing Properties** > **"Dialing Properties" Tab** -> **International Dial Prefix**.

Example: The user logs on to the device using the extension/mobility ID "31434". If the check box is activated, the device sends the number "498972231434". Otherwise, the device sends the number "8972231434".

8.1.14 Keysets/Keylayout

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Keysets/Keylayout

This area features the following components:

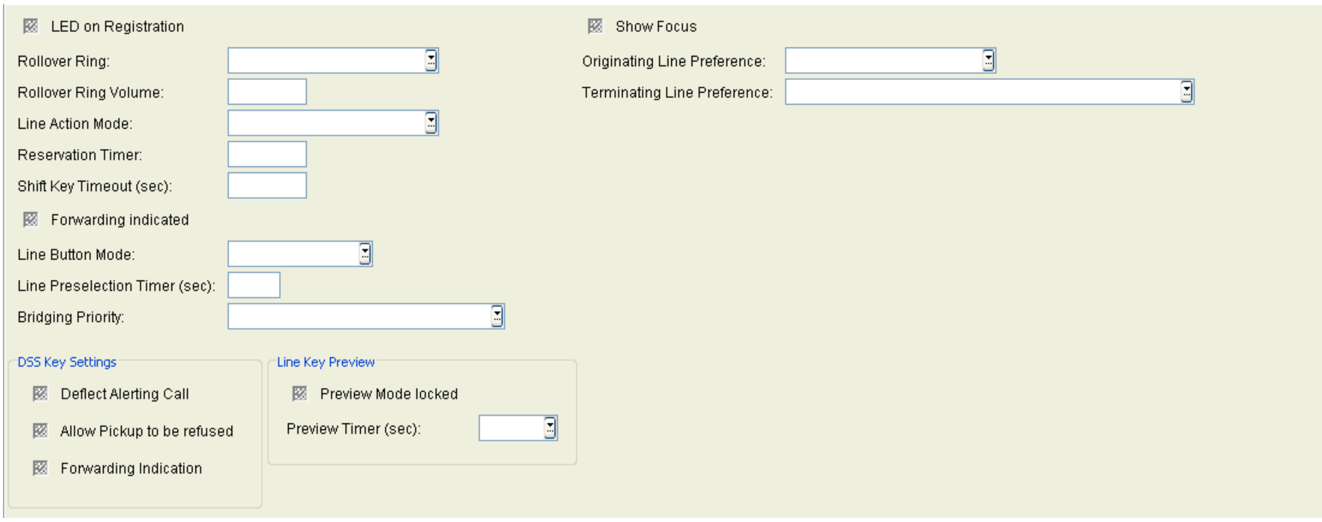
- General Data
- Possible Action Buttons
- "Keysets" Tab
- "Destinations" Tab
- "Send URL Server CA Certificate" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.14.1 "Keysets" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Keysets/Keylayout > "Keysets" Tab



LED on Registration

Check box for activating the display when restarting the IP phone indicating whether the workpoint was registered successfully.

Only available in SIP workpoints.

Rollover Ring:

Type of alerting when busy.

Possible options:

- **No ring**
- **Alert Ring**
- **Standard**
- **Alerting**

Only available in SIP workpoints.

Rollover Ring Volume:

Volume of alerting when busy.

Only available in SIP workpoints.

Line Action Mode:

Defines what should happen to a line (call) when a connection is established over another line.

Possible options:

- **Call hold**
  The original call is put on hold.
- **Release**
  The connection to the original call is cleared down (the call is ended).

Only available in SIP workpoints.

Reservation Timer:

Time in seconds indicating how long a line reservation can be maintained.

Default: 60 s.

Only available in SIP workpoints.

Shift Key Timeout (sec)

Duration of Shift key mode in seconds.

Forwarding indicated

Check box for activating alerting on a line key when call forwarding is active for its destination.

Only available in SIP workpoints.

Line Button Mode

Line Button functionality.

Possible options:

- **Single button**

- **Preselection**

Line Preselection Timer (sec)

Duration of line preselection in seconds.

Bridging Priority

Possible options:

- **Bridging overrides preview**
- **Preview overrides bridging**

Show Focus

Check box for activating the display showing which line is currently active (line has the focus).

Only available in SIP workpoints.

Originating Line Preference:

Defines the preferred line to be used for outgoing calls.

Possible options:

- **Idle line preference**
- **Primary line preference**
- **Last line preference**
- **No preference**

Only available in SIP workpoints.

Terminating Line Preference:

Defines the preferred line to be used for incoming calls.

Possible options:

- **Ringing line preference**
- **Calling line preference with prime line preferred**
- **Ringing line preference**
- **Ringing line preference with prime line preferred**
- **No preference**

Only available in SIP workpoints.

DSS Key Settings

Deflect Alerting Call

Check box for activating the "Deflect Alerting Call" feature.

Allow Pickup to be refused

Check box for activating the "Reject Group Pickup" feature.

Forwarding Indication

Checkbox for activating the forwarding indication.

Line Key Preview

Preview Mode locked:

Switch to lock preview mode

Preview Timer (sec)

Duration of preview mode in seconds.

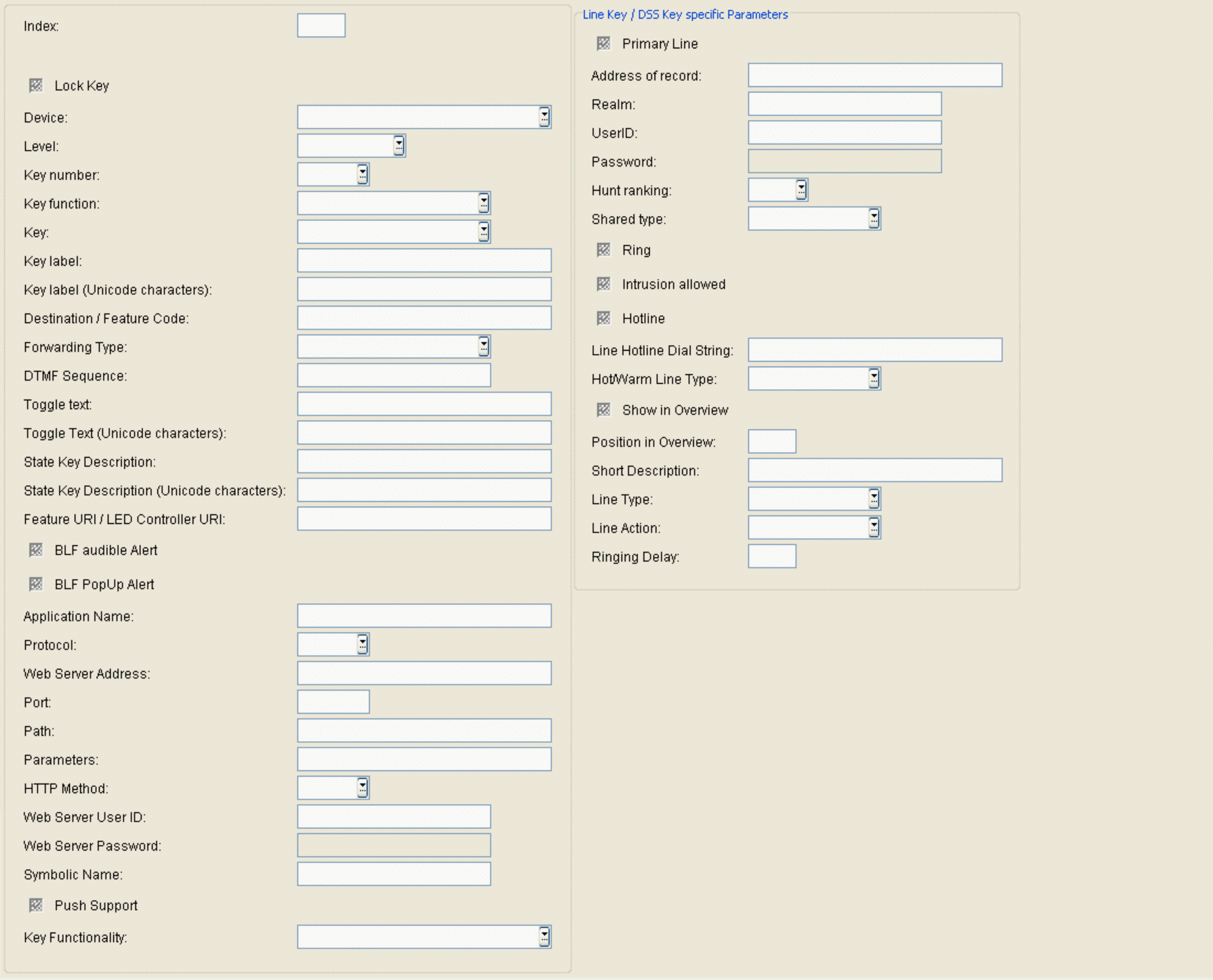
Possible options:

- **2**
- **3**
- **4**
- **6**
- **8**
- **10**
- **15**
- **20**
- **30**
- **40**
- **50**
- **60**

8.1.14.2 "Destinations" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Keysets/Keylayout > "Destinations" Tab

> When creating a key layout, make sure that the key used by a mobile user for the primary line is available on all device types.
> If the primary line is assigned to a key that does not exist on the device to which the mobile user is logged on, then there is no primary line key available to the mobile user. This can be avoided by entering the appropriate settings in the **SIP Mobile User Interaction** > **SIP User Keylayout** mask.



Index:

Name of the key layout function.

Lock Key

Locks the key for the user.

Device:

Specifies the device to which the relevant layout applies.

Possible options:

- **Base device**
- **1st Key module**
- **2nd Key module**
- **1st Self Labeling Key module**
- **2nd Self Labeling Key module**
- **OpenStage 15 Key module**

Only available in SIP workpoints.

Level:

Key level for the Shift functionality.

Possible options:

- **1. Level**
- **2. Level**
- **3. Level**
- **4. Level**
- **Fixed Keys**
  Fixed Keys are assigned to a fixed key number. They cannot be deleted or created on the IP Device.

Only available in SIP workpoints.

Key number:

Number of the key assigned the relevant function.

If **Level** "Fixed Keys" is selected, the following key numbers are fixed:

1 Fixed Keys - release

2 Fixed Keys - forwarding

3 Fixed Keys - voice dial

9 Fixed Keys - redial

Depending on the selected key number, **Key function** shows a selection of possible values.

Only available in SIP workpoints.

Key function:

The following key functions are supported:

- **Key unused**
- **Selected dialing**
- **Abbreviated dialing**
- **Repeat dialing**
- **Missed calls**
- **Voice messages**
- **Forwarding**
- **Loudspeaker**
- **Mute**
- **Ringer off**
- **Hold**
- **Alternate**
- **Blind Transfer**
- **Join** (optiPoint) **/ Transfer call** (OpenStage)
- **Deflect**
- **Setup menu**
- **Room echoing**
- **Room muffled**
- **Shift**
- **Notebook**
- **Settings**
- **Phone lock**
- **Conference**
- **Local Conference**
- **Headset**
- **Do not disturb**
- **Group pickup**
- **Repertory dial**
- **Line**
- **Feature Toggle**
- **Show Phone Screen**
- **Swap screen**
- **Mobility**
- **Call park**
- **Call pickup**
- **Cancel/Release**

- **Ok Confirm**
- **Callback Request**
- **Cancel Callback**
- **Consultation Transfer**
- **DSS**
- **State Key**
- **Immediate Ring**
- **Preview Key**
- **Call Recording**
- **AICS Zip**
- **Server Feature**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **BLF**
- **Start Application**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **Send URL**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **Built-in Forwarding**
  Only available for ’Fixed Keys’.
- **Built-in Release**
  Only available for ’Fixed Keys’.
- **Built-in Voice Dial**
  Only available for ’Fixed Keys’.
- **Built-in Redial**
  Only available for ’Fixed Keys’.
- **Start Phonebook**

Key:

Indicates whether this key is a ’Fixed Key’or a freely programmable key.

Key label:

A key label can be entered here for every function key in the case of Self labeling Keys workpoints (for example, optiPoint 420 standard).

Only available in SIP workpoints.

Key label (Unicode characters):

You can enter the key label in unicode characters for devices in the OpenStage family.

Destination / Feature Code:

Destination data to be dialed. This can be a digit string or a URL. Feature codes that need to be sent to external servers (not the SIP server at which the phone is registerd) have the following format:

<feature code>@<IP address>

Example: **123@10.2.54.2**

If the destination has been entered for the "Repertory dial" key function, extra control characters can be entered in a digit string:

- **$Q** = clear (CL)
- **$R** = consult (CS)
- **$S** = OK
- **$T** = Pause (PA)

Only available in SIP workpoints.

Forwarding Type:

Selection of situations when forwarding should be enabled.

Possible options:

- **on busy**
- **on no reply**
- **unconditionally**

Only available in SIP workpoints.

DTMF Sequence

DTMF Sequence for this target.

Toggle Text:

Text describing the server function selected with Feature Toggle.

Only available in SIP workpoints.

Toggle Text (Unicode characters):

Text in unicode describing the server function selected with Feature Toggle.

Only available on OpenStage devices.

State Key Description:

Description text for the state key.

State Key Description (Unicode characters):

Description text for the state key in unicode. Only available on devices in the OpenStage family (SIP version).

Feature URI / LED Controller URI

URI used to control this feature on the server.

BLF audible Alert

Audible Alert additional to busy lamp field.

BLF PopUp Alert

Additional to busy lamp field a message pops up in display.

Application Name:

Name of the application to be started with the function key.

Protocol

Protocol of Web Server.

Possible options:

- **HTTP**
- **HTTPS**

Web Server Address

Host name, domain name, or IP address of web server.

Port

Port number of web server: If the port is null, the fully qualified URL will not include the port element.

Path

Directory path and name of the program or web page.

Examples: **servlet/IppGenericServlet** or **webpage/checkin.xml**

The path should have a slash at the beginning and no slash at the end. If the slash at the beginning is missing, a slash will be automatically inserted. If there is an additional slash at the end, it will be automatically removed. The slashes in the path should be forward slashes ('/'). If backslashes ('\') are used instead, the web server may not find the appropriate program or web page.

Parameters

Null, one, or more parameter-value pairs in the format “<parameter>=<value>”, with each pair separated by an ampersand (“&”), e. g. **parameter1=value1&parameter2=value2**. A comma (“,”) is not used as a separator because it could be part of the key or value. If the key or value contains an ampersand, it must be replaced by “&amp;”.

The question mark will be automatically added between the path and the parameters. If there is a question mark at the beginning of the parameters, it will be automatically stripped off.

HTTP Method

HTTP method to be used.

Possible options:

- **Get**
- **Post**

Web Server User ID

User identity known by the server. This information is used for phone authentication by the server.

Web Server Password

Password known by the server. It is used for phone authentication by the server.

Symbolic Name

Symbolic name.

Push Support

Enables or disables push support.

Key Functionality

Possible options:

- **Toggle Call Forwarding**
- **Unspecified Call**
- **Unspecified**

Line Key / DSS key specific Parameters

Primary line

Only available in SIP workpoints.

Address of record:

Only available in SIP workpoints.

Realm:

Entry of the SIP realm.

Only available in SIP workpoints.

UserID:

Only available in SIP workpoints.

Password:

Only available in SIP workpoints.

Hunt ranking:

Only available in SIP workpoints.

Shared type:

Possible options:

- **Private**
- **Shared**
- **Unknown**

Only available in SIP workpoints.

Ring

Only available in SIP workpoints.

Intrusion allowed

Check box for allowing intrusion.

Only available in SIP workpoints.

Hotline

Line Hotline Dial String:

Destination for the line hotline.

Only available in SIP workpoints.

Hot/Warm Line Type:

Possible options:

- **Ordinary**
- **Hot Line**
- **Warm Line**

Only available in SIP workpoints.

Show in Overview

Checkbox for activating the line display in the line overview.

Only available in SIP workpoints.

Position in Overview

Position of key in Line Overview.

Only available in SIP workpoints.

Short Description:

Description of relevant line.

Only available on OpenStage devices.

Line Type:

Possible options:

- **normal**
- **direct**

Line Action:

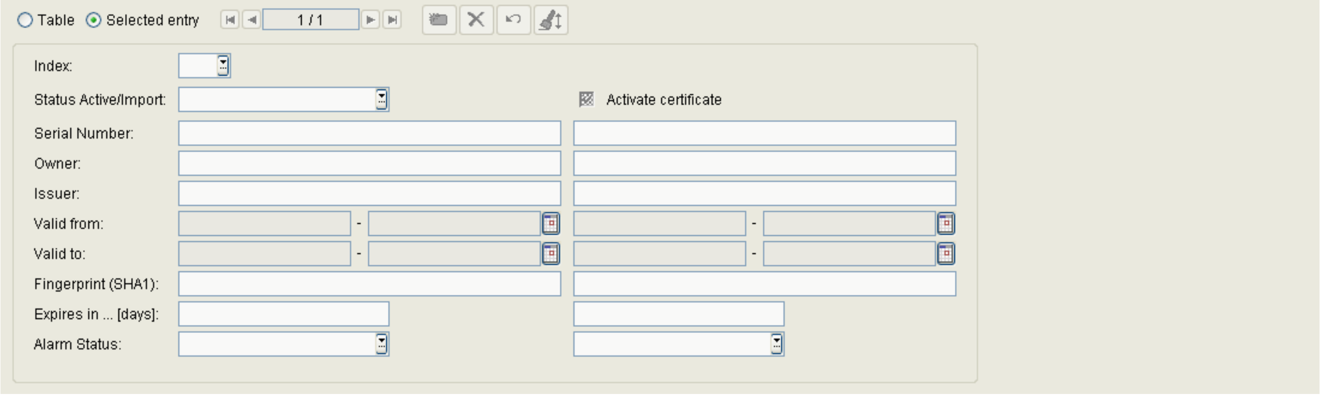
Possible options:

- **Consult**
- **Transfer**
- **No Action**

Ringing Delay:

8.1.14.3 "Send URL Server CA Certificate" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Keysets/Keylayout > "Send URL Server CA Certificate" Tab



For a parameter description, please refer to **IP Devices** > **IP Phone Configuration** > **LDAP** > **"CA Certificates" Tab**.

8.1.15 Signaling and Payload Encryption (SPE)

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Signaling and Payload Encryption (SPE)

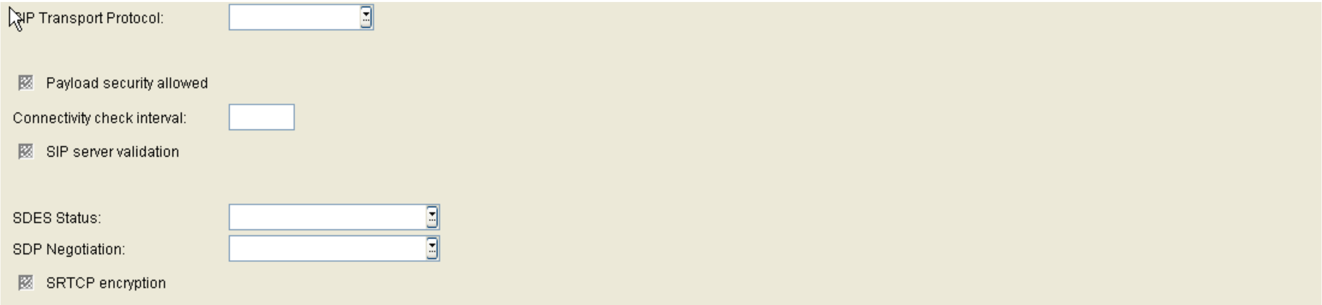
This area features the following components:

- General Data
- Possible Action Buttons
- "SIP Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

8.1.15.1 "SIP Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Signaling and Payload Encryption (SPE) > "SIP Settings" Tab



SIP Transport Protocol:

▨ Payload security allowed

Connectivity check interval:

▨ SIP server validation

SDES Status:

SDP Negotiation:

▨ SRTCP encryption

SIP Transport Protocol:

Protocol for SIP signaling.

Possible options:

- **UDP**
- **TCP**
- **TLS**

Payload security allowed

When activated, payload security is allowed.

Connectivity check interval

Connectivity check interval in seconds.

SIP server validation

When activated, the TLS connection to the SIP server is validated.

SDES Status

Select the SDES status.

Possible options:

- **disabled**
- **enabled**

SDP Negotiation

Select the SDP negotiation.

Possible options:

- **SRTP and RTP**
- **SRTP only**

- **Fallback to RTP**

SRCTP Encryption

When activated, SRCTP encryption will be applied.

SRTP Key Negotiation Method

Select the SRTP key negotiation method.

Possible options:

- **MIKEY**
- **SDES**

Secure Payload Type

Select the secure payload type.

Possible options:

- **SRTP and RTP**
- **SRTP only**
- **Fallback to RTP**

SRTCP encryption

When activated, SRTCP will be encrypted.

8.1.16 Miscellaneous

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous

This area features the following components:

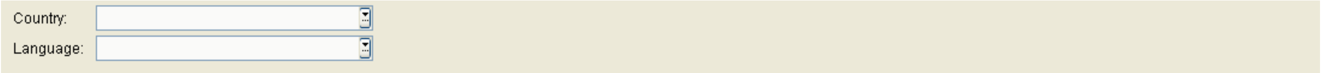
- General Data
- Possible Action Buttons
- "Country & Language" Tab
- "Messaging Services" Tab
- "SIP Error Notification" Tab
- "Display/Phone Settings" Tab
- "Help Internet URL" Tab
- "Phone Lock" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.16.1 "Country & Language" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Country & Language" Tab



Country:

Country where the workpoint is operated.

Possible options:

- **AE - United Arab Emirates**
- **AF - Afghanistan**
- **AL - Albania**
- **AM - Armenia**
- **AR - Argentina**
- **AT - Austria**
- **AU - Australia**
- **AZ - Azerbaijan**
- **BA - Bosnia and Herzegovina**
- **BD - Bangladesh**
- **BE - Belgium**
- **BG - Bulgaria**
- **BO - Bolivia**
- **BR - Brazil**
- **BY - Belarus**
- **CH - Switzerland**
- **CI - Ivory Coast**
- **CL - Chile**
- **CM - Cameroon**
- **CN - China**
- **CO - Columbia**
- **CR - Costa Rica**
- **CR - Serbia**
- **CY - Cyprus**
- **CZ - Czech Republic**
- **DE - Germany**
- **DZ - Algeria**
- **DK - Denmark**
- **EC - Ecuador**

- **EE - Estonia**
- **EG - Egypt**
- **ES - Spain**
- **FI - Finland**
- **FR - France**
- **GB - Great Britain**
- **GE - Georgia**
- **GR - Greece**
- **GT - Guatemala**
- **HN - Honduras**
- **HK - Hong Kong**
- **HR - Croatia**
- **HU - Hungary**
- **ID - Indonesia**
- **IE - Ireland**
- **IL - Israel**
- **IN - India**
- **IR - Iran**
- **IT - Italy**
- **JO - Jordan**
- **JP - Japan**
- **KE - Kenya**
- **KG - Kyrgyzstan**
- **KR - Korea**
- **KW - Kuwait**
- **KZ - Kazakhstan**
- **LB - Lebanon**
- **LK - Sri Lanka**
- **LT - Lithuania**
- **LU - Luxembourg**
- **LV - Latvia**
- **MA - Morocco**
- **MD - Moldova**
- **MK - Macedonia**
- **MV - Maldives**
- **MX - Mexico**
- **MY - Malaysia**
- **NA - Namibia**
- **NG - Nigeria**

- **NI - Nicaragua**
- **NL - Netherlands**
- **NO - Norway**
- **NP - Nepal**
- **NZ - New Zealand**
- **OM - Oman**
- **PA - Panama**
- **PE - Peru**
- **PH - Philippines**
- **PK - Pakistan**
- **PL - Poland**
- **PT - Portugal**
- **PY - Paraguay**
- **RO - Romania**
- **RU - Russia**
- **SA - Saudi Arabia**
- **SE - Sweden**
- **SG - Singapore**
- **SI - Slovenia**
- **SK - Slovakia**
- **SV - El Salvador**
- **TH - Thailand**
- **TJ - Tajikistan**
- **TN - Tunisia**
- **TR- Turkey**
- **TM - Turkmenistan**
- **TZ - Tanzania**
- **UA - Ukraine**
- **US - United States of America**
- **UY - Uruguay**
- **UZ - Uzbekistan**
- **VE - Venezuela**
- **VN - Vietnam**
- **ZA - South Africa**
- **ZW - Zimbabwe**

Language:

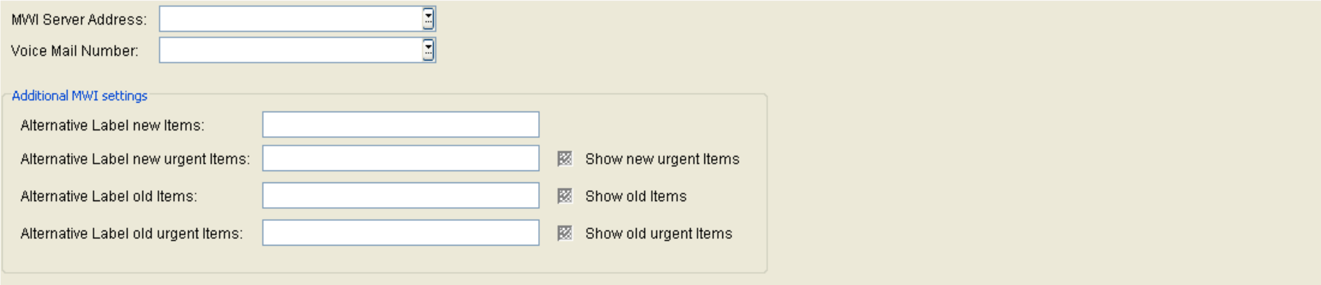
Language to be used for local applications.

Possible options:

- **bg - bulgarian**
- **ca - catalan**
- **cs - czech**
- **da - danish**
- **de - german**
- **el - greek**
- **en_GB - english (GB)**
- **en_US - english (US)**
- **en - english**
- **es - spanish**
- **et - estonian**
- **fi - finnish**
- **fr - french**
- **hr - croatian**
- **hu - hungarian**
- **it - italian**
- **ja - japanese**
- **lv - latvian**
- **mk - macedonian**
- **ms - malayan**
- **nl - dutch**
- **no - norwegian**
- **pl - polish**
- **pt - portuguese**
- **pt_Br - brazilian**
- **ro - romanian**
- **ru - russian**
- **sk - slovak**
- **sl - slovanian**
- **sr - serbian (cyrillic)**
- **sr_Latn - serbian (Latin)**
- **sv - swedish**
- **tr - turkish**
- **zh - chinese**

8.1.16.2 "Messaging Services" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Messaging Services" Tab



MWI Server Address:

Voice Mail Number:

Additional MWI settings

Alternative Label new Items:

Alternative Label new urgent Items: ☑ Show new urgent Items

Alternative Label old Items: ☑ Show old Items

Alternative Label old urgent Items: ☑ Show old urgent Items

MWI Server Address:

IP address or host name of the MWI server.

Voice Mail Number:

Phone number of the voicemail system (message server).

Additional MWI settings

Show new urgent Items

Shows the count of new urgent messages.

Show old Items

Shows the count of old messages.

Show old urgent Items

Shows the count of old urgent messages.

Alternative Label new Items

Label for the count of new messages.

Alternative Label new urgent Items

Label for the count of new urgent messages.

Alternative Label old Items

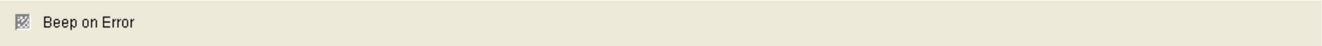
Label for the count of old messages.

Alternative Label old urgent Items

Label for the count of old urgent messages.

8.1.16.3 "SIP Error Notification" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "SIP Error Notification" Tab



☒ Beep on Error

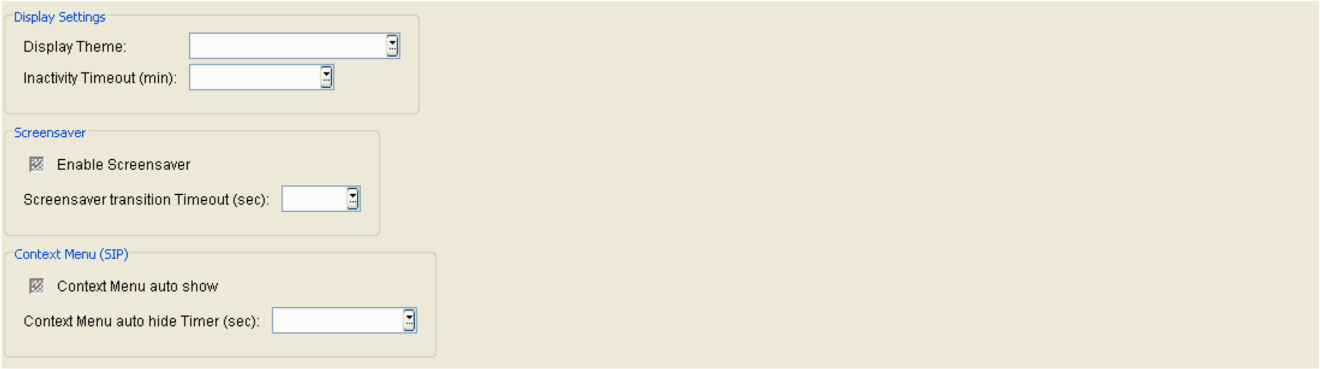
Beep on Error

Check box for activating acoustic error signaling during communication with Microsoft RTC.

Only available in SIP workpoints.

8.1.16.4 "Display/Phone Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Display/ Phone Settings" Tab



Display Settings

Display Theme

Defines the layout of the graphical user interface on OpenStage phones.

Possible options:

- **Silver Blue**
- **Anthracite Orange**

Not used Timeout (min):

Time in minutes before the screen is dimmed, if no activities have taken place on the screen until now.

Possible Options:

- **0 (no timeout)**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Screensaver

Enable Screensaver

This check box enables the screensaver.

Screensaver transition Timeout (sec)

Time interval in seconds for changing the images.

Possible Options:

- **5**
- **10**
- **20**
- **30**
- **60**

Context Menu (SIP)

Context Menu auto show

When active, the context menu will be shown automatically.

Context Menu auto hide Timer (sec)

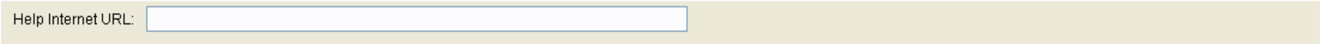
The context menu will be hidden after the timeout specified here, in seconds.

Possible Values:

- **No auto hide**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

8.1.16.5 "Help Internet URL" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Help Internet URL" Tab



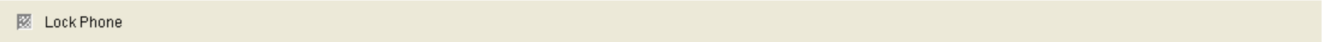
Help Internet URL:

Help Internet URL:

URL of the Web help page on the Internet containing information on the telephone.

8.1.16.6 "Phone Lock" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Phone Lock" Tab



▨ Lock Phone

Lock Phone

Locks the phone.

8.2 SIP Mobile User Interaction

In the **SIP Mobile User Interaction** area, you can configure, modify or delete mobile users. You can also log off mobile users, obtain information about logons and logoffs, create user data profiles, and define defaults for key layouts.

Call: Main Menu > Mobile Users > SIP Mobile User Interaction

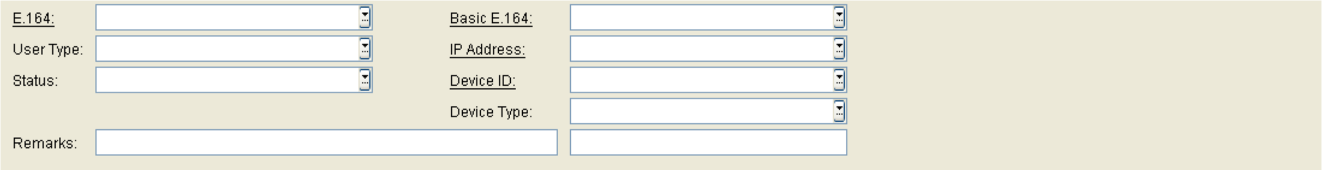
This menu consists of the following submenus:

- SIP Mobile User
- Logon/Logoff
- Automatic Logoff
- SIP User Keylayout
- Mobile User Response Test Settings

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is identical for the **SIP Mobile User** and **Logon/Logoff** interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of workpoints. The base data associated with the workpoints found is displayed in the **Object** view (no changes possible).



You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.

All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, **only** the workpoints that correspond to the specified device type and that also belong to the specified IP address range are selected.

E.164:

Complete E.164 phone number (Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

User Type:

Displays which type of data the remainder of the fields contain.

Possible options:

- **Mobility enabled Device**
  Mobility Phone data.
- **Mobile User**
  Mobile User data.

For more information on mobility, see Section 3.7, "DLS Mobility - General Information".

Status:

Displays mobility status.

Possible options:

- **Mobile User logged on**
  Mobile User data: a Mobile User is logged on.
- **Mobile User logged off**
  Mobile User data: no Mobile User is logged on.
- **Mobility enabled Device**
  Mobility Phone data: no Mobile User is logged on to the Mobility Phone.
- **Device used by Mobile User**
  Mobility Phone data: a Mobile User is logged on to the Mobility Phone.

For more information on mobility, see Section 3.7, "DLS Mobility - General Information".

Basic E.164:

E.164-Rufnummer des Mobility -Telefons.

Beispiel: **498972212345**

IP Address:

IP address of the workpoint.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

Physical MAC address of the workpoint.

Example: **00:0E:A6:85:71:80**

Device Type:

Workpoint device type.

All workpoint types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for an entry in the database.

Clear Window

Deletes the contents of all fields in the **Search** view. This deletes all previous search criteria so you can enter new criteria.

Save

Saves the changes.

Discard

Discards any changes made.

Logon Mobile User

Logs a mobile user on to a mobility terminal.

If you click this button, a dialog window appears. The terminal's E.164 phone number must be specified if a mobile user is selected in the general part of the mask. The mobile user's mobility ID is entered if a terminal is specified in the general part.

Logoff Mobile User

Logs a mobile user off a terminal.

If a mobile user is selected in the general part of the mask, it will be logged off the terminal. If a terminal is selected, the mobile user logged on to it is logged off.

Reset Mobile User

To be used in case the end device cannot be reached by the DLS. The mobile user and the phone he is currently logged onto are set to "logged off" in the DLS database.

New

Creates a new Mobile User or a default Mobile User.

Migration to Mobile User

Migrate a Basic User to a Mobile User. See also Section 16.13.4.2, "Creating Mobile Users via Migration".

Migration to Device

Migrate a logged on Mobile User to a Basic User.

Refresh

Refreshes the window contents from the database.

Delete

Delete an object.

8.2.1 SIP Mobile User

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP Mobile User

This area features the following components:

- General Data
- Possible Action Buttons
- "Mobile / Basis User" Tab
- "Archives Data" Tab
- "Response Test Settings" Tab

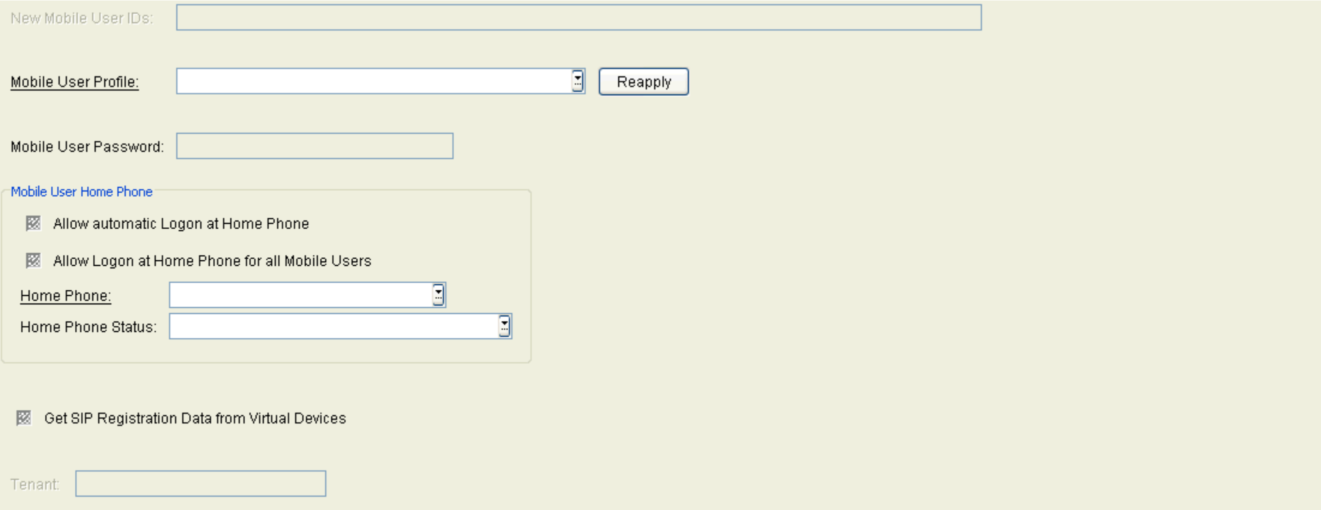
For information on general interface operation, see Section 5.4.2, "Work Area".

8.2.1.1 "Mobile / Basis User" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP Mobile User > "Mobile / Basis User" Tab

For an introduction to mobility, see Section 3.7, "DLS Mobility - General Information".

For information on mobility administration, see Section 16.13, "Configuring and Administrating Mobility".



New Mobile User IDs:

Mobile User Profile: Reapply

Mobile User Password:

Mobile User Home Phone

☒ Allow automatic Logon at Home Phone

☒ Allow Logon at Home Phone for all Mobile Users

Home Phone:

Home Phone Status:

☒ Get SIP Registration Data from Virtual Devices

Tenant:

New Mobile User IDs:

E.164 call numbers of all Mobility phones for which a Mobile User is to be created. If there is more than one Mobility phone, the E.164 call numbers are entered comma-separated.

On clicking the button ▤, a list of all available call numbers is displayed. From this table, you can select the desired numbers, similar to the multile selection in table view (see Section 5.4.2.4).

Mobile User Profile:

Selection list for the profile to be used for the Mobile User.

Reapply:

Apply the Mobile User profile to the Mobile User again. On starting this function, the DLS user will be asked whether this should be done as a merge of the data or by replacing all user data by profile/default data. If the merge option is chosen (click on "Yes"), those user parameters which are also configured in the profile are overwritten by the profile data. That user data which is not contained in the profile will not be touched. If, for instance, the profile contains additional keys, they will be added to the keys currently configured on the mobile user’s phone; but in case of concurrent key definitions, the key definitions of the profile will overwrite those currently set on the phone.

If the replace option (click on "No") is chosen instead of the merge option, those user parameters which are also configured in the profile are overwritten by the profile data. That user data which is not contained in the profile will be overwritten with default values.

Mobile User Password:

With this password, the user can log on to the phone, both at the device itself and via the WBM (Web Based Manager).

Mobile User Home Phone

Allow automatic Logon at Home Phone

If this check box is activated, the Mobile User is logged on automatically to that Home Phone whose E.164 call number has been entered under **Home Phone**.

Allow Logon at Home Phone for all Mobile Users

If actived, all Mobile Users are allowed to log on at that home phone whose E.164 number has been entered under **Home Phone**.

Home Phone

E.164 number of the Home Phone assigned to this Mobile User.

Home Phone Status

Displays the current status of the Mobile User at the Home Phone.

Possible values:

- **Mobile User logged on at Home Phone**
- **Mobile User logged off from Home Phone**

Get SIP Registration Data from Virtual Devices

If this check box is activated, data for SIP access is taken from the corresponding plug&play configuration, that is, from the virtual device which has the same E.164 number as the newly created mobile user. The access data for the SIP server is located at **IP Phone Configuration** > **Gateway/Server**.

Tenant

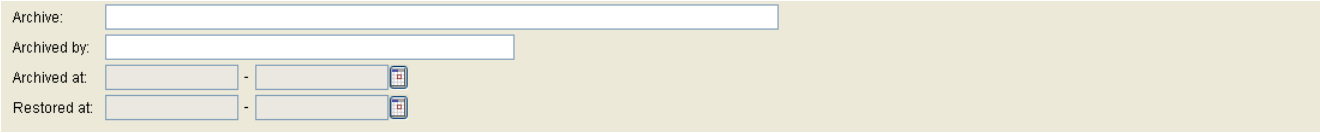
Name of the tenant the Mobile User belongs to.

8.2.1.2 "Archives Data" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP Mobile User > "Archives Data" Tab

For an introduction to mobility, see Section 3.7, "DLS Mobility - General Information".

For information on mobility administration, see Section 16.13, "Configuring and Administrating Mobility".



Archive:

Archived by:

Archived at: -

Restored at: -

Archive:

Path for the ZIP archive file from the DLS system.

Archived by:

Name of the DLS user who created the archive.

Archived at:

Indicates the date and time of the archive.

Restored at:

Displays the date and time of the archive restore.

8.2.1.3 "Response Test Settings" Tab

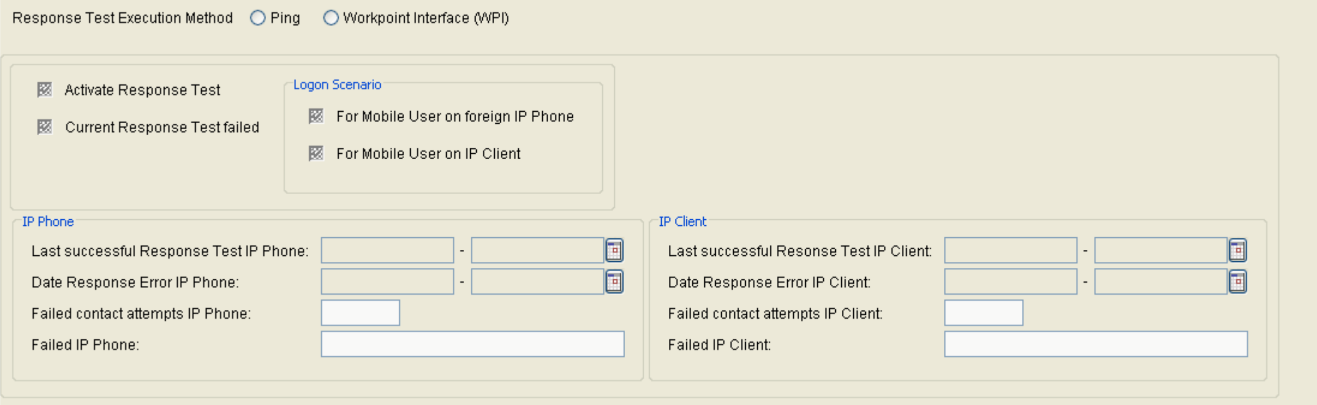
Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP Mobile User > "Response Test Settings" Tab

This functions checks if an IP Phone or IP Client to which a Mobile User is logged on is reachable by the DLS.

If the IP Phone or IP Client is unreachable according to the settings (see Section 8.2.5, "Mobile User Response Test Settings") and a Home Phone is assigned to the Mobile User, the Mobile User will be logged off from the current IP Phone or IP Client and logged on to the assigned Home Phone. This prevents the Mobile User from becoming unreachable.

A failled attempt means that within 10 minutes no conntact has been established. The Response Test failed, if the number of 'Failed contact attempt IP Phone' or 'Failed contatct attempt IP Client' is higher then the number of 'Response Test Retries' on mask 'Mobile User Response Test Settings'.

A contact attempt is considered to be failed when no contact could be established within 10 seconds. The respond test has failed when the counter **Failed contact attempts IP Phone** or **Failed contact attempts IP Client** is greater than the value of **Response Test Retries** in the mask **Mobile Users** > **SIP Mobile User Interaction** > **Mobile User Response Test Settings**.



Response Test Execution Method ○ Ping ○ Workpoint Interface (WPI)

▨ Activate Response Test

▨ Current Response Test failed

Logon Scenario

▨ For Mobile User on foreign IP Phone

▨ For Mobile User on IP Client

IP Phone

Last successful Response Test IP Phone: -

Date Response Error IP Phone: -

Failed contact attempts IP Phone:

Failed IP Phone:

IP Client

Last successful Resonse Test IP Client: -

Date Response Error IP Client: -

Failed contact attempts IP Client:

Failed IP Client:

Response Test Execution Method

- **Ping**
  The DLS tries to reach the IP Phone or IP Client via ping.
- **Workpoint Interface (WPI)**
  The DLS tries to reach the IP Phone or the IP Client via its workpoint interface by means of a ContactMe request. If the IP Phone or the IP Client sends a corresponding message, in which with the "ReasonForContact" parameter has the value "solicited", the test was successful. Otherwise, the test is considered failed.

Activate Response Test

Activates or deactivates the response test for this mobile user.

Current Response Test failed

If no contact could be established after 10 seconds, the error counter is incremented.

Logon Scenario

For Mobile User on foreign IP Phone

If activated, response tests are executed for a Mobile User at a foreign IP Phone, that is, at a phone which is not the Home Phone of this Mobile User.

For Mobile User on IP Client

If activated, response tests are executed for a Mobile User at an IP Client, that is, at an IP Client which is not the Home Phone of this Mobile User.

IP Phone

Last successful Response Test IP Phone

Date of the last successful response test for this IP Phone.

Time Response Test Error IP Phone

Date of the last failed response test for dieses IP Phone.

Failed contact attempts IP Phone

Number of failed contact attempts for this IP Phone.

Failed IP Phone

IP Address of the IP Phone that could not be reached.

IP Client

Last successful Response Test IP Client

Date of the last successful response test for this IP Client.

Time Response Test Error IP Client

Date of the last failed response test for this IP Client.

Failed contact attempts IP Client

Number of failed contact attempts for this IP Client.

Failed IP Client

IP address of the IP Client that could not be reached.

8.2.2 Logon/Logoff

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Logon/Logoff

This area features the following components:

- General Data
- Possible Action Buttons
- "History" Tab

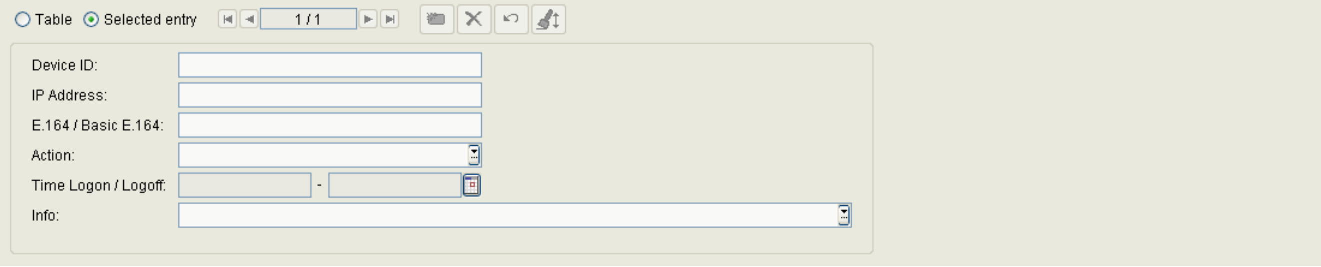
For information on general interface operation, see Section 5.4.2, "Work Area".

8.2.2.1 "History" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Logon/Logoff > "History" Tab

All successfull or failed actions concerning mobile users are logged here.

> For an introduction to mobility, see Section 3.7, "DLS Mobility - General Information".
>
> For information on mobility administration, see Section 16.13, "Configuring and Administrating Mobility".



Device ID

Device ID of the Mobility Phone with which the action logged here has proceeded (display only).

IP Address

IP address of the Mobility Phone with which the action logged here has proceeded (display only).

E.164 / Basic E.164

E.164 and Basic E.164 of the Mobility Phone with which the action logged here has proceeded (display only).

Action

Type of action that took place (display only).

Possible entries:

- **Logon**
- **Logoff**

Time Logon/Logoff

Time of the logon, logoff or the failed attempt (display only).

Info

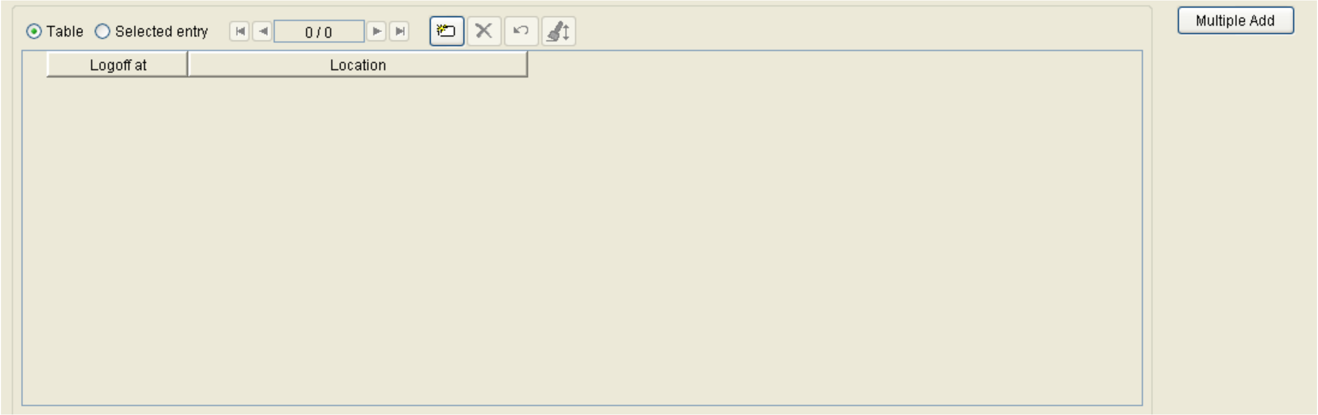
Additional information on the logon, logoff or the failed attempt (display only).

Possible entries:

- **Password or E.164 invalid**
- **Internal Error**
- **User logged in on another phone**
- **Second logon not permitted**
- **Forced logoff**
- **Forced logoff failed**
- **Forced logoff because of second logon**
- **Successful Logon**
- **Successful Logoff**
- **Forced logoff refused (phone busy)**

8.2.3 Automatic Logoff

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Automatic Logoff



This function enables the user to schedule a daily automatic logoff of all SIP mobile users for selected locations. This ensures e.g. that all devices are logged at start of work, and thus are available for SIP mobile users.

Logoff at:

Next daily logoff is scheduled on this time. The current time of the timezone defined for this location will be used.

> Switching from daylight saving time to regular time (one hour back) will not lead to a second execution of a job that has been started in the time interval hereby doubled. When switching from regular time to daylight saving time (one hour advance), a job which is scheduled for this skipped time will not be executed.

Location

Location where automatic logoff will happen at entered time. Locations are entered as described under Section 6.2.2, "Location".

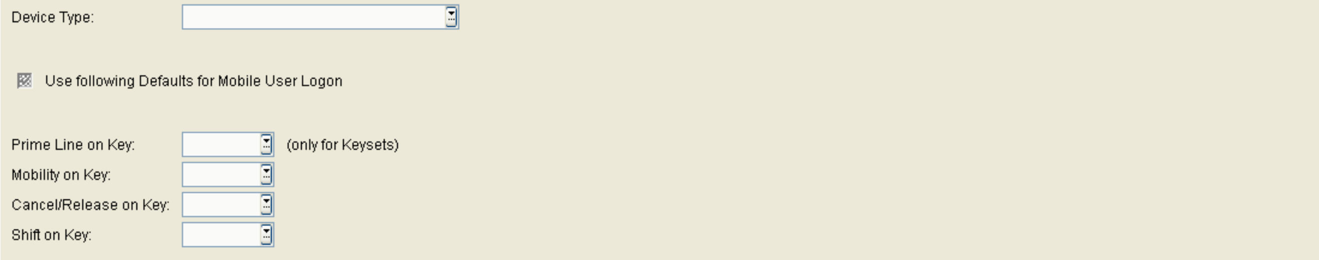
Multiple Add

Add multiple locations to one logoff time.

8.2.4 SIP User Keylayout

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP User Keylayout

> The default key layout defined here can not be overridden instantly by changing a template and reapplying the relevant user data profile while the mobile user is logged on. However, the changes will be made after the mobile user has logged off and on again.



Device Type:

☒ Use following Defaults for Mobile User Logon

Prime Line on Key: (only for Keysets)
Mobility on Key:
Cancel/Release on Key:
Shift on Key:

Device Type:

Select the device type for key layout.

Possible options:

- **OpenStage 40**
- **OpenStage 60**
- **OpenStage 80**
- **optiPoint 410 advance**
- **optiPoint 410 economy**
- **optiPoint 410 economy plus**
- **optiPoint 410 standard**
- **optiPoint 420 advance**
- **optiPoint 420 economy**
- **optiPoint 420 economy plus**
- **optiPoint 420 standard**

Use following Defaults for Mobile User Logon

Check box for activating the default setting specified below.

Prime Line on Key

Key number of the primary line key (only for phones on which the mobile user profile already has a primary line key).

Value range: **1 ... 19** or none.

Default: **5**

Mobility on Key:

Number of the key where Mobility should be programmed.

Value range: **1** ... **19** or none.

Default: **10**

Release on Key:

Configure Cancel/Release key on key

Value range: **1 ... 19** or none.

Defaults:
optiPoint 410/420 economy/economy plus/standard: **11**
optiPoint 410 advance: **18**
optiPoint 420 advance: **17**

Shift on Key:

Number of the key where Shift should be programmed.

Value range: **1** ... **19** or none.

Defaults:
optiPoint 410/420 economy/economy plus/standard: **12**
optiPoint 410 advance: **19**
optiPoint 420 advance: **18**

Possible Action Buttons

Search

Searches for all registered IP phones that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Refresh

Refreshes the content of the relevant page.

8.2.5 Mobile User Response Test Settings

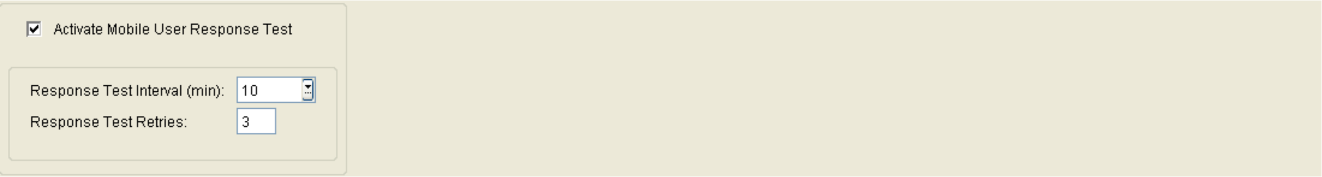
Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Mobile User Response Test Settings

Here, response tests for logged on Mobile Users can be displayed and managed. (See also Section 8.2.1.3, ""Response Test Settings" Tab")

This area features the following components:

- General Data
- Possible Action Buttons
- "Protocol" Tab

General Data



☑ Activate Mobile User Response Test

Response Test Interval (min): 10

Response Test Retries: 3

Activate Mobile User Response Test:

Central switch for activating or deactivating the Mobile User response tests.

Response Test Interval (min):

Interval in which the response tests will be performed, in minutes.

Possible Options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**
- **240**

Default value: **30**

Response Test Retries:

Number of response test retries when no connection could be established.

Value range: **0** ... **9**

Default value: **5**

Possible Action Buttons

Save

Saves the changes.

Discard

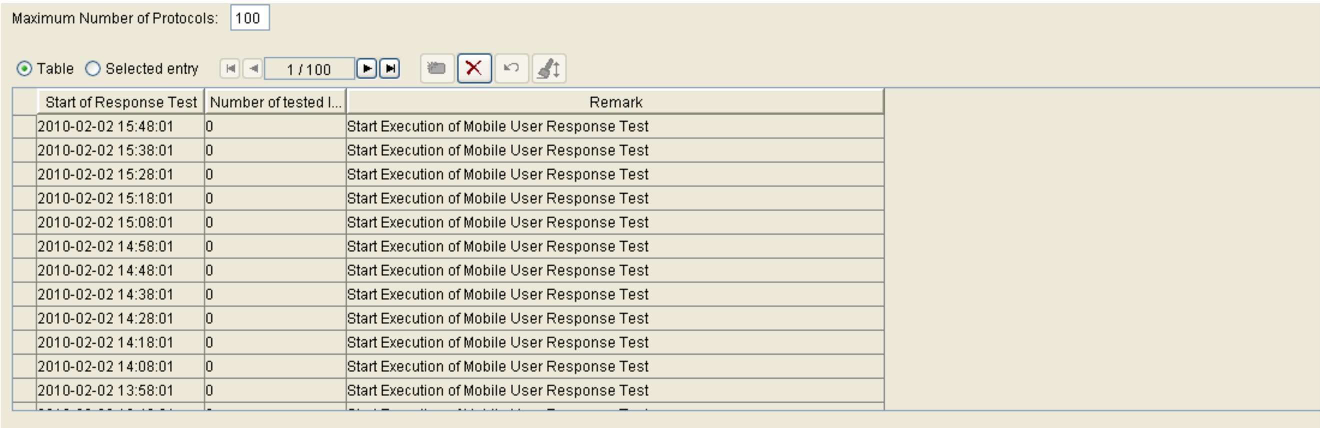
Discards any changes made.

Refresh

Refreshes the screen contents from the database.

8.2.5.1 "Protocol" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Mobile User Response Test Settings > "Protocol" Tab



Maximum Number of Protocols: 100

● Table ○ Selected entry

Start of Response Test	Number of tested I...	Remark
2010-02-02 15:48:01	0	Start Execution of Mobile User Response Test
2010-02-02 15:38:01	0	Start Execution of Mobile User Response Test
2010-02-02 15:28:01	0	Start Execution of Mobile User Response Test
2010-02-02 15:18:01	0	Start Execution of Mobile User Response Test
2010-02-02 15:08:01	0	Start Execution of Mobile User Response Test
2010-02-02 14:58:01	0	Start Execution of Mobile User Response Test
2010-02-02 14:48:01	0	Start Execution of Mobile User Response Test
2010-02-02 14:38:01	0	Start Execution of Mobile User Response Test
2010-02-02 14:28:01	0	Start Execution of Mobile User Response Test
2010-02-02 14:18:01	0	Start Execution of Mobile User Response Test
2010-02-02 14:08:01	0	Start Execution of Mobile User Response Test
2010-02-02 13:58:01	0	Start Execution of Mobile User Response Test

Maximum Number of Protocols

At most as many protocol entries as specified here are created.

Start of Response Test

Date and time of response test start

Number of tested IP Devices

Number of IP Phones or IP Clients that have been tested.

Remark

Annotation about the particular protocol entry.

8.3 User Data Administration

In this area, Mobile User data are displayed and managed. These data are not modifiable via DLS, e. g. phonebook entries. The data are sent to the DLS for storage when a Mobile User is logging off; when a Mobile User is logging on, they are sent to the end device by the DLS.

The memory requirements for each Mobile User is displayed, as well as date, device ID, and IP address of the end device. Furthermore, the total amount of used memory can be determined.

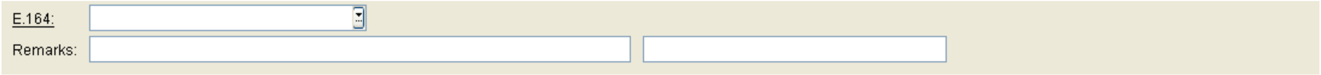
The displayed user data can be deleted. This should only be done with deleted Mobile Users.

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "Statistics" Tab

General Data

This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP phones. The base data associated with the IP phones found is displayed in **Object** view.



E.164:

Complete E.164 phone number (Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP phones that match the search criteria.

Clear Window

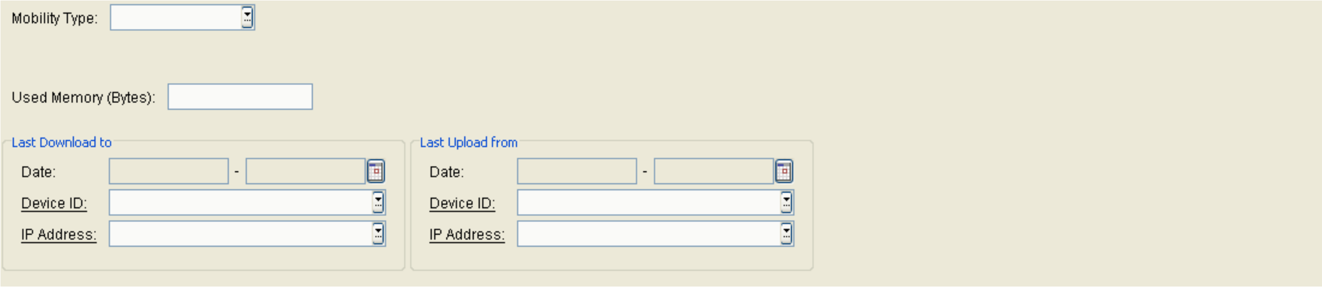
Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Determine overall Memory usage

By clicking this button, the total memory use of the user data stored in all workpoints can be determined.

8.3.1 "Statistics" Tab

Call: Main Menu > Mobile Users > User Data Administration > "Statistics" Tab



Mobility Type

Shows the mobility type (SIP or HFA Mobility).

Used Memory (Bytes):

Memory in bytes used by user data of this IP Device.

Last Download to

Date:

Date and time of the last sending of user data to the IP Device.

Device ID:

ID of the IP Device to which the user data have been sent.

IP Address:

IP address of the workpoint to which the user data have been sent.

Last Upload from

Date:

Date and time of the last saving of user data sent by the IP Device.

Device ID:

ID of the IP Device whose user data have been saved.

IP Address:

IP address of the IP Device whose user data have been saved.

8.4 Mobility Statistics

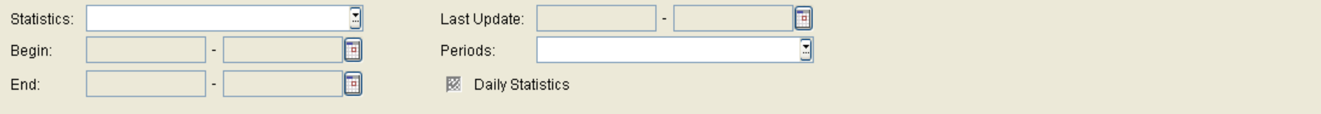
This area displays the mobility statistics. With its help, the administrator can overview all mobile users withinin a defined space of time. That way, e. g. periods of peak occupancy can be determined. For this purpose, the mobile user logon/logoff history is analyzed (see Main Menu > Mobile Users > SIP Mobile User Interaction > Logon/Logoff).

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "SIP Mobility" Tab

General Data

This part of the contents area is identical for all interfaces associated with this menu. In **Search** view, it is used for entering parameters to find a specific group of statistics. In **Object** view, the base data associated with the statistics found is displayed, or the base data for a new statistics are defined.



Statistics:

Name of the statistics.

Begin:

Begin of the time interval in which actions are observed. If **Daily Statistics** is active, this field is read-only.

End:

End of the time interval in which actions are observed. If **Daily Statistics** is active, this field is read-only.

Last Update:

Creation date of the statistics currently displayed.

Periods:

Sets the period during the observation time interval. After the expiration of each period, an entry in the table is created.

Possible Options:

- **1 min**
- **2 min**
- **3 min**
- **4 min**
- **5 min**
- **10 min**
- **15 min**
- **20 min**
- **30 min**
- **1 h**
- **2 h**
- **3 h**

- **4 h**
- **6 h**
- **24 h**

Daily Statistics

The checkbox indicates whether the statistics currently displayed is a **Daily Statistics**.

Possible Action Buttons

Search

Searches for all statistics that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the Search view before new search criteria are entered.

Delete

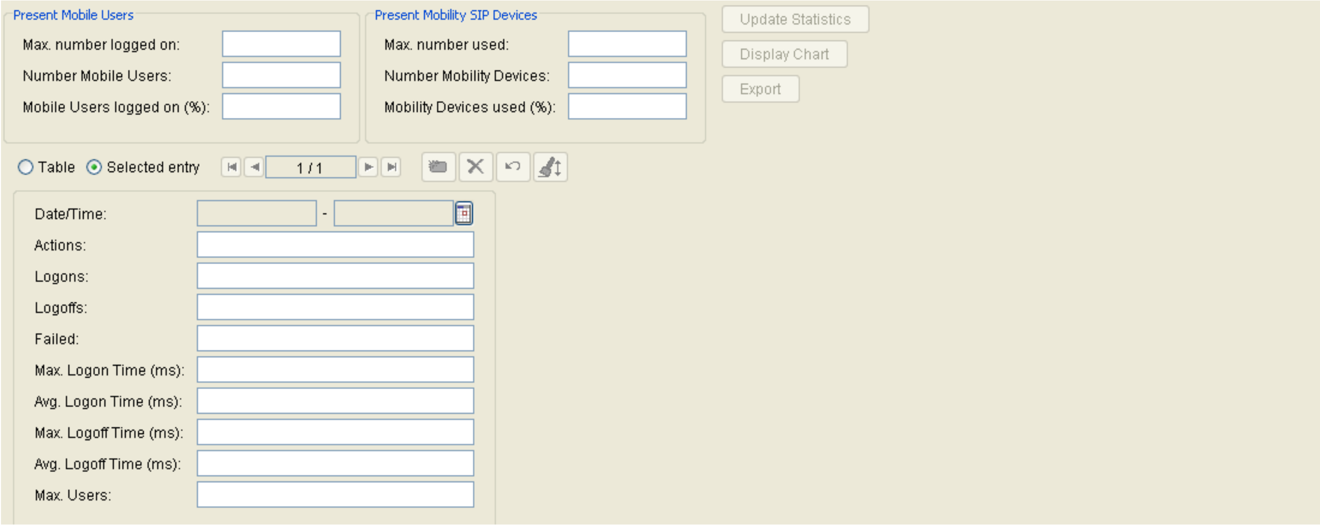
Delete the statistics currently displayed.

New

Creates new statistics.

8.4.1 "SIP Mobility" Tab

Call: Main Menu > Mobile Users > Mobility Statistics > "SIP Mobility" Tab



Present Mobile Users

Max. number logged on:

Maximum number of mobile users logged on at the same time within the observation time interval.

Number Mobile Users:

Number of mobile users extant within the observation time interval.

Mobile Users logged on (%)

Indicates the percentage of extant mobile users which have been logged on within the time interval.

Present Mobility SIP Devices

Max. number used:

Maximum number of mobility enabled SIP devices at which mobile users have been logged on within the observation time interval.

Number Mobility Devices:

Number of mobility enabled DIP devices extant at the end of the observation time interval.

Mobility Devices used (%):

Indicates the percentage of mobility enabled devices at which mobile users have been logged on within the observation time interval.

Update Statistics

If the date of **End** (of the observation time interval) is later than the date of **Last Update**, the statistics can be updated using this button. The button is inactive if the date of **Begin** and **End** are in the past.

Display Chart

Via this button, the content of the current statistics is displayed graphically.

Export

Via this button, the content of the current statistics is stored in a file in csv format. The file name will be requested in a dialog window.

Date/Time:

Time stamp with date and time at the beginning of the observation period. if, f. e., the period is set to 5 min, all successive values, actions etc. will be determined and entered in the table. At this, they are provided with the appropriate time stamp.

Actions:

Total number of actions within the period indicated.

Logons:

Number of logons within the period indicated.

Logoffs:

Number of logons within the period indicated.

Failed:

Number of failed actions within the period indicated.

Max. Logon Time (ms):

Maximum processing time for a logon within the period indicated in milliseconds.

Avg. Logon Time (ms):

Average processing time for a logon within the period indicated, in milliseconds.

Max. Logoff Time (ms):

Maximum processing time for a logoff within the period indicated, in milliseconds.

Avg. Logoff Time (ms):

Average processing time for a logoff within the period indicated, in milliseconds.

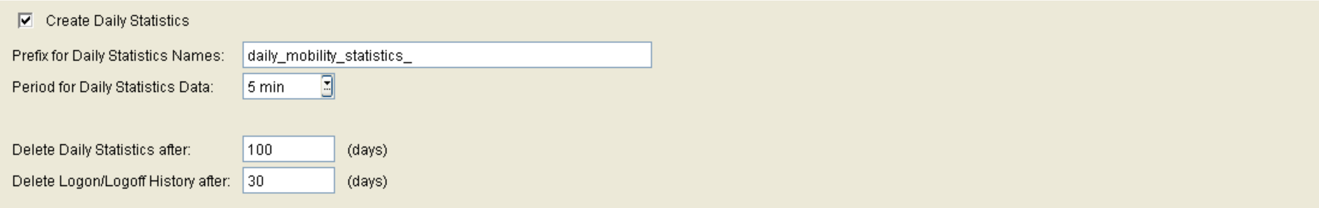
Max. Users:

Maximum number of mobile users logged on at the same time within the period indicated.

8.5 Mobility Statistics Configuration

Call: Main Menu > Mobile Users > Mobility Statistics Configuration

With this area, the daily mobility statistics (see Mobility Statistics) can be configured. The daily statistics are usually generated short after midnight. This is the time configuration changes get valid.



☑ Create Daily Statistics

Prefix for Daily Statistics Names: daily_mobility_statistics_

Period for Daily Statistics Data: 5 min

Delete Daily Statistics after: 100 (days)

Delete Logon/Logoff History after: 30 (days)

Create Daily Statistics

If this checkbox is active, a statistics according to the further parameters is created daily.

Prefix for Daily Statistics Names:

Name prefix for automatically created statistics.

Period for Daily Statistics Data:

Sets the period for the daily statistics. For each period, an entry is created in the table.

Possible Options:

- **1 min**
- **2 min**
- **3 min**
- **4 min**
- **5 min**
- **10 min**
- **15 min**
- **20 min**
- **30 min**
- **1 h**
- **2 h**
- **3 h**
- **4 h**
- **6 h**
- **24 h**

Delete Daily Statistics after:

Delete daily statistics after the number of days entered here. If 0 is entered, there will be no automatic deletion.

Delete Logon/Logoff History after:

Delete entries in the logon/logoff history after the number of days entered here. If **0** is entered, there will be no automatic deletion.

Possible Action Buttons

Save

Saves the configuration.

Discard

Discards previously unsaved modificationes in the configuration.

Refresh

Updates the display of the configuration from the database.

9 Gateways

Call: Main Menu > Gateways

This menu item consists of the following area:

- Gateway Configuration
- QoS Data Collection
- VoIP Security V1

9.1 Gateway Configuration

Call: Main Menu > Gateways > Gateway Configuration

This area features the following components:

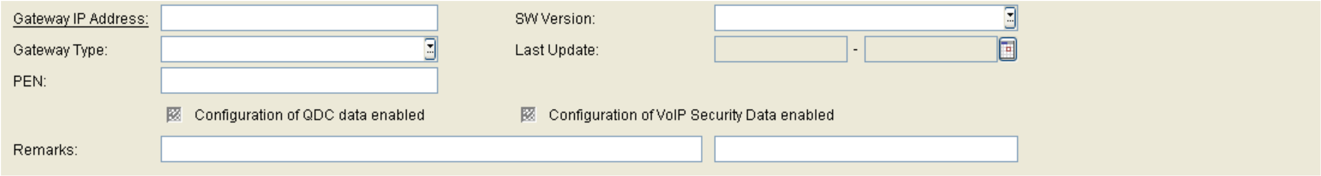
- General Data
- Possible Action Buttons
- "Gateway Connection" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area only applies to the **Gateway Configuration**. It is used for entering parameters in **Search** view to find a specific group of gateways. The base data associated with the gateways found is displayed in the **Object** view (no changes possible).


Gateway IP Address:
SW Version:
Gateway Type:
Last Update:
PEN:
☒ Configuration of QDC data enabled
☒ Configuration of VoIP Security Data enabled
Remarks:

You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.

All fields are combined internally using a logical AND. For example, if you specify a gateway type and a gateway IP address range, only **those** gateways that correspond to the specified gateway type and that also belong to the specified IP address range are selected.

Gateway IP Address:

IP address of the gateway.

Example: **192.117.1.193**

Gateway Type:

Type of the gateway.

Possible options:

- **HG1500**
- **HG3530**
- **HG3540**
- **HG3550**
- **HG3570**
- **HG3575**
- **RG2700**

PEN:

Position of the gateway board (slot).

Example: **1-17-3**

SW Version:

Gateway software version. This value is read-only in search results.

Last Update:

Time when the gateway was last updated. This value is read-only in search results.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Configuration of QDC data enabled

Check box indicating whether the gateway is capable of processing QDC data. The check box is set while reading the gateway data and can only be read.

Configuration of VoIP Security Data enabled

Check box indicating whether the gateway is capable of processing VoIP security data. The check box is set while reading the gateway data and can only be read.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all gateways that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new gateway.

Save

Saves the changes made to configuration entries.

Discard

Discards any unsaved changes.

Delete

Deletes all selected objects.

Read Gateway Data

Reads the data for all selected gateways. The gateway is entered in the DLS and can be modified using the DLS.

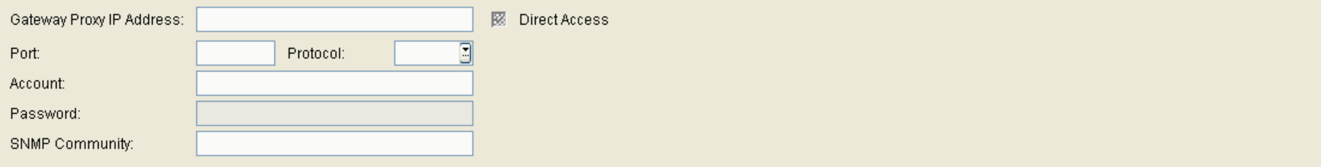
Refresh

Refreshes the content of the relevant page.

9.1.1 "Gateway Connection" Tab

Call: Main Menu > Gateways > Gateway Configuration > "Gateway Connection" Tab

> Different configuration parameters are assigned default values or deactivated (if not relevant), depending on gateway type.
> For information on configuration, see Section 16.3, "Configuring a Gateway in DLS".



Gateway Proxy IP Address:		▨ Direct Access	
Port:		Protocol:	
Account:			
Password:			
SNMP Community:			

Gateway Proxy IP Address:

Proxy IP address of the gateway.

Direct Access

If this check box is activated, the connection between HiPath 4000/HG 3550 and the DLS is via direct access and not via the Assistant.

Port:

Proxy port of the gateway.

Protocol:

Protocol used for communicating between the DLS and the gateway.

Possible options:

- **http**
- **https**

Account

User name for accessing the gateway proxy. The user ID is the first part of the URL.

Password:

Password necessary for accessing the gateway proxy.

SNMP Community:

Community string used for authentication on the SNMP server.

9.2 QoS Data Collection

Call: Main Menu > Gateways > QoS Data Collection

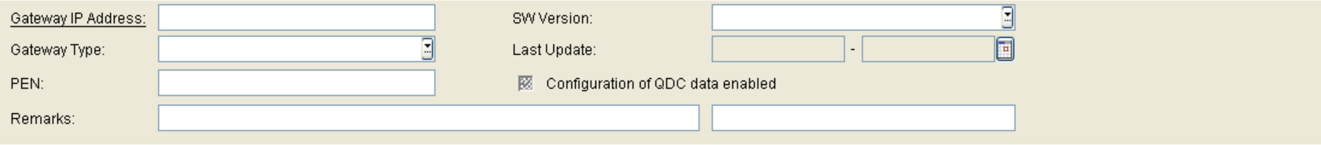
This area features the following components:

- General Data
- Possible Action Buttons
- "Server Data" Tab
- "Report Settings" Tab
- "Threshold Values" Tab

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of gateways. The base data associated with the gateways found is displayed in the **Object** view (no changes possible except under **Remarks**).



> You can use the following wildcards in all text and selection list fields in **Search** view:
>
> - * (asterisk): Stands for any sequence of characters.
> - ? (question mark): Stands for exactly one character.
> - ^ (circumflex): Stands for an empty field.
>
> Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.
>
> All fields are combined internally using a logical AND. For example, if you specify a gateway type and an IP address range, only **those** gateways that correspond to the specified gateway type and that also belong to the specified IP address range are selected.

Gateway IP Address:

IP address of the gateway.

Example: **192.117.1.193**

Gateway Type:

Type of the gateway.

Possible options:

- **HG1500**
- **HG3530**
- **HG3540**
- **HG3550**
- **HG3570**
- **HG3575**
- **RG2700**

PEN:

Position of the gateway board (slot).

Example: **1-17-3**

SW Version:

Gateway software version. This value is read-only in search results.

Last Update:

Time when the gateway was last updated. This value is read-only in search results.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Configuration of QDC data enabled

Check box indicating whether the gateway is capable of processing QDC or VoIP security data. The check box is set while reading the gateway data and can only be read.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all gateways that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Get

Loads a template that has already been saved. For more information, see Section 15.4, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.4, "Editing Templates".

Rename

Changes the name of a saved template. For more information, see Section 15.4, "Editing Templates".

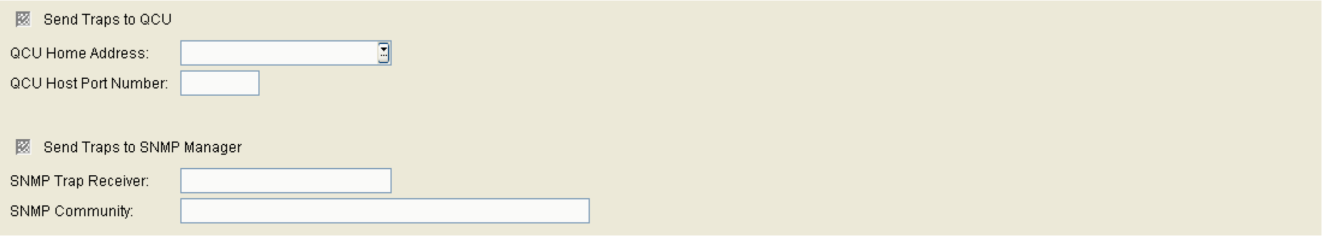
Delete

Deletes a saved template. For more information, see Section 15.4, "Editing Templates".

9.2.1 "Server Data" Tab

Call: Main Menu > Gateways > QoS Data Collection > "Server Data" Tab

More information on QDC can be found in the QDC Interface Description (P31003-H1000-X104-*-7618) and the QDC Service Manual (P31003-H1000-S104-*-7620).



Send Traps to QCU

Check box for sending traps to the QCU.

QCU Home Address:

IP address or host name of the server that logs the QDC data. Corresponds to the value entered in the gateway under **Explorer - Payload - QDC**.

QCU Host Port Number:

Port number for the server that logs the QDC data. Corresponds to the value entered in the gateway under **Explorer - Payload - QDC**.

Send Traps to SNMP Manager

Check box for sending traps to the SNMP Manager.

SNMP Trap Receiver:

Check box for activating the function that sends errors to the SNMP Manager. Matches the value entered in the gateway under **Maintenance - SNMP - Communities - Trap Communities**.

SNMP Community:

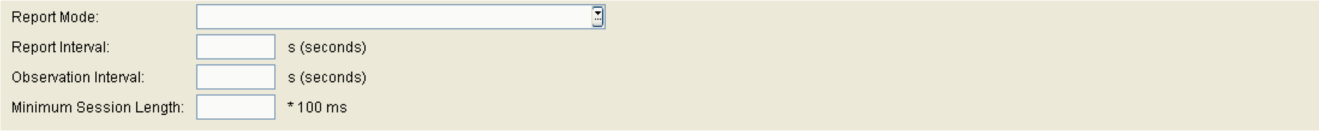
Name of the SNMP community. Matches the value entered in the gateway under **Maintenance - SNMP - Communities - Trap Communities**.

Default: **public**

9.2.2 "Report Settings" Tab

Call: Main Menu > Gateways > QoS Data Collection > "Report Settings" Tab

More information on QDC can be found in the QDC Interface Description (P31003-H1000-X104-*-7618) and the QDC Service Manual (P31003-H1000-S104-*-7620).



Report Mode:		
Report Interval:		s (seconds)
Observation Interval:		s (seconds)
Minimum Session Length:		* 100 ms

Report Mode:

Possible options:

- **Off**
  No report.
- **EOS Threshold exceeded**
  Send report at the end of the connection and when the threshold is exceeded.
- **EOR Threshold exceeded**
  Send report at the end of the reporting interval and when the threshold is exceeded.
- **EOS (End of Session)**
  Send report at the end of the connection.
- **EOR (End or Report Interval)**
  Send report at the end of the reporting interval.

Report Interval:

Value range: **0** ... **3600** seconds.

Default: **60** seconds.

Observation Interval:

Value range: **0** ... **3600** seconds.

Default: **10** seconds.

Minimum Session Length:

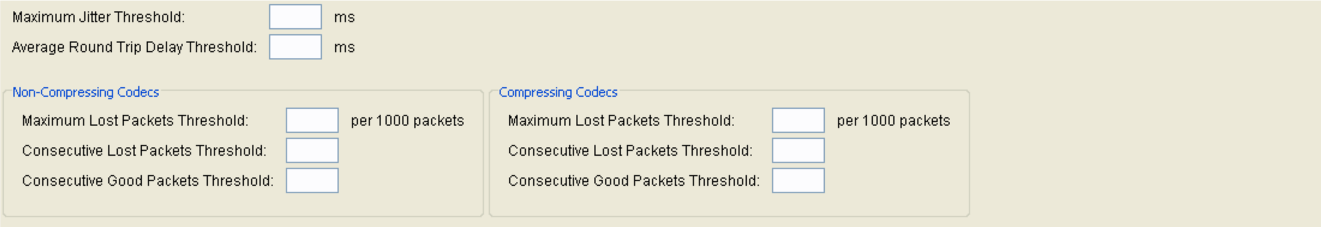
Value range: **0** ... **5000** (x 100 ms)

Default: **20** (= 2 seconds)

9.2.3 "Threshold Values" Tab

Call: Main Menu > Gateways > QoS Data Collection > "Threshold Values" Tab

More information on QDC can be found in the QDC Interface Description (P31003-H1000-X104-*-7618) and the QDC Service Manual (P31003-H1000-S104-*-7620).


Maximum Jitter Threshold: ms
Average Round Trip Delay Threshold: ms
Non-Compressing Codecs
Maximum Lost Packets Threshold: per 1000 packets
Consecutive Lost Packets Threshold:
Consecutive Good Packets Threshold:
Compressing Codecs
Maximum Lost Packets Threshold: per 1000 packets
Consecutive Lost Packets Threshold:
Consecutive Good Packets Threshold:

Maximum Jitter Threshold:

Maximum threshold in milliseconds for runtime fluctuations during data transmission to trigger a report.

Value range: **0** ... **255** ms.

Default: **15**

Average Round Trip Delay Threshold:

Average response time (in milliseconds) for signal transmission.

Default: **100**

Non-Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during uncompressed transmission.

Value range: **0** ... **255** (per 1000 packets).

Default: **10**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during uncompressed transmission.

Value range: **0** ... **255**

Default: **2**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during uncompressed transmission.

Value range: **0** ... **255**

Default: **8**

Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during compressed transmission.

Value range: **0** ... **255** (per 1000 packets).

Default: **10**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during compressed transmission.

Value range: **0** ... **255**

Default: **2**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during compressed transmission.

Value range: **0** ... **255**

Default: **8**

9.3 VoIP Security V1

Call: Main Menu > Gateways > VoIP Security V1

This area features the following components:

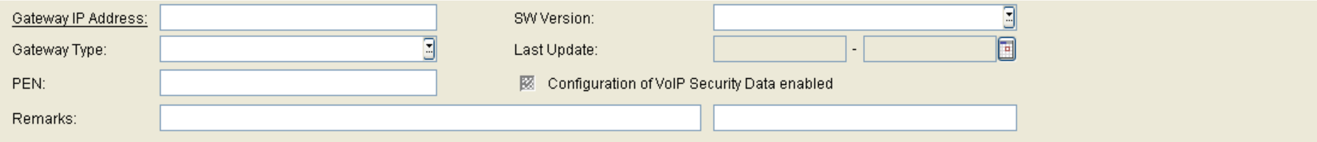
- General Data
- Possible Action Buttons
- "Voice over IP Security" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of gateways. The base data associated with the gateways found is displayed in the **Object** view (no changes possible except under **Remarks**).



☒ Configuration of VoIP Security Data enabled

> You can use the following wildcards in all text and selection list fields in **Search** view:
> - * (asterisk): Stands for any sequence of characters.
> - ? (question mark): Stands for exactly one character.
> - ^ (circumflex): Stands for an empty field.
>
> Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.
>
> All fields are combined internally using a logical AND. For example, if you specify a gateway type and an IP address range, only **those** gateways that correspond to the specified gateway type and that also belong to the specified IP address range are selected.

Gateway IP Address:

IP address of the gateway.

Example: **192.117.1.193**

Gateway Type:

Type of the gateway.

Possible options:

- **HG1500**
- **HG3530**
- **HG3540**
- **HG3550**
- **HG3570**
- **HG3575**
- **RG2700**

PEN:

Position of the gateway board (slot).

Example: **1-17-3**

SW Version:

Gateway software version. This value is read-only in search results.

Last Update:

Time when the gateway was last updated. This value is read-only in search results.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Configuration of VoIP Security Data enabled

Check box indicating whether the gateway is capable of processing VoIP security data. The check box is set while reading the gateway data and can only be read.

Remarks:

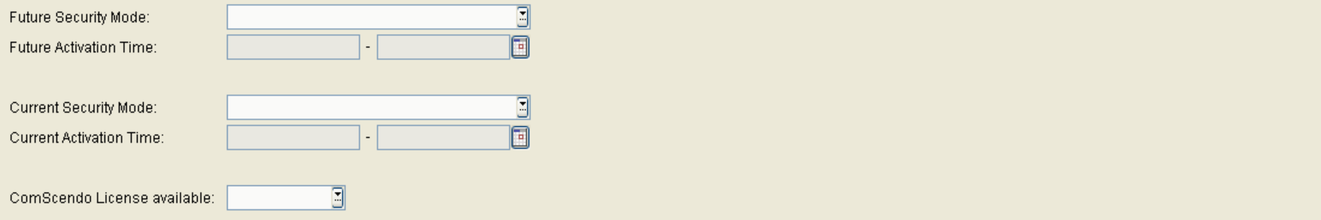
Fields for general information.

9.3.1 "Voice over IP Security" Tab

Call: Main Menu > Gateways > VoIP Security V1 > "Voice over IP Security" Tab

This interface displays only the relevant status. Security mode is administered in the **Key Distribution** area, see Section 11.1, "Key Distribution".

Further information on activating and deactivating the Security Mode may be found in Section 16.11.3, "Changing Security Mode".



Future Security Mode

New encryption mode (display only).

Possible options:

- **Encryption on**
- **Encryption off**

Future Activation Time:

Future activation time (display only).

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Current Security Mode

Current encryption mode (display only).

Possible options:

- **Encryption on**
- **Encryption off**

Current Activation Time:

Current activation time (display only).

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

ComScendo License available

Displays whether the license information could be read by the gateway, and if so, whether a license is available for VoIP security.

Possible options:

- **unknown**
  License information could not be read (DLS assumes in this case that a license is present).
- **yes**
  License available. Encryption can be switched on for this gateway (and the assigned workpoints).
- **no**
  No license available. DLS prevents encryption being switched on.

10 Software Deployment

Call: Main Menu > Software Deployment

This menu consists of the following submenus:

- Workpoint Deployment
- Manage Rules

The **Software Deployment** area is used for the user-friendly distribution of software images and other workpoint software.

> Note the difference between **Software Deployment** and **File Deployment** in the DLS interface (see Section 10.1.1 and Section 10.1.2).
>
> **Software deployment** refers to the distribution of workpoint software (IP phones and IP clients). **File deployment**, on the other hand, refers to the distribution of any binary or ASCII files that perform a certain task in the workpoint.
>
> Both functions are combined in the DLS main menu under **Software Deployment**.

For information on general interface operation, see Section 5.4.2, "Work Area".

> When distributing software for optiPoint WL2 professional workpoints, ensure that the workpoints have sufficient battery capacity. If not, it may not be possible to operate the software successfully.

10.1 Workpoint Deployment

Call: Main Menu > Software Deployment > Workpoint Deployment

The distribution of software (firmware) and other data to individual IP clients and IP phones can be controlled using the DLS.

For this to work, both the files to be distributed and the required workpoints must be registered at the DLS. The FTP server and network drives must also be registered at the DLS as these supply the data to the workpoints (see Section 6.2.4, "FTP Server Configuration" and Section 6.2.6, "Network Drive Configuration").

> Deployment via a network drive is not available in the onboard variants of the DLS on OpenScape Voice.

This area can be split into the following groups:

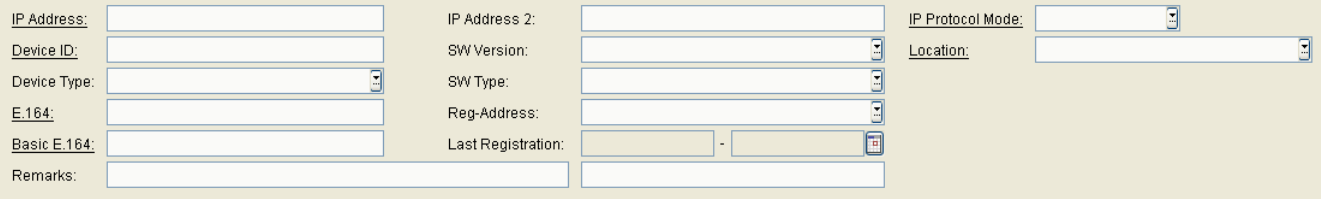
- General Data
- Possible Action Buttons
- Software and File Deployment consisting of:
  - "Software Deployment" Tab
  - "File Deployment" Tab
- Display of Inventory Data consisting of:
  - "Software Inventory" Tab
  - "LDAP Inventory" Tab
  - "MOH Inventory" Tab
  - "INCA Inventory" Tab
  - "Java Midlet Inventory" Tab
  - "Logo File Inventory" Tab
  - "SYSTEM/RINGTONE Inventory" Tab
  - "APM Inventory" Tab
  - "NETBOOT Inventory" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of workpoints. The base data associated with the workpoints found is displayed in **Object** view (no changes possible except under **Remarks**).



Some areas do not contain all of the fields described.

> You can use the following wildcards in all text and selection list fields in **Search** view:
>
> - * (asterisk): Stands for any sequence of characters.
> - ? (question mark): Stands for exactly one character.
> - ^ (circumflex): Stands for an empty field.
>
> Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.
>
> All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only the workpoints that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of the workpoint. For OpenStage, an IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

Physical MAC address of the workpoint.

Example: **00:0E:A6:85:71:80**

Device Type:

Workpoint device type.

All workpoint types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Examples: **optiPoint 410 standard**, **optiClient 130**.

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.7.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version used by the workpoint.

Example for IP phones and IP clients: **5.0.12**.

Information on the difference between the software and license version can be found in Section 15.6, "Distribution of Workpoint Software".

SW Type:

Software type used by the workpoint.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**.

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of last IP phone registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Location:

Current location of the IP Device.

Remarks:

Fields for general information.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

A search is performed in the **Search** view for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Deploy

A software or file deployment job is started in the **Object** and **Table** views. For more information, see Section 15.6, "Distribution of Workpoint Software".

10.1.1 "Software Deployment" Tab

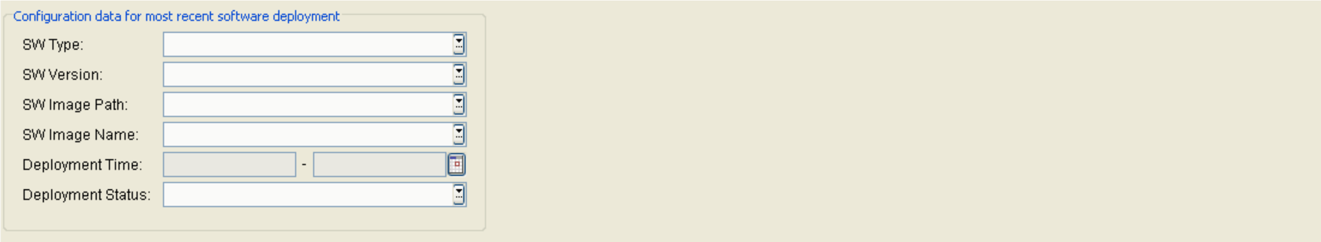
Call: Main Menu > Software Deployment > Workpoint Deployment > "Software Deployment" Tab

This tab shows the data entered for the last software deployment job that was performed for workpoints with the DLS.

"Software" is always used to refer to application software for a specific type of workpoint (for example, optiPoint 410 standard). This software is generally provided as a software image (mostly a file with the extension *.app*) that can be distributed ("deployed") to workpoints.

> All software images provided with and after the introduction of DLS contain a DLS interface for communication with the DLS (new software format). This interface is not available in any existing and previously available software images (old software format).

For an overview of all software types supported by the DLS, see Section 3.5, "Overview of Software and File Types".



Configuration data for most recent software deployment

SW Type:

SW Version:

SW Image Path:

SW Image Name:

Deployment Time: -

Deployment Status:

Configuration data for most recent software deployment

SW Type:

Software type used by the workpoint.

Example: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**

SW Version:

Software version used by the workpoint.

Example for IP phones and IP clients: **5.0.12**

SW Image Path:

Path name of the directories in which the file is saved with the software image.

Examples: **/Directory1/Subdirectory2** for IP phone files, **\Directory1\Subdirectory2** for IP client files.

SW Image Name:

File name of the software image.

Examples: **vxworks.app**, **op410std-siemens-hfa-V5.0.12-L12345678.app**

Deployment Time:

Time when the last software deployment job was started (for a calendar, see Section 5.4.2.4, "Time field with calendar button").

Deployment Status:

Result (status) of the last software deployment job.

Possible options:

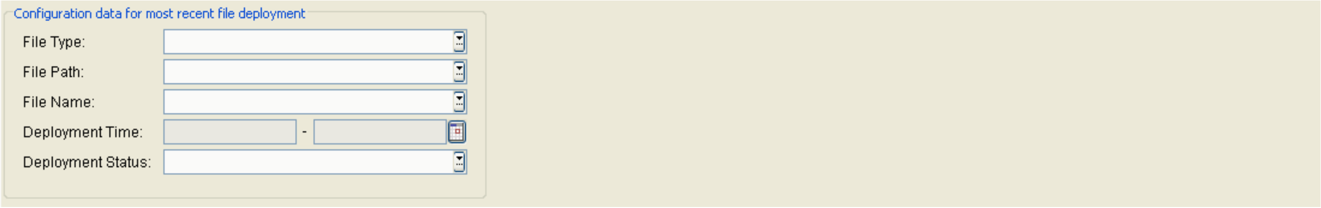
- **Deployment rejected**:
  Deployment could not be started. Possible reason: Configuration settings only permit deployment to be performed when the workpoint is idle; this was not the case.
- **Deployment initiated**:
  Deployment was started but is not yet complete.
- **Deployment finished**:
  Deployment was successfully completed.
- **Deployment failed**:
  An error occurred in the course of deployment.

10.1.2 "File Deployment" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "File Deployment" Tab

This tab shows the data (file type) entered for the last file deployment job that was performed for workpoints with the DLS.

For an overview of all file types supported by the DLS, see Section 3.5, "Overview of Software and File Types".



Configuration data for most recent file deployment

File Type:

File Path:

File Name:

Deployment Time: -

Deployment Status:

Configuration data for most recent file deployment

File Type:

Type of file (see Section 3.5, "Overview of Software and File Types").

Example: **Java Midlet** when the last action of a Java application was distributed to the IP phone.

File Path:

Path name of the directory in which the appropriate file type is saved.

Examples: **/Directory1/Subdirectory2** for IP phone files, **\Directory1\Subdirectory2** for IP client files.

File Name:

Name of the distributed file.

Deployment Time:

Time when the last software deployment job was started (for a calendar, see Section 5.4.2.4, "Time field with calendar button").

Deployment Status:

The result (status) of the last software deployment job is displayed.

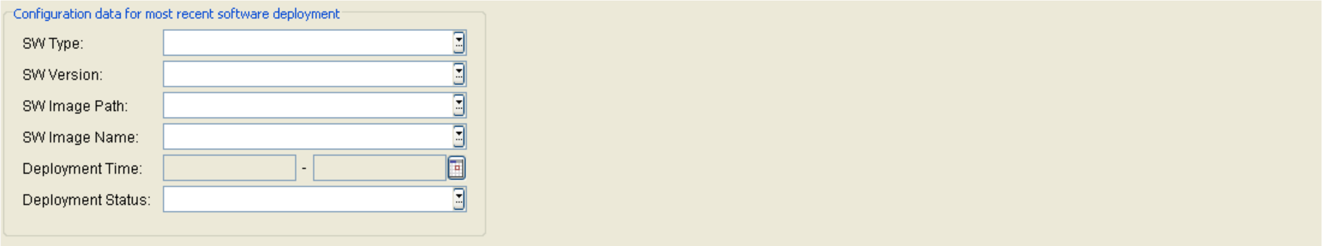
Possible status:

- **Deployment rejected**:
  Deployment could not be started.
- **Deployment initiated**:
  Deployment was started but is not yet complete.

- **Deployment finished**:
  Deployment was successfully completed.
- **Deployment failed**:
  An error occurred in the course of deployment.

10.1.3 "Software Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "Software Inventory" Tab



Inventory/Status data for software installation

SW Repository:

Address of the FTP server (for IP phones) or network computer (for IP clients) from which the software was downloaded. The address can be either an IP address or a host name.

SW Image Name:

The file name of the software downloaded.

Installation Date:

Date when the last software was downloaded or installed.

Installation Status:

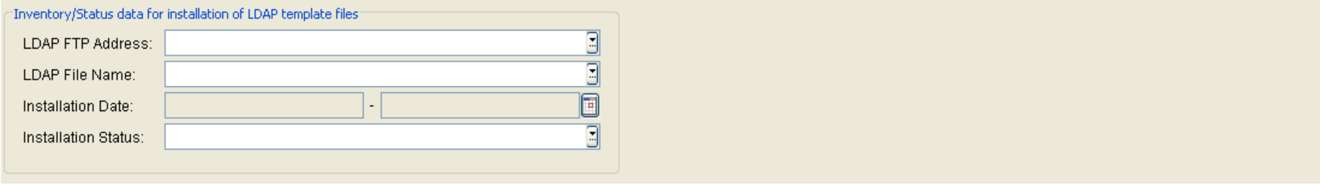
The status of software installation is displayed here.

Language Package:

Shows the installed language package.

10.1.4 "LDAP Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "LDAP Inventory" Tab



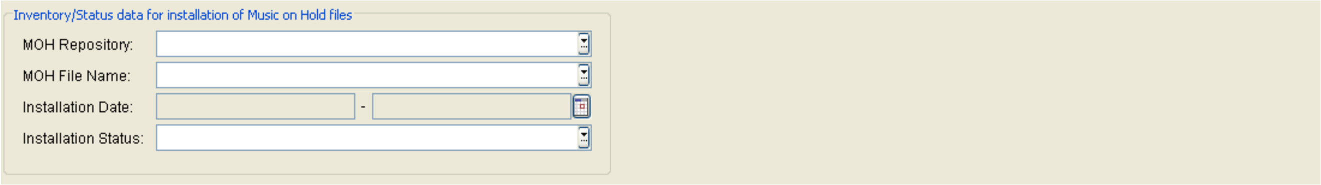
Inventory/Status data for installation of LDAP template files

LDAP FTP Address:	
LDAP File Name:	
Installation Date:	-
Installation Status:	

The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

10.1.5 "MOH Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "MOH Inventory" Tab



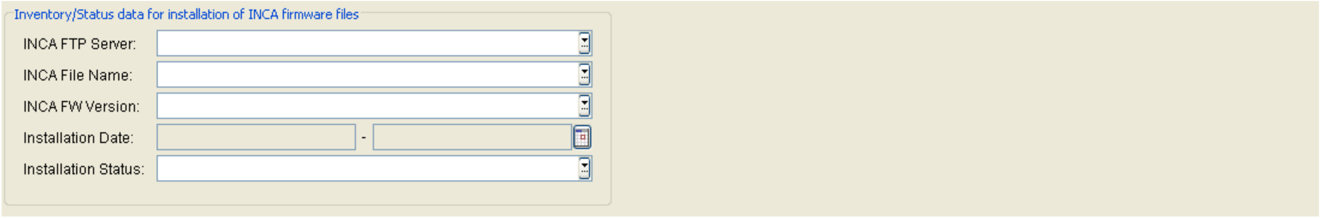
Inventory/Status data for installation of Music on Hold files

MOH Repository:	
MOH File Name:	
Installation Date:	-
Installation Status:	

> The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

10.1.6 "INCA Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "INCA Inventory" Tab



Inventory/Status data for installation of INCA firmware files

INCA FTP Server:	
INCA File Name:	
INCA FW Version:	
Installation Date:	-
Installation Status:	

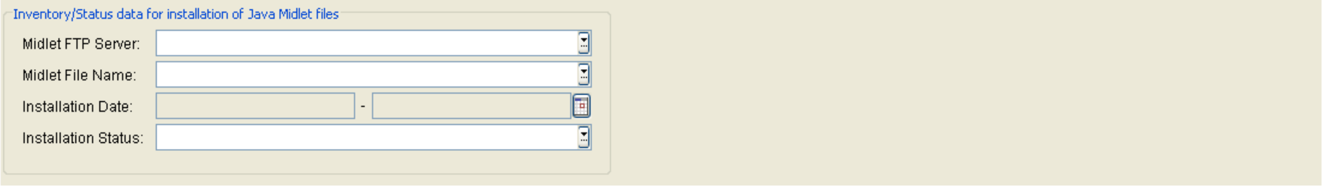
The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

INCA FW Version:

Version of INCA Firmware.

10.1.7 "Java Midlet Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "Java Midlet Inventory" Tab



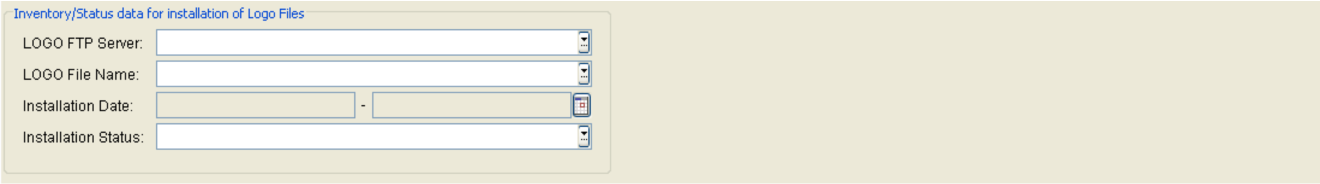
Inventory/Status data for installation of Java Midlet files

Midlet FTP Server:	
Midlet File Name:	
Installation Date:	-
Installation Status:	

The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

10.1.8 "Logo File Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "Logo File Inventory" Tab



Inventory/Status data for installation of Logo Files

LOGO FTP Server:

LOGO File Name:

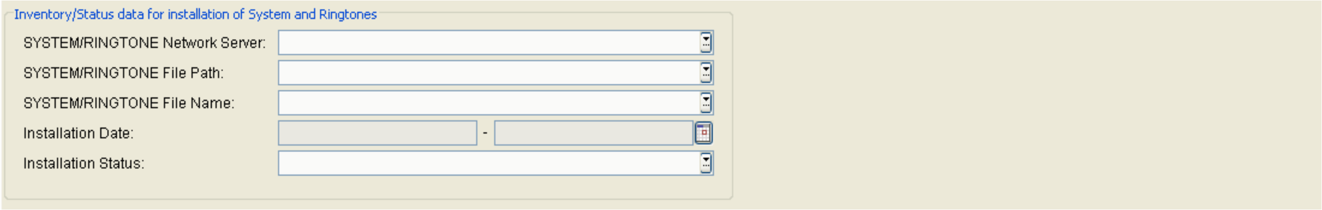
Installation Date: -

Installation Status:

The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

10.1.9 "SYSTEM/RINGTONE Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "SYSTEM/RINGTONE Inventory" Tab



Inventory/Status data for installation of System and Ringtones

SYSTEM/RINGTONE Network Server:

SYSTEM/RINGTONE File Path:

SYSTEM/RINGTONE File Name:

Installation Date: -

Installation Status:

SYSTEM/RINGTONE Network Server:

Address of the network computer from which the ringtones were downloaded. The address can be either an IP address or a host name.

SYSTEM/RINGTONE File Path:

Directory on the network computer from which the ringtones were downloaded, starting from the network path released.

SYSTEM/RINGTONE File Name:

Name of the file with ringtones that were downloaded.

Installation Date:

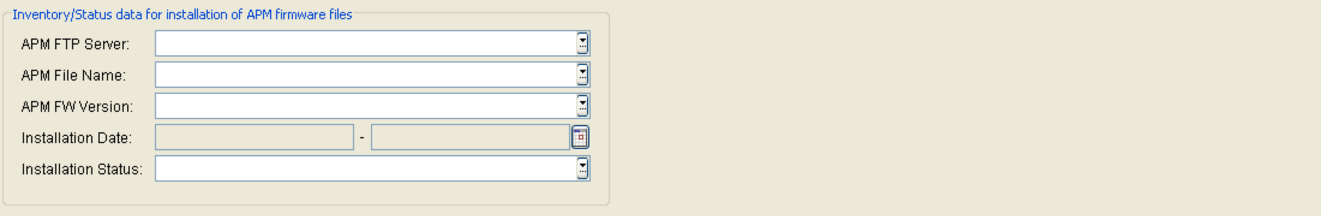
Date on which the last ringtones were downloaded or installed.

Installation Status:

The status of ringtone installation is displayed here.

10.1.10 "APM Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "APM Inventory" Tab



Inventory/Status data for installation of APM firmware files

APM FTP Server:

APM File Name:

APM FW Version:

Installation Date: -

Installation Status:

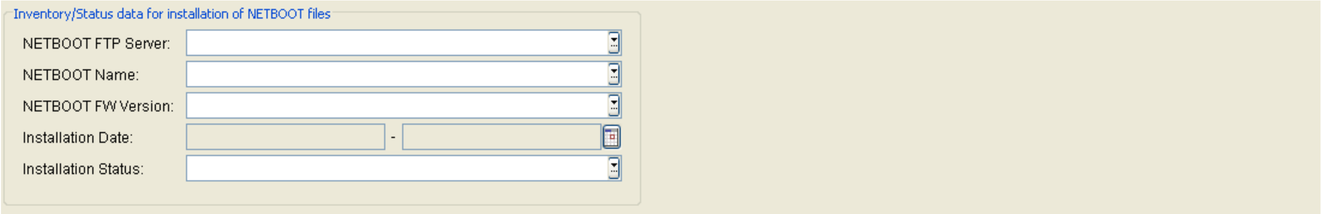
The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

APM FW Version:

Version of APM Firmware.

10.1.11 "NETBOOT Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "NETBOOT Inventory" Tab


Inventory/Status data for installation of NETBOOT files

NETBOOT FTP Server:	
NETBOOT Name:	
NETBOOT FW Version:	
Installation Date:	-
Installation Status:	

The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

NETBOOT FW Version:

Version of NETBOOT Firmware.

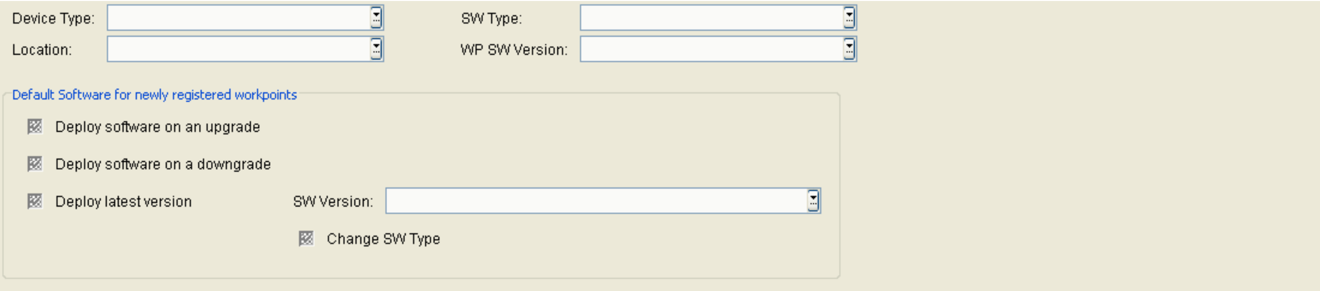
10.2 Manage Rules

Call: Main Menu > Software Deployment > Manage Rules

You can use deployment rules to control the distribution of software and limit the resulting transmission traffic.

If automatic software distribution is initiated for a workpoint, this workpoint checks first if there is a rule for the workpoint device type. If there is no rule or if the rule has been deactivated, no software is distributed to this workpoint.

For information on using deployment rules, see Section 15.6.2, "Automatic Deployment".



Device Type:
SW Type:
Location:
WP SW Version:
Default Software for newly registered workpoints
▨ Deploy software on an upgrade
▨ Deploy software on a downgrade
▨ Deploy latest version
SW Version:
▨ Change SW Type

Device Type:

Device type of the workpoints to which the rule should apply.

Examples: **optiPoint 410 standard**, **optiClient 130**.

SW Type:

Type of software type which is currently installed on the workpoints to which the rule should apply.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**.

WP SW Version:

Version of the software which is currently installed on the workpoints to which the rule should apply.

Location

Location name (IP range and gatekeeper) to which the deployment rules are assigned.

Default Software for newly registered workpoints

Deploy software on an upgrade

Check box for activating the deployment function in the case of an upgrade.
This means that deployment is performed if the software at the workpoint is **older** than the newest software or the software generally selected.

> ⓘ If you want to deactivate (but not delete) the rule, deactivate this and the following option.

Deploy software on a downgrade

Check box for activating the deployment function in the case of a downgrade.
This means that deployment is performed if the version number of the software at the workpoint is higher than the version of the software generally selected.

> ⓘ If you want to deactivate (but not delete) the rule, deactivate this and the previous option.

Deploy latest version

Check box for activating the deployment function with the latest version of a software type.
This means that during an update (downgrade), the latest software is transmitted to all workpoints that do not yet have this software version.

SW Version:

Software version of the software image selected.

Example for optiPoint and optiClient: **5.0.12**.

Change SW Type:

When switch is activated, the workpoint's software type is replaced by the one of the selected software image.

Possible Action Buttons

Search

Searches for configured deployment rules on the basis of the criteria specified.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Adds a new deployment rule.

Save

Saves the changes. A newly created rule is immediately effective.

Discard

Discards any changes made.

Delete

Deletes an existing deployment rule.

11 Voice over IP Security V1

Call: Main Menu > Voice over IP Security V1

This menu consists of the following submenu:

- Key Distribution
- Diagnosis

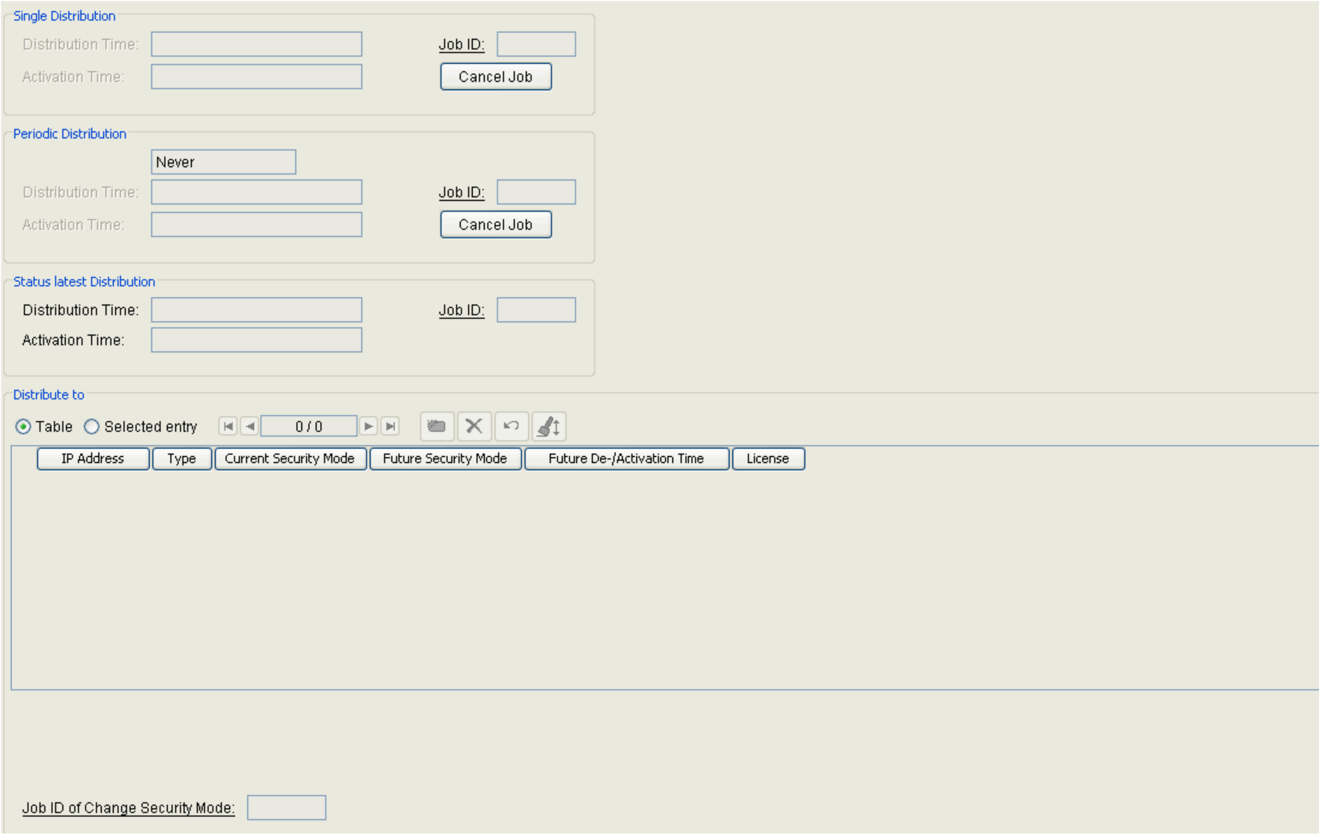
11.1 Key Distribution

Call: Main Menu > Voice over IP Security V1 > Key Distribution

This function is not available in the onboard variants of DLS on OpenScape Voice.

Use the **Voice over IP Security V1** area to administer the properties of key distribution for VoIP Security v1.

For more information on key distribution, see Section 16.11.2, "Distributing a PSS". See also Section 6.5, "Alarm Configuration".



Single Distribution

Distribution Time:

Time of single distribution (for schedule, see Section 5.4.2.4, "Time field with calendar button").

Activation Time:

Time of activation for single distribution (for schedule, see Section 5.4.2.4, "Time field with calendar button"). The time of activation must be at least 10 minutes after the distribution time.

Job ID:

Automatically allocated job ID for the single distribution of keys (display only). **PSS** is placed in front of each consecutive number.

Cancel Job

Button for discarding a job for single distribution.

Periodic Distribution

Interval between key distributions. Possible values:

- **Daily**
- **Weekly**
- **Every 2 weeks**
- **Every 4 weeks**
- **Never**

Distribution Time:

Time of periodic distribution last started (for schedule, see Section 5.4.2.4, "Time field with calendar button").

Activation Time:

Time of activation of the periodic distribution last started (for schedule, see Section 5.4.2.4, "Time field with calendar button").

Job ID:

Automatically allocated job ID for the periodic distribution of keys (display only). **PSS** is placed in front of each consecutive number.

Cancel Job

Button for discarding a job for periodic distribution.

Status latest Distribution

Distribution Time:

Time of the last single or periodic distribution (display only).

Activation Time:

Time of the last single or periodic activation for distribution (display only).

Job ID:

Automatically allocated job ID for the single or periodic distribution of keys (display only). **PSS** is placed in front of each consecutive number.

Distribute to

This list contains all of the gateways that are entered in the DLS using **Read Gateway Data** and that are capable of processing VoIP Security data (see Section 9.1.1).

IP Address

IP address of the gateway (display only).

Type

Type of the gateway (display only).

The following gateways are supported at the moment:

- **HG 1500**
- **HG 3530**
- **HG 3550**

Current Security Mode

Current encryption setting (display only).

Possible options:

- **Encryption on**
- **Encryption off**

Future Security Mode

Future encryption setting (display only).

Possible options:

- **Encryption on**
- **Encryption off**

Future De-/Activation Time

Time at which the security mode is activated or deactivated (display only).

License

Displays whether the license information could be read by the gateway, and if so, whether a license is available for VoIP security.

Possible options:

- **unknown**
  License information could not be read (DLS assumes in this case that a license is present).
- **yes**
  License available. Encryption can be switched on for this gateway (and the assigned workpoints).
- **no**
  No license available. DLS prevents encryption being switched on.

Job ID of Change Security Mode

Automatically allocated job ID for switching the security mode on/of (display only). PSS is placed in front of each consecutive number.

Possible Action Buttons

Read Gateway Data

Reads data for the selected gateway. Corresponds to the function in **Gateway Configuration**, see Section 9.1, "Gateway Configuration". Values that have changed since the last read (for example, current security mode or license) are updated in the gateway table.

Change Security Mode

Switches the security mode on or off for the selected gateway. This also applies to workpoints connected to this gateway. For more information, see Section 16.11.3, "Changing Security Mode".

Key Distribution

Enables once-off or periodic distribution to all gateways (and the connected workpoints) for which security mode is switched on at the time of distribution. For more information, see Section 16.11.2, "Distributing a PSS".

Refresh

Refreshes the content of the page.

11.2 Diagnosis

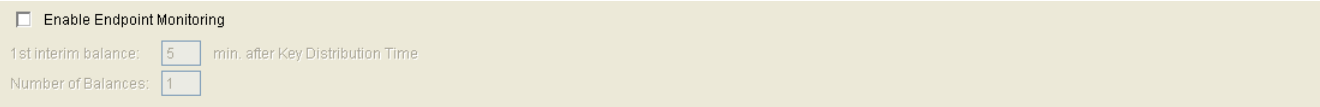
You can configure diagnostics for key distribution here.

Call: Main Menu > Voice over IP Security V1 > Diagnosis

11.2.1 "Configuration" Tab

Call: Main Menu > Voice over IP Security V1 > Diagnosis > "Configuration" Tab

A status request can be generated if network problems occur between key distribution and activation time. If a problem occurs, an alarm is generated (see Section 6.5, "Alarm Configuration").



☐ Enable Endpoint Monitoring

1st interim balance: 5 min. after Key Distribution Time

Number of Balances: 1

Enable Endpoint Monitoring

Activated: You can define the time and number of interim reports.

Deactivated: Only a final report is created. The result is stored in the log, see Section 11.2.2, ""Protocol" Tab".

1st interim balance

Time in minutes when the first interim report is created (calculated from the distribution time).

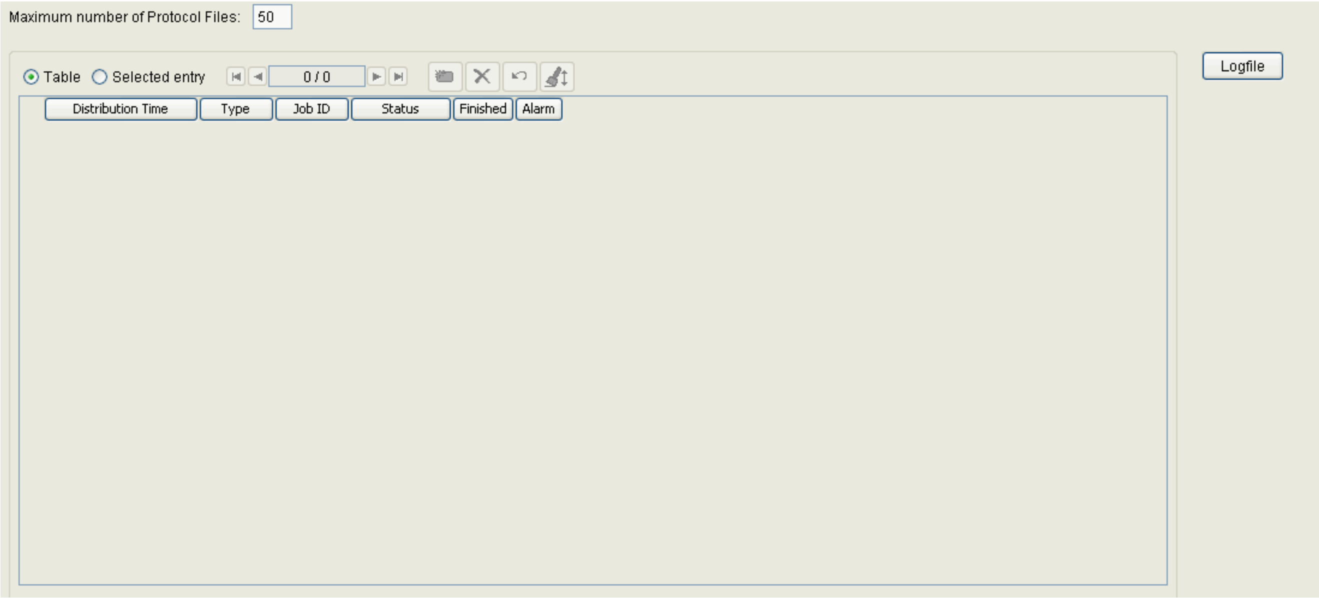
Number of Balances

Total number of reports. You can select a value between 1 and 5.

11.2.2 "Protocol" Tab

Call: Main Menu > Voice over IP Security V1 > Diagnosis > "Protocol" Tab

A log file is created for each key distribution. You can view it by clicking the **Logfile** button. You can delete the selected log file by clicking the ✕ icon.



Maximum number of Protocol Files: 50

Distribution Time

Time of key distribution.

Type

Type of key distribution.

Possible values:

- **single**
- **periodic**

Job ID

Job ID of each key distribution.

Status

Status of each key distribution. Possible values:

- **active**
- **finished**
- **cancelled**

Finished

Number of successfully finished key distributions.

Alarm

Displays if an alarm was activated (check box).

Logfile

Display the log file by clicking this button.

12 Element Manager

Call: Main Menu > Element Manager

Information on the relevant system types are managed here.

This menu consists of the following submenus:

- Element Manager Configuration

To use plug&play functionality, you must adjust a number of configurations here.

For background information on plug&play, see Section 15.5, "Workpoint Autoconfiguration (Plug&Play)".

For information on configuring the DHCP server for full plug&play, see Section 4.10.4, "DHCP Server in a Windows Environment" and Section 4.10.5, "DHCP Server in a Linux/Unix Environment".

For information on general interface operation, see Section 5.4.2, "Work Area".

12.1 Element Manager Configuration

Call: Main Menu > Element Manager > Element Manager Configuration.

Information on the different system types is entered in separate tabs in Element Manager.

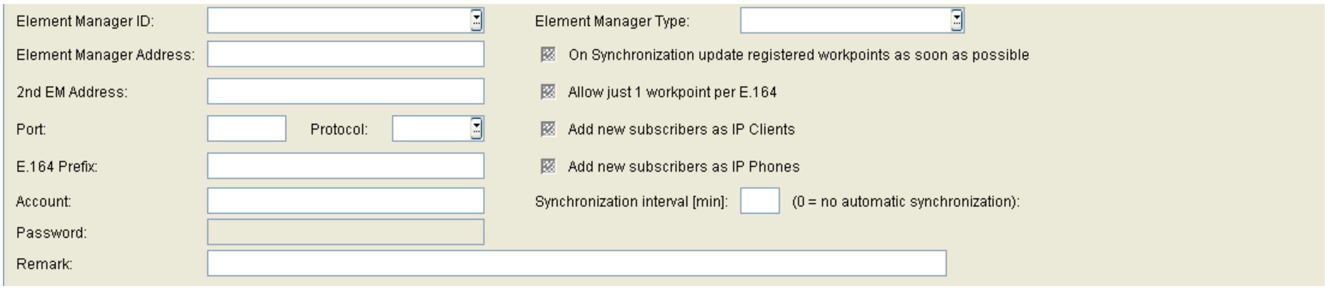
This area features the following components:

- General Data
- Possible Action Buttons
- "OpenScape Voice" Tab
- "OpenScape Voice Assistant" Tab
- "OpenScape Voice Assistant V3.0" Tab
- "HiPath 4000 Assistant" Tab
- "HiPath 3000/5000" Tab
- "OpenScape Office MX/LX" Tab
- "OpenOffice EE" Tab
- "HiPath DXWeb Pro" Tab
- "Protocol" Tab

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of Element Managers. The base data associated with the Element Managers found is displayed in the Object view (no changes possible except under Remark).

For more information on modifying the configuration, see Section 15.2, "Changing the Element Manager Configuration and Creating Jobs".



Element Manager ID:

Element Manager Address:

2nd EM Address:

Port: Protocol:

E.164 Prefix:

Account:

Password:

Remark:

Element Manager Type:

▨ On Synchronization update registered workpoints as soon as possible

▨ Allow just 1 workpoint per E.164

▨ Add new subscribers as IP Clients

▨ Add new subscribers as IP Phones

Synchronization interval [min]: (0 = no automatic synchronization):

Element Manager ID:

Freely preset ID (mandatory). Uniquely identifies the Element Manager that supplies data to the workpoints when necessary.

Element Manager Address:

Host name or IP address of the Element Manager.

2nd EM Address

Hostname or IP address of the 2nd node.

> This parameter is only relevant for geographically separated OpenScape Voice clusters.

Port:

Port used by the Element Manager for communication with the DLS. The following list specifies the ports used by the individual Element Managers for different protocols:

- OpenOffice EE: **443** (HTTPS)
- HiPath 3000 / 5000: **8085** (HTTP) or **443** (HTTPS)
- HiPath 4000 (Web service): **443** (HTTPS)
- HiPath 4000 (JDBC): **1527**
- OpenScape Voice: **8767** (HTTP)
- OpenScape Voice Assistant: **443** (HTTPS)
- OpenScape MX/LX: **443** (HTTPS)

Protocol:

Protocol used for exchanging data with the Element Manager.

Possible options:

- **http**
- **https**

E.164 Prefix:

Prefix for the E.164 number. Used for workpoints on OpenScape Voice, HiPath 3000/5000, OpenOffice EE, and HiPath DXWebPro. With Hipath 3000/5000 Version < V7, this is used only for HFA phones. If nothing is entered, the call number of the workpoint must be unique in the net. In other DLS menus, only the call number has to be entered for E.164. This field is not used for HiPath 4000; instead, the corresponding values should be entered in the **Virtual Node IDs (HFA)** table in the "HiPath 4000 Assistant" tab. If nothing is entered here, the phone number of the IP phone or IP client must be unique in the network. In other DLS interfaces, you only have to enter the phone number for E.164 fields.

Example: **4989722** (or no input).

Account:

The access code is needed for HiPath 4000 Assistant and for OpenScape Voice Assistant. The "uas_read" account is needed for HiPath 4000 Assistant; this must be activated there.

For example, JDBC ID in HiPath 4000.

Password:

Password required for Element Manager access. The entry is made by clicking the key icon in a dialog window.

For example, JDBC password in HiPath 4000.

Element Manager type:

Select the Element Manager type. You may only enter data in the corresponding tab.

Possible options:

- **HiPath 4000 (JDBC)** (see **"HiPath 4000 Assistant" Tab**)
- **OpenScape Voice Assistant V3.0** (see **"OpenScape Voice Assistant V3.0" Tab**)
- **OpenScape Voice Assistant** (see **"OpenScape Voice Assistant" Tab**)
- **HiPath 3000/5000** (see **"HiPath 3000/5000" Tab**)
- **HiPath DXWeb Pro** (see **"HiPath DXWeb Pro" Tab**)
- **OpenScape Voice** (see **"OpenScape Voice" Tab**)
- **HiPath 4000 (Webservice)** (see **"HiPath 4000 Assistant" Tab**)
- **OpenOffice EE** (see **"OpenOffice EE" Tab**)

- **OpenScape Office MX/LX** (see **"OpenScape Office MX/LX" Tab**)

On Synchronization update registered workpoints as soon as possible

If this check box is activated, jobs are immediately executed during element manager synchronization.

Allow just 1 workpoint per E.164 number

If this check box is activated, only those workpoints will be updated which have been updated before by the same Element Manager or are assigned to it (**IP Devices** > **IP Device Management** > **IP Device Configuration** > **"EM Synchronization" Tab** > **Referenced Element Manager**). Thereby, the security risk of sending registration data automatically to IP Devices with manipulated E.164 numbers is avoided, in case multiple workpoints are registered with the same E.164.

Add new subscribers as IP Clients

If this check box is activated, new IP clients are created for stations (that is, E.164 numbers) transmitted during synchronization with the telephone system but not yet present in the DLS.

Add new subscribers as IP Phones

If this check box is activated, new IP phones are created for stations (that is, E.164 numbers) transmitted during synchronization with the telephone system but not yet present in the DLS. This check box is activated by default.

Synchronization Interval [min]:

Defines the intervals for periodic synchronization between the telephone systems configured in the Element Manager and the DLS.

Value range: **10 ... 300** minutes or **0** for no automatic synchronization.

Default: **0**

Remark:

Field for general information.

Possible Action Buttons

Search

Searches for all Element Managers already entered in the DLS and that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new Element Manager configuration.

Save

Saves the Element Manager configuration.

Discard

Discards any changes made and new entries.

Delete

Deletes the Element Manager configuration.

Synchronize

Synchronization transfers registration data from the Element Manager to the DLS database. This operation runs in the background. A protocol file is created after synchronization, which can take a few minutes.

> An error message is issued if you try to start a synchronization session on the Element Manager where a session is already in progress.

Synchronization generates or modifies workpoints; it can also result in job generation. These jobs are generated without consultation.

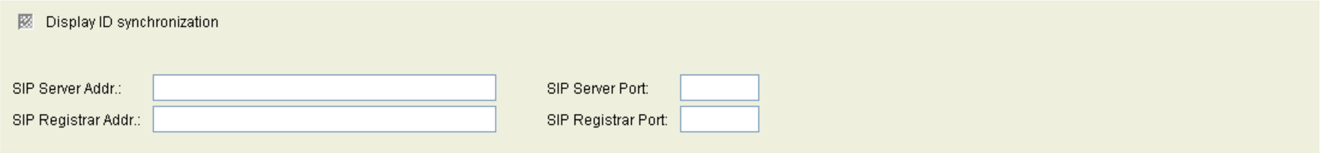
Refresh

Refreshes the contents of the current mask from the database.

12.1.1 "OpenScape Voice" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "OpenScape Voice" Tab.

For more information on modifying the configuration, see Section 15.2, "Changing the Element Manager Configuration and Creating Jobs".



☒ Display ID synchronization

SIP Server Addr.: ______ SIP Server Port: ______

SIP Registrar Addr.: ______ SIP Registrar Port: ______

Display ID synchronization

Checkbox for activating the synchronization of the display ID.

SIP Server Addr:

IP address of the SIP server. This value is not supplied by OpenScape Voice, it must be configured manually.

SIP Server Port:

Port number of the SIP server. This value is not supplied by OpenScape Voice, it must be configured manually.

SIP Registrar Addr:

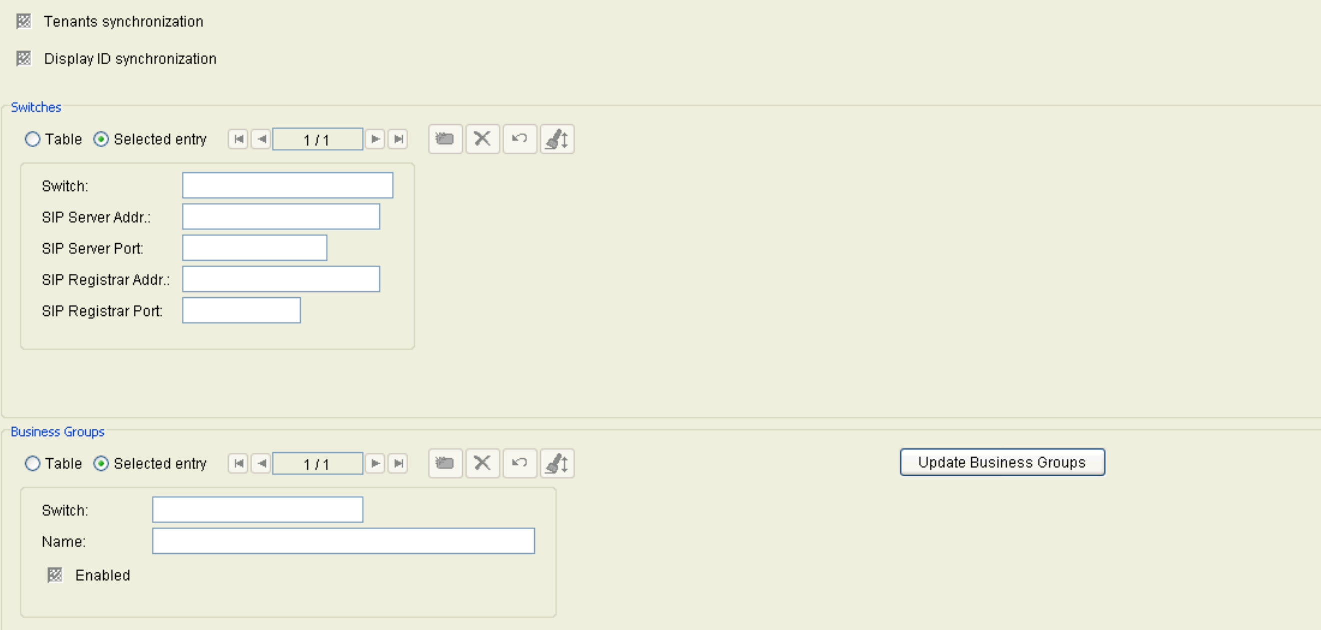
IP address of the SIP registrar. This value is not supplied by OpenScape Voice, it must be configured manually.

SIP Registrar Port:

Port number of the SIP registrar. This value is not supplied by OpenScape Voice, it must be configured manually.

12.1.2 "OpenScape Voice Assistant" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "OpenScape Voice Assistant" Tab.



▨ Tenants synchronization

▨ Display ID synchronization

Switches

○ Table ● Selected entry 1 / 1

Switch:

SIP Server Addr.:

SIP Server Port:

SIP Registrar Addr.:

SIP Registrar Port:

Business Groups

○ Table ● Selected entry 1 / 1

Update Business Groups

Switch:

Name:

▨ Enabled

Tenants synchronization

When activated, the tenants will be synchronized as well when **Update Business Groups** is executed.

Display ID synchronization

Checkbox for activating the synchronization of the display ID.

Switches

Switch

Switch name of the administrated switch. The entry is optional. When clicking **Update Business Groups**, it will be set by OpenScape Voice Assistant. The switch name is case-sensitive and must match to that one defined inside the OpenScape Voice Assistant.

SIP Server Addr:

IP address or hostname of the SIP server. This value is not supplied by OpenScape Voice, it must be configured manually.

SIP Server Port:

Port number of the SIP server. This value is not supplied by OpenScape Voice, hence it must be configured manually.

SIP Registrar Addr:

IP address or hostname of the SIP registrar. This value is not supplied by OpenScape Voice, hence it must be configured manually.

SIP Registrar Port:

Port number of the SIP registrar. This value is not supplied by OpenScape Voice, hence it must be configured manually.

Business Groups

Name

Name of Business Group.

Enabled

Only enabled Business Groups will be synchronized.

Update Business Groups

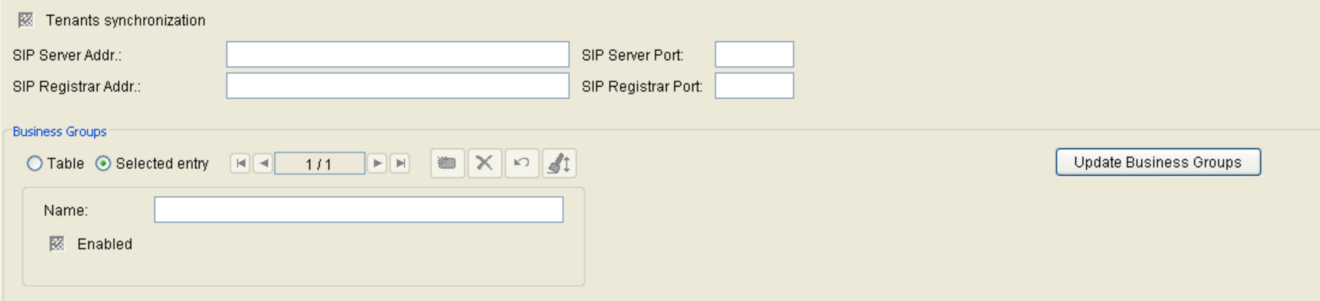
Stations are sorted into business groups. Before you start a synchronization session, you must first find out which business groups are available and then activate the relevant check boxes. If **Tenants synchronization** is activated, the tenants will be synchronized as well. The refresh is performed in the background; the protocol file is only created at the end. It may take a few minutes to provide this file.

> Synchronization cannot be started while business groups are being refreshed. If you try, however, an appropriate advisory message appears.

12.1.3 "OpenScape Voice Assistant V3.0" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "OpenScape Voice Assistant V3.0" Tab.

This configuration mask is valid for OpenScape Voice Assistant V3.0 and lower.


☒ Tenants synchronization

SIP Server Addr.:

SIP Server Port:

SIP Registrar Addr.:

SIP Registrar Port:

Business Groups

○ Table ● Selected entry 1 / 1

Name:

☒ Enabled

Tenants synchronization

During **Update Business Groups**, the tenants will be synchronized as well.

SIP Server Addr:

IP address of the SIP server. This value is not supplied by Open Scape Voice, but must be configured manually.

SIP Server Port:

Port number of the SIP server. This value is not supplied by Open Scape Voice, but must be configured manually.

SIP Registrar Addr:

IP address of the SIP registrar. This value is not supplied by Open Scape Voice, but must be configured manually.

SIP Registrar Port:

Port number of the SIP registrar. This value is not supplied by Open Scape Voice, but must be configured manually.

Business Groups

Name

Name of the Business Group.

Enabled

Only enabled Business Groups will be synchronized.

Update Business Groups

Stations are sorted into business groups. Before you start a synchronization session, you must first find out which business groups are available and then activate the relevant check boxes. If **Tenants synchronization** is activated, the tenants will be synchronized as well. The refresh is performed in the background; the protocol file is created not until the end. It may take a few minutes to provide this file.

> Synchronization cannot be started while business groups are being refreshed. If you try anyhow, an appropriate advisory message appears.

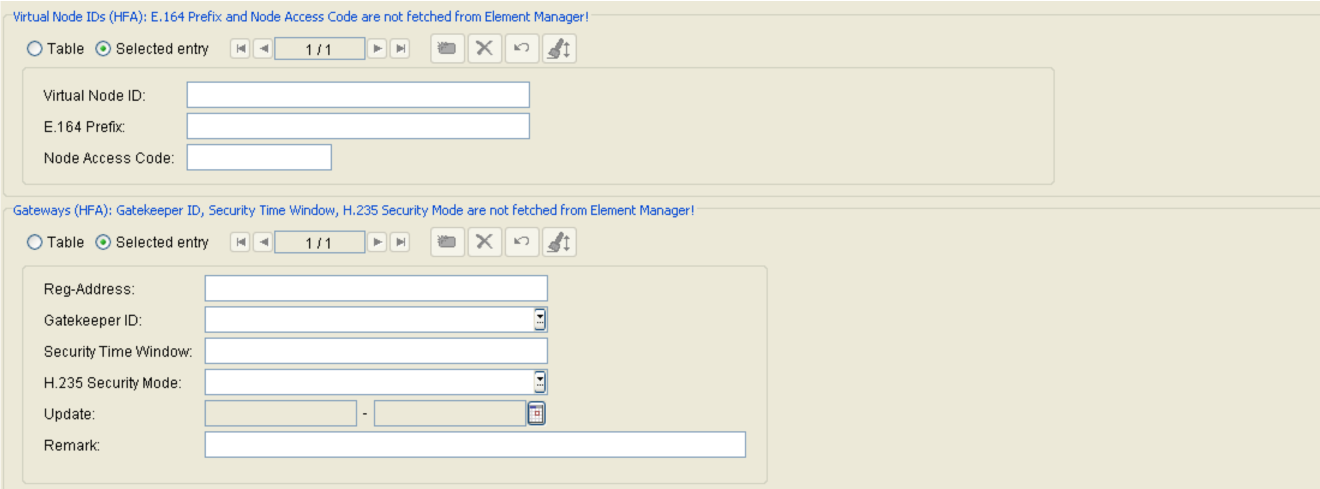
12.1.4 "HiPath 4000 Assistant" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "HiPath 4000 Assistant" Tab.

> The synchronization of DLS Elementmanager data with those of HiPath 4000 Assistant (H4K Assistant) is possible only if the data within the H4K Assistant are synchronized. That is, the upload status found in H4K Assistant under **Configuration Management** > **Network** > **System** > **Basic Data** must be SYNCHRONOUS. Otherwise, the synchronization of the data within the H4K Assistant by means of AMO UPLOA must be started first by the H4K Assistant action "Upload".

> The settings of this tab are also valid for HiPath 4000 V6.

For more information on modifying the configuration, see Section 15.2, "Changing the Element Manager Configuration and Creating Jobs".



Virtual Node IDs (HFA): E.164 Prefix and Node Access Code are not fetched from Element Manager!

○ Table ● Selected entry 1 / 1

Virtual Node ID:

E.164 Prefix:

Node Access Code:

Gateways (HFA): Gatekeeper ID, Security Time Window, H.235 Security Mode are not fetched from Element Manager!

○ Table ● Selected entry 1 / 1

Reg-Address:

Gatekeeper ID:

Security Time Window:

H.235 Security Mode:

Update: -

Remark:

Virtual Node IDs (HFA): E.164 Präfix and Node Access Code are not fetched from Element Manager!

Virtual Node ID

ID of the virtual node if a HiPath 4000 is distributed across several virtual nodes and different CO accesses are used within the node. With this solution, you can generate unique E.164 numbers for all nodes by creating different subscriber phone number/node number combinations. This value is supplied by HiPath 4000.

If entries are not available for either **Virtual Node ID** or **E.164 Prefix**, no HFA workpoints are transferred. If entries are not available for **Virtual Node ID**, but there is an entry for **E.164 Prefix**, all HFA workpoints as assigned this prefix.

E.164 Prefix

Prefix for the E.164 number. This value is not supplied by HiPath 4000 - it must be configured.

If the table is empty or a **virtual node ID** is entered without an **E.164 prefix**, no workpoints are created. If a line is present containing just one **E.164 prefix** and no **virtual node ID**, all HFA workpoints are assigned this prefix (default prefix). If there are other entries, however, with one **virtual node ID** and one **E.164 prefix** each, the corresponding prefix is used for each one. The default prefix is used for lines for which only the **virtual node ID** is set without an assigned **E.164 prefix**.

If the E.164 prefix is modified and there are workpoint entries for it, then all associated E.164 numbers are immediately adapted (the E.164 is composed of the extension and the E.164 prefix). Depending on the number or workpoints, this process can take a few minutes but runs in the background. Synchronization cannot be performed during this time. If you try, however, an appropriate error message appears.

Node Access Code

Node Access Code for numbering plan.

Gateways (HFA): Gatekeeper ID, Security Time Window, H.235 Security Mode are not fetched from Element Manager!

Reg-Address:

Host name or the gateway server address. This value is supplied by HiPath 4000.

Gatekeeper ID

Unique gatekeeper ID. This value is not supplied by HiPath 4000, it must be configured manually.

Security Time Window:

Indicates the maximum time difference permitted between the individual devices that should run synchronously in H.235. This value is not supplied by HiPath 4000, it must be configured manually.

H.235 Security Mode:

Voice encryption setting. This value is not supplied by HiPath 4000, it must be configured manually.

Possible options:

- **None**
  No voice encryption.

- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Update

Time of the last PBX or gateway server update.

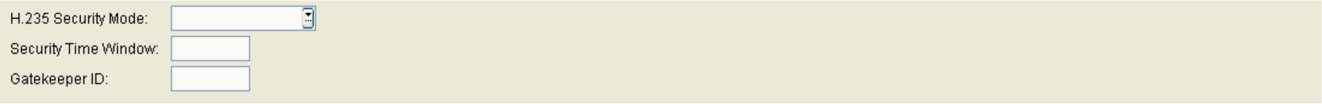
Remark

Field for general information.

12.1.5 "HiPath 3000/5000" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "HiPath 3000/5000" Tab.

For more information on modifying the configuration, see Section 15.2, "Changing the Element Manager Configuration and Creating Jobs".



H.235 Security Mode:

Security Time Window:

Gatekeeper ID:

H.235 Security Mode:

Voice encryption setting. This value is not supplied by HiPath 3000/5000, it must be configured manually.

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Security Time Window:

Indicates the maximum time difference permitted between the individual devices that should all run synchronously in H.235. This value is not supplied by HiPath 3000/5000, it must be configured manually.

Gatekeeper ID:

Gatekeeper ID. This value is not supplied by HiPath 3000/5000, it must be configured manually.

12.1.6 "OpenScape Office MX/LX" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "OpenScape Office MX/LX" Tab.

No additional data are required for OpenScape Office MX/LX

No additional data is required for OpenScape Office MX/LX.

12.1.7 "OpenOffice EE" Tab

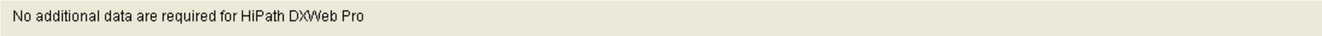
Call: Main Menu > Element Manager > Element Manager Configuration > "OpenOffice EE" Tab.

No additional data are required for OpenOffice EE

No additional data is required for OpenOffice EE.

12.1.8 "HiPath DXWeb Pro" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "HiPath DXWeb Pro" Tab.



No additional data are required for HiPath DXWeb Pro

No additional information is required for HiPath DXWebPro.

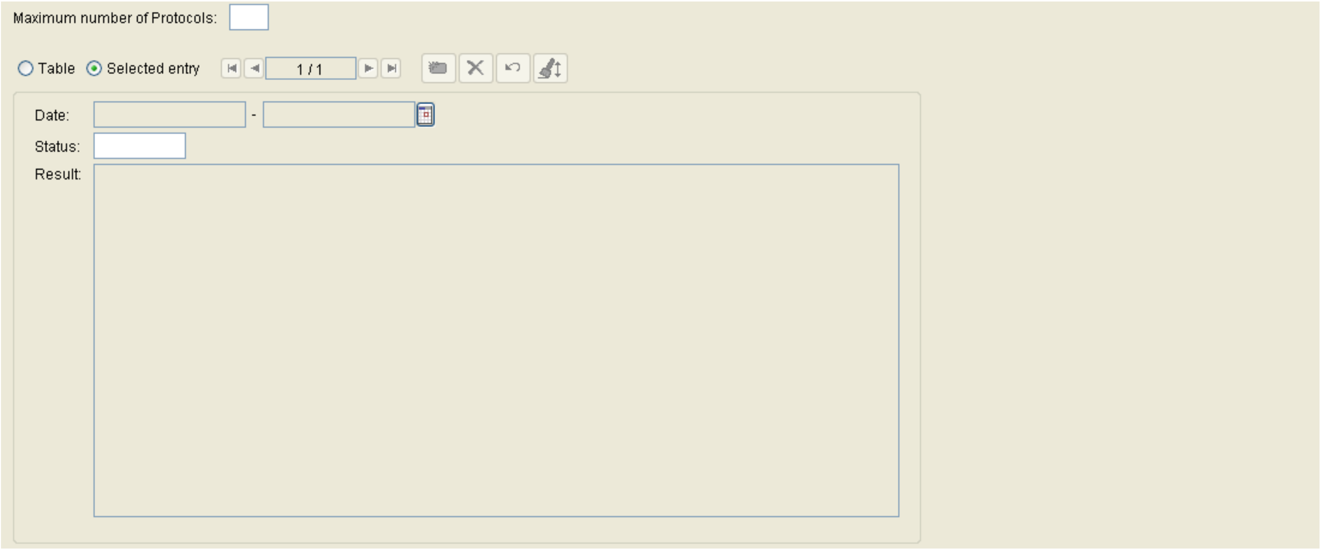
Interface description

The HiPath DXWeb Pro data (reg. address, station phone number, user password, E.164 prefix) is transmitted to the DLS via a database table. First, the system checks if a table called "DLS" exists in an Access database called "HiPath DX" (JDBC URL=jdbc:odbc:HiPathDX) on the PC where DLS is installed. If not, the system expects to find the data in the internal DLS database ("DLS" table). For compatibility reasons, both options and tables are present. Newer versions of HiPath DXWeb Pro use the Access database. If the DLS determines that the Access database/table is in use, it deletes the "DLS" table from the internal DLS database and blocks the option of working with older HiPath DXWebPro versions.

If the E.164 prefix is not supplied by the DX, the **E.164 Prefix (HFA)** parameter from the DLS mask is used. The E.164 prefix and the station phone number together produce the complete E.164 number.

12.1.9 "Protocol" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "Protocol" Tab



Maximum number of Protocols

Maximum number of protocol files.

Value range: 1 ... 20.

Date

Time of synchronization with the Element Manager identified in the **Element Manager ID** column.

Status

Identification status. This column may contain one of the following values:

- **OK**
- **Not OK**
- **Cancelled**
- **OK (partially failed)**

Result

Contents of the protocol file.

Possible Action Buttons

Logfile

Click this button to view the log file.

13 Profile Management

Call: Main Menu > Profile Management

This menu consists of the following submenus:

- Device Profile
- User Data Profile
- Template Overview

13.1 Device Profile

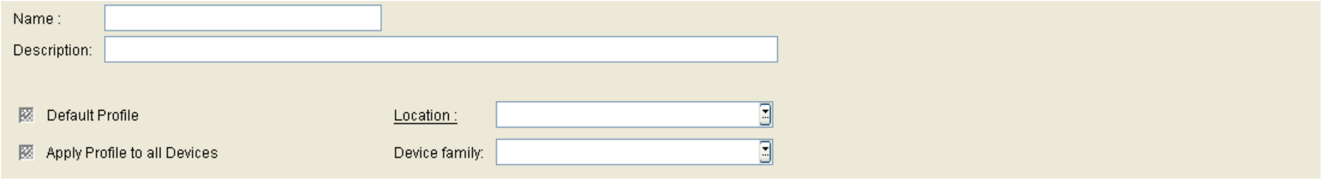
Call: Main Menu > Profile Management > Device Profile

This area features the following components:

- General Data
- Possible Action Buttons
- "Templates" Tab
- "Supported Devices of IP Device" Tab
- "Tenants" Tab

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of profiles, and for entering parameters which are valid for all tabs. The base data associated with the profiles found is displayed in the Object view.



Name :

Description:

▨ Default Profile

Location :

▨ Apply Profile to all Devices

Device family:

Name:

Profile name.

Description:

Brief description of the profile.

Default Profile

If this check box is activated, the profile is also used on IP devices that have not entered this profile under **IP Devices** > **IP Device Management** > **IP Device Configuration** > **"Profile" Tab** > **Device Profile**. The profile can only be used if the location and device type for the profile and the IP device match - unless the switch **Apply Profile to all Devices** is active. This profile is also used when registering a IP device for which the **Apply Default Profiles at IP Device Registration** check box is activated (**IP Devices** > **IP Device Management** > **IP Device Configuration** > **"General" Tab**).

To configure settings for all locations, create profiles and assign the **Default Location** to them. These profiles are then applied to all IP devices which have the appropriate device type, resp. to all IP devices, if the switch **Apply Profile to all Devices** is active. You can configure further, location-specific settings by creating profiles for specific locations. These profiles will, if applicable, overwrite the settings of those profiles which are assigned to the **Default Location**.

To use Location Service IP Infrastructure, a default device profile has to be defined and assigned to the IP Infrastructure location.

Apply Profile to all Devices

If this check box is activated, the current default is assigned to all devices that are not entered in the **Supported Devices** list.

Location

Location where the selected profile should apply as the default profile.

Device Family

The profile is valid for the device family specified here.

Possible options:

- **IP Phone**
- **IP Client**
- **IP Gateway**

Possible Action Buttons

Search

Searches for Device Profiles that meet the search criteria.

Clear Window

Deletes the content of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new Device Profile.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Export Profile

Export the selected Device Profiles to a file in zip format.

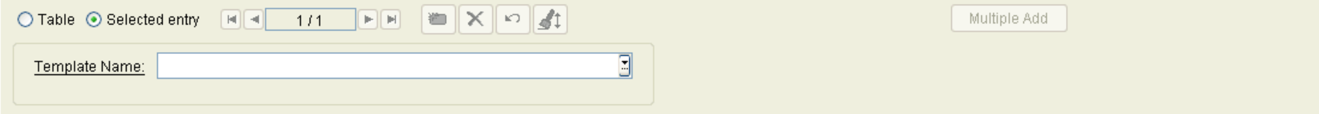
Import Profile

Import a Device Profile from a file in zip format.

13.1.1 "Templates" Tab

Call: Main Menu > Profile Management > Device Profile > "Templates" Tab

You can define an appropriate template here. You can add another template in the **New** and **Object** view with the ▭ button and delete it with the ☒ button.



○ Table ● Selected entry 1 / 1

Template Name:

Template Name

Name of the selected template.

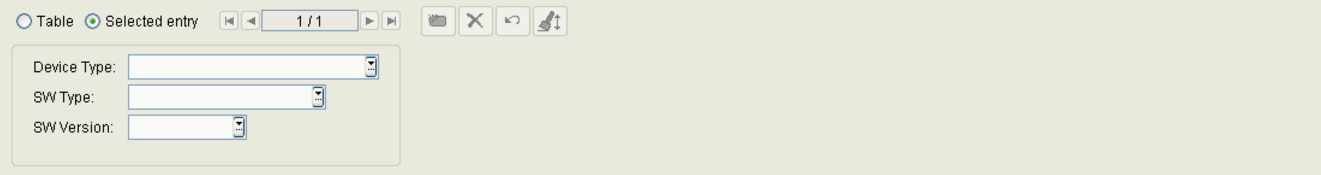
Multiple Add

Adds multiple templates to one Device Profile.

13.1.2 "Supported Devices of IP Device" Tab

Call: Main Menu > Profile Management > Device Profile > "Supported Devices of IP Device" Tab

You can define the IP Devices that should be supported by the profile here. You can add another device in the **New** and **Object** view with the ⧉ button and delete it with the ☒ button.



○ Table ● Selected entry 1 / 1

Device Type:

SW Type:

SW Version:

Device Type

IP Device type.
All IP Devices supported by DLS can be found in Section 3.4, "Area of Application".

Examples: **optiPoint 410 standard**, **optiClient 130**.

SW Type:

Type of software for the device.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**.

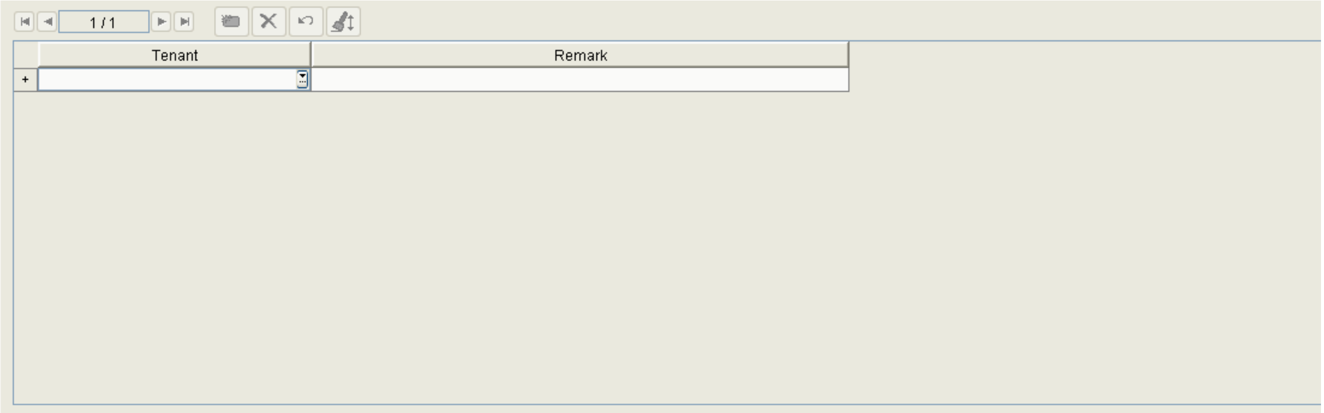
SW Version

Example for optiPoint and optiClient: **5.0.12**.

13.1.3 "Tenants" Tab

Call: Main Menu > Profile Management > Device Profile > "Tenants" Tab

> This tab is available only if the Multi-Tenancy function of the DLS is installed. See also Section 16.16.1, "Install/Deinstall Multi-Tenancy".



Tenant

Name of the tenant.

Remark

Information on the tenant.

13.2 User Data Profile

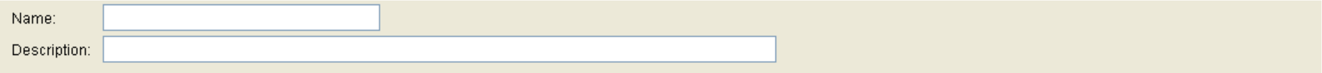
Call: Main Menu > Profile Management > User Data Profile

This area features the following components:

- General Data
- Possible Action Buttons
- "Templates" Tab
- "Tenants" Tab

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of profiles, and for entering a description. The base data associated with the profiles found is displayed in the Object view.



Name:

Description:

Name:

Profile name.

Description:

Brief description of the profile.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all User Data Profiles that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new User Data Profile.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Export Profile

Export selected User Data Profiles into a zip file.

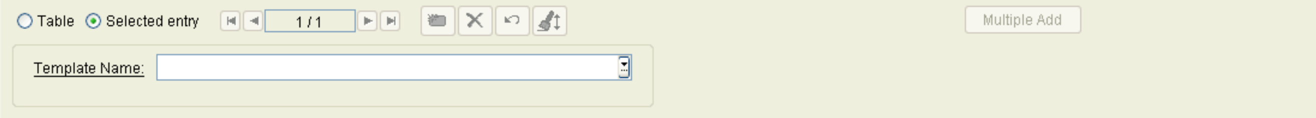
Import Profile

Import User Data Profiles from a zip file.

13.2.1 "Templates" Tab

Call: Main Menu > Profile Management > User Data Profile > "Templates" Tab

You can define one or more templates for the user data profile here. You can add another template in the **New** and **Object** view with the ▭ button and delete it with the ☒ button.



○ Table ● Selected entry

Template Name:

Template Name

Name of the template.

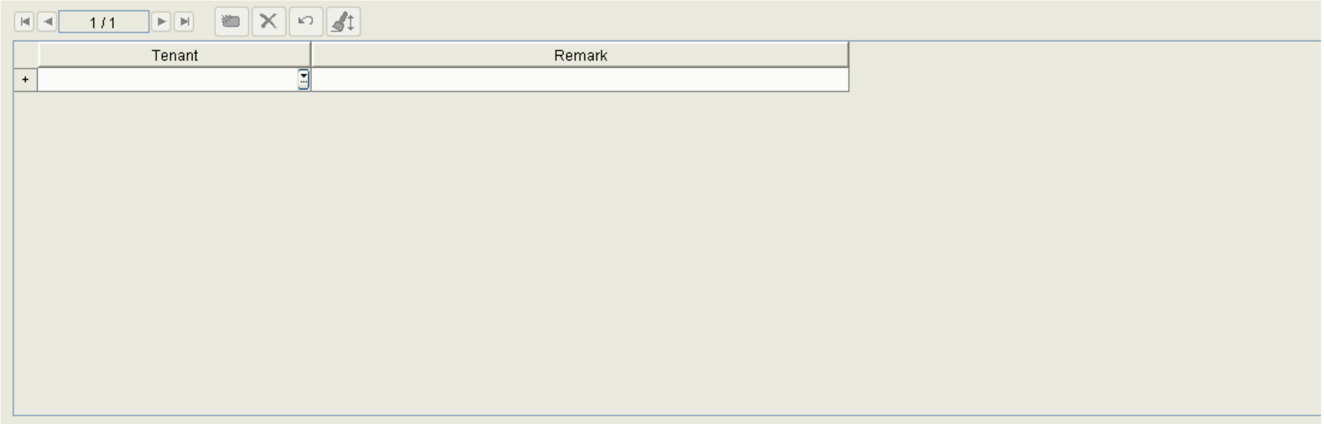
Multiple Add

Adds multiple templates to one User Data Profile.

13.2.2 "Tenants" Tab

Call: Main Menu > Profile Management > User Data Profile > "Tenants" Tab

> This tab is available only if the DLS multi tenancy function is installed. See chapter Section 16.16.1, "Install/Deinstall Multi-Tenancy".



Tenant

Name of the tenant.

Remark

Information on the tenant.

13.3 Template Overview

Call: Main Menu > Profile Management > Template Overview

Use this area to

- search for existing templates,
- change the name and the description of templates,
- delete templates, and
- export all templates in XML format into a .zip file or import them from a .zip file. Single templates can be imported from a .zip file as well.

Changes to template attributes and attribute values are not possible here. For more information, see Section 15.4, "Editing Templates".

> ⚠ If data changes are made in configuration forms that have been generated using templates, these changes are not automatically applied to the templates.
> These changes must be manually saved to the template (Section 15.4, "Editing Templates").

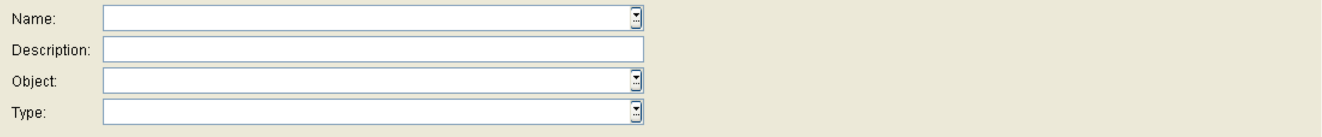
This area features the following components:

- General Data
- Possible Action Buttons
- "Template data" Tab
- "Tenants" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

This part of the content area is used for entering parameters in **Search** view to find a specific group of templates, and for importing and exporting template data. The base data associated with the templates found is displayed in the **Object** view (no changes possible).



Name:	
Description:	
Object:	
Type:	

You can use the following wildcards in all text and selection list fields in **Search** view:

- * (asterisk): Stands for any sequence of characters.
- ? (question mark): Stands for exactly one character.
- ^ (circumflex): Stands for an empty field.

All fields are combined internally using a logical AND. For example, if you specify a name and a description, only **those** templates that correspond to the specified name and that contain a corresponding description are selected.

Name:

Name of the template.

Description:

Description of the template.

Object:

Template object type.

Example: **IP Phone SNMP Settings**

Type:

Specifies the type of parameters stored in the template.

Possible entries:

- **IP client**
- **IP phone**
- **User Data**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all template that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Delete

Deletes one or more templates (multiple selections possible in table view).

Refresh

Refreshes the content of the relevant page.

Import Template

Import templates in XML format from a zip file. Single templates can be imported from a .zip file as well. They are selected by name in a popup window.

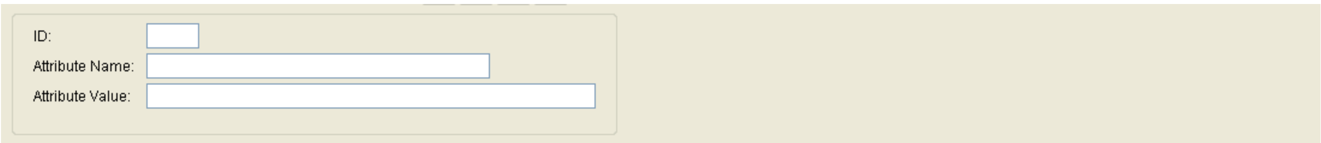
> Existing templates with the same name are overwritten during an import.

Export Template

Export the selected templates in XML format to a .zip file. Multiple template selection is possible in table view. A pop-up window prompts you to enter the file path.

13.3.1 "Template data" Tab

Call: Main Menu > Profile Management > Template Overview > "Template data" Tab



ID:

Attribute Name:

Attribute Value:

ID

ID for improved sorting (for example, for key assignments).

Attribute Name

Name of the attribute defined in the template.

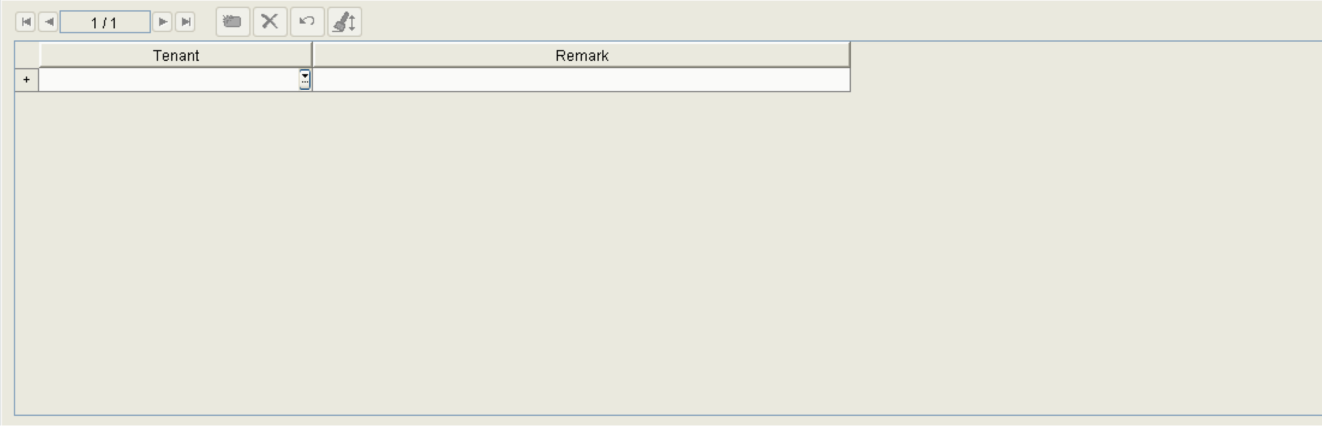
Attribute Value

Value of the relevant attribute name.

13.3.2 "Tenants" Tab

Call: Main Menu > Profile Management > Template Overview > "Tenants" Tab

> This tab is available only if the Multi-Tenancy function of the DLS is installed. See also Section 16.16.1, "Install/Deinstall Multi-Tenancy".



Tenant

Name of the tenant.

Remark

Information on the tenant.

14 Job Coordination

Call: Main Menu > Job Coordination

This menu consists of the following submenus:

- Job Control
- Daily Status
- Job Configuration

More complex deployment tasks are performed in the **Job Coordination** area. This area is used for configuring, performing, and logging deployment jobs (see also the operating sequence in Section 15.7).

14.1 Job Control

Call: Main Menu > Job Coordination > Job Control

This area features the following components:

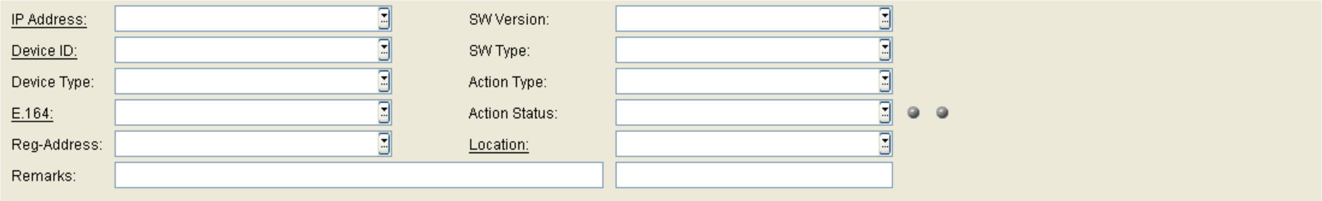
- General Data
- Possible Action Buttons
- "Basic Data" Tab
- "Deployment Data" Tab
- "Configuration Data" Tab
- "XML Application Data" Tab

This function lets you view a large volume of information on the individual jobs and discard, delete, or reactivate existing jobs. New jobs are not created here but rather by defining the activities to be performed in the job (for an example, see Section 15.7, "Using Job Coordination").

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of jobs. The base data associated with the jobs found is displayed in the Object view.



IP Address:		SW Version:	
Device ID:		SW Type:	
Device Type:		Action Type:	
E.164:		Action Status:	
Reg-Address:		Location:	
Remarks:			

> You can use the following wildcards in all text and selection list fields in **Search** view:
>
> - * (asterisk): Stands for any sequence of characters.
> - ? (question mark): Stands for exactly one character.
> - ^ (circumflex): Stands for an empty field.
>
> Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.
>
> All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only those IP Devices that correspond to the specified device type and that also belong to the specified IP address range are selected.

IP Address:

IP address of a IP Device or an address range.

In the case of jobs for IP ranges, **000.000.000.000** is displayed here in the **Search** view.

Format: **000.000.000.000**, 000 = value between 000 and 255.

Device ID:

Device ID of an IP Device or address range.

In the case of jobs for device ID areas, **00:00:00:00:00:00** is displayed here in the **Search** view.

Format: XX:XX:XX:XX:XX:XX, XX = Hex value between 00 and FF.

Device Type:

IP Device type.

In the case of jobs for different device types, nothing is displayed here in the **Search** view.

Format: Up to 30 characters.

All IP Devices supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **optiPoint 410 standard**, **optiClient 130**

E.164:

Complete phone number of an IP Device.

In the case of jobs for different phone numbers, nothing is displayed here in the **Search** view.

Format: Up to 15 characters.

See also Section 17.1, "E.164".

Reg-Address

IP address or host name of the registry server where the IP Device is registered.

SW Version:

Software version of an IP device.

In the case of jobs for different version numbers, nothing is displayed here in the **Search** view.

Example for optiPoint and optiClient: **5.0.12**.

SW Type:

Type of Software to be downloaded.

In the case of jobs for different software types, nothing is displayed here in the **Search** view.

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**.

Action Type:

Possible options:

- **IP Device Configuration**
- **IP Device Notification**
- **Mobile User Configuration**
- **Mobile User Migration**
- **Software Deployment**
- **Music on Hold File Deployment**
- **LDAP Template File Deployment**
- **INCA Firmware Deployment**
- **Java Midlet Deployment**
- **Logo File Deployment**
- **Application and Systemtone Deployment**
- **System and Ringtone Deployment**
- **APM Firmware Deployment**
- **Netboot Deployment**

- **IP Device Notification**
- **Screensaver Deployment**
- **File Deployment**
- **Scan IP Devices**
- **Read IP Device Data**
- **Read specific IP Device Data**
- **Reset IP Device**
- **Restore Factory Setting**
- **Gateway Configuration**
- **Read Gateway Data**
- **Gateway Probe**
- **Mobile User Logon**
- **Mobile User Logoff**
- **Push XML Application**
- **File Upload**

Action Status:

Possible action status:

- **expired**
  A timeout occurred when executing the deployment job because the time entered for **Job Configuration** was exceeded, for example, by an IP Device that was unavailable for an extended period of time. The job can be cancelled and deleted with the result that no more actions are performed for the job.
- **cancelled**
  The deployment job was cancelled. In the case of cancelled jobs, only the time of execution is modified (to re-start the job at a future time). The job can be deleted.
- **active**
  The deployment job was entered in the job table but has not started running because the execution time, for example, has not yet been reached. The job can be cancelled and deleted with the result that no more actions are performed for the job.
- **confirmed**
  The deployment job was accepted by the IP Device and waits until the status of the IP Device permits processing. The job can be cancelled and deleted with the result that the job execution is no longer interrupted.
- **failed**
  The deployment job was started but could not be executed. The job can be cancelled and deleted.
- **finished**
  The deployment job was executed correctly. The job can be cancelled and deleted.

- **running**
  The deployment job is currently being executed. The job can be cancelled and deleted with the result that the job execution is no longer interrupted.

Status Indicator for Jobs

The status indicator for a job can be reset over a pop-up menu by clicking **Reset Status** (see Section 5.4.1, "Main Menu").

Left hand indicator ball:
🟢 Job is not running.
🟡 Job is running.

Right hand indicator ball:
🟢 Job has been executed without errors.
🔴 Job has been cancelled with errors.

Location:

Current location of the IP Device.

Remarks:

Fields for general information.

Possible Action Buttons

Search

Searches for all deployment jobs that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves changes to the existing deployment job. The Save option is only available after a change to an interrupted job.

Discard

Discards changes to the existing deployment job. The Discard option is only available after a change to an interrupted job.

Delete

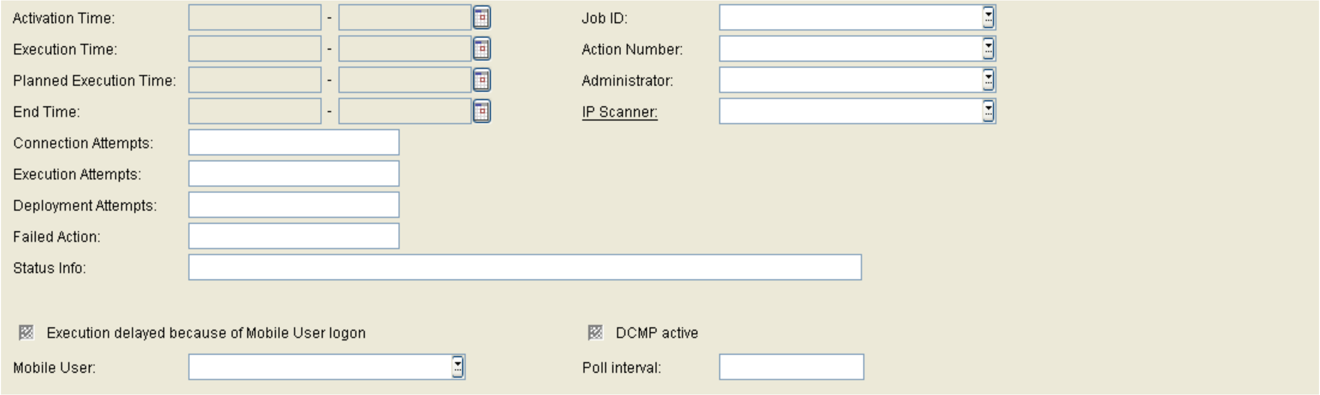
Deletes the deployment job displayed in the **Object** view.

Cancel Job

Interrupts the deployment job displayed in the **Object** view.

14.1.1 "Basic Data" Tab

Call: Main Menu > Job Coordination > Job Control > "Basic Data" Tab



Activation Time:

Time for the activation of the deployment job (see Section 5.4.2.4, "Time field with calendar button").

Execution Time:

Time for the execution of the deployment job (see Section 5.4.2.4, "Time field with calendar button").

> Interrupted deployment jobs can be reactivated by entering a future point in time. For all other job statuses, the time displayed here indicates the time of execution, irrespective of whether it is in the past or the future.

Planned Execution Time:

Time when the deployment job will be started.

> For devices running in different timezones, device local time +/- timeshift related to the timezone is displayed.

End Time:

Time for ending the deployment job (see Section 5.4.2.4, "Time field with calendar button").

> For deployment jobs that were already executed, the time at which these job were ended is displayed here.

Connection Attempts:

Number of retries needed to perform the job (**0** means not yet executed).

Execution Attempts:

Number of execution retries needed to perform the job (**0** means not yet executed).

Deploy Attempts:

Number of deployment retries needed to perform the job (**0** means not yet executed, only for deployment jobs).

Failed Action:

In the job table, this is the number of the action that could not be successfully completed and caused DLS to automatically generate and execute a **Read IP Device Data**.

The field only contains one value for jobs of the type **Read IP Device Data** generated by the DLS. The administrator is shown as **@DLS** for these jobs.

Status Info:

Messages can indicate the successful completion of a deployment job as well as to a fault. The following status messages are output (sorted in alphabetical order based on the **Status Info**):

Status Info	Description	Trigger
action type not implemented[1]	-	neutral
equal item names	Identical entry names.	IP phone
failed	Failed.	IP phone
file-not-found	Error, for example, when opening stored templates or when opening the deployment file.	IP client
ignored - dial plan error	Error in the numbering plan.	IP phone
image path not contactable	Removed image path is not available.	IP client
initiated	The job was initiated but not yet finished.	neutral
internal ERROR[1]	-	neutral
invalid data	Invalid data.	IP phone
invalid format	Invalid format.	IP phone
invalid function key	Invalid function key.	IP phone
invalid Index	Invalid Index.	IP phone
invalid item name	Invalid item name.	IP phone

Status Info	Description	Trigger
local deployment path not specified	Item "dls-deployment-local-path" is not set.	IP client
local deployment path not writable	Local deployment path not writable.	IP client
missing item content	Missing item content.	IP phone
missing item name	Missing item name.	IP phone
nonce not valid[1]	-	neutral
not a Feature Toggle key	Not a Feature Toggle key.	IP phone
not a line key	Not a line key.	IP phone
not a repertory dialing key	Not a Repertory Dialing key.	IP phone
not a selected dialing key	Not a selected dialing key.	IP phone
not implemented	Not implemented.	IP phone
not readable	Not readable.	IP phone
not supported	Not supported.	IP phone
OK	Deployment was successful.	neutral
read only	Read-only.	IP phone
server-not-contactable	The remote server is not available.	IP client
Self Labeling Key Sidecar not available	The optiPoint Self Labeling Key Module is not available.	IP phone
unknown item	Unknown item.	IP phone
not a DSS key	Not a DSS key.	IP phone

[1] For internal debugging only; Not relevant for the DLS user.

Job ID:

ID of the jobs. The Job ID is the name that was entered when the job was created (see Section 5.4.2.1, "Toolbar"). If a name was not entered, the action number is used for the job ID.

The job ID for jobs that distribute and activate a PSS (Pre-Shared Secret) are prefixed with PSS.

Action Number:

Action number of the job. This sequential number is automatically generated for every action in every deployment job (one for each IP address edited).

Administrator:

User names for this job. The name corresponds to the user who defined the action. Enter **@DLS** as the name for automatically generated actions.

IP Scanner:

IP scanner for this job. The name is set when the IP scanner is configured, see Section 7.4.4, "Scan IP Devices".

Execution delayed because of Mobile User logon

The job is delayed because of Mobile User logon.

Mobile User:

Mobile User currently logged on.

DCMP active

If this check box is activated, the device periodically checks for DLS jobs on the DCMP (DLS Contact-Me Proxy).

Poll Interval

Interval (in minutes) between two polls from the device to the DCMP.

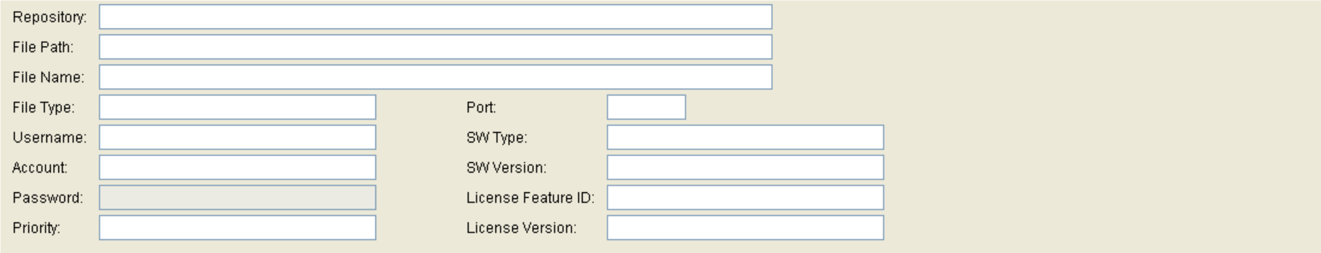
14.1.2 "Deployment Data" Tab

Call: Main Menu > Job Coordination > Job Control > "Deployment Data" Tab

The software deployment data is displayed here for jobs with the following action types.

- **INCA Firmware Deployment**
- **Java Midlet Deployment**
- **LDAP Template File Deployment**
- **Logo File Deployment**
- **System and Ringtone Deployment**
- **Software Deployment**
- **Music on Hold File Deployment**

Data for a job may be available in either the "Deployment Data" Tab or the "Configuration Data" Tab.



Repository:

IP address or host name of the FTP server (for IP phones) or network computer (for IP clients) from which the software is downloaded.

File Path:

Directory on the FTP server (for IP phones) or on the network computer (for IP clients) from which the software is downloaded. In the case of IP phone software, the path begins with the configured "virtual" root directory. For IP client software, it begins with the shared network path.

File Name:

The file name of the software downloaded.

File Type:

Deployment type of the file downloaded.

Examples:
INCA (INCA firmware deployment)
MIDLET (Java midlet deployment)
LDAP (LDAP template file deployment)

LOGO (Logo file deployment)
RINGTONE (System and ringtone deployment)
APP (Software deployment)
MOH (Hold music file deployment)

Username:

Username ("login") of the FTP access to the server from which the software is downloaded.

Account

Not currently used in DLS.

Password:

Password of the FTP access to the server from which the software is downloaded.

Priority:

Signals whether deployment should pause when a IP Device is busy and wait until it frees up (**normal**) or if deployment should be performed at the set time irrespective of the IP Device status (**high**).

Port:

Port used for the FTP server from which the software is downloaded. Permanently set to port 21.

SW Type:

Software type of the software that is downloaded (for software deployment).

Examples: **Siemens HFA**, **Siemens SIP**, **T-Com HFA**.

SW Version:

Software version of the IP Device.

Example for optiPoint: **5.0.12**.

License Feature ID:

If the downloaded software requires a license, then this field contains the product ID (HLM terminology) used for registering the software in HiPath License Management (for software deployment).

Example for optiPoint 410 standard HFA: **OPTI410STDHFA**.

License Version:

If the downloaded software requires a license, then this field contains the product version (HLM terminology) used for registering the software in HiPath License Management (for software deployment).

Example for optiPoint only: **6.0.0**

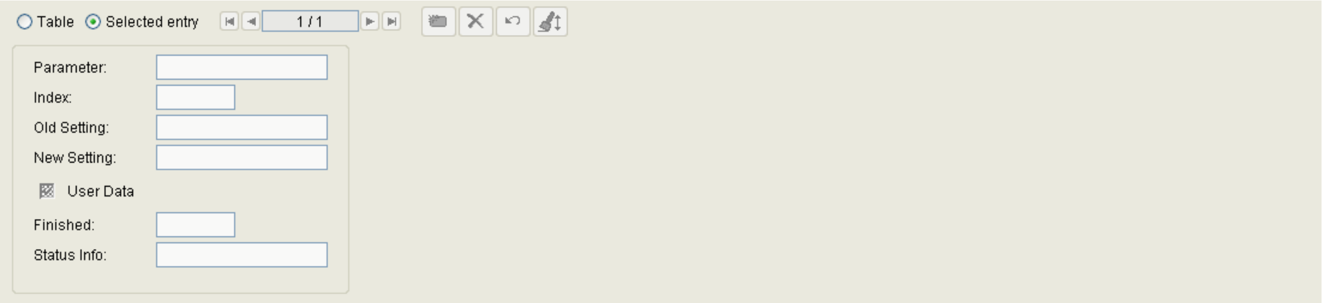
14.1.3 "Configuration Data" Tab

Call: Main Menu > Job Coordination > Job Control > "Configuration Data" Tab

Configuration data for jobs with the **IP Device Configuration** action type is displayed here.

All configuration data for this job is displayed in tabular form.

Data for a job may be available in either the "Deployment Data" Tab or the "Configuration Data" Tab.



○ Table ● Selected entry 1 / 1

Parameter:

Index:

Old Setting:

New Setting:

▨ User Data

Finished:

Status Info:

Parameter

Name of the parameter used to perform modifications in this job.

Index

Index within the parameter you want to change (if available).
If a IP Device parameter can accept more values (value list), an index is created for each value. The field remains empty if there is only one value.

Old Setting

Value of the parameter before the change. Only wildcards are displayed here if the parameter is a password.

New Setting

Value of the parameter after the change. Only wildcards are displayed here if the parameter is a password.

User Data

If this check box is active, user-specific data was sent to the IP device instead of device-specific data (display only).

Finished

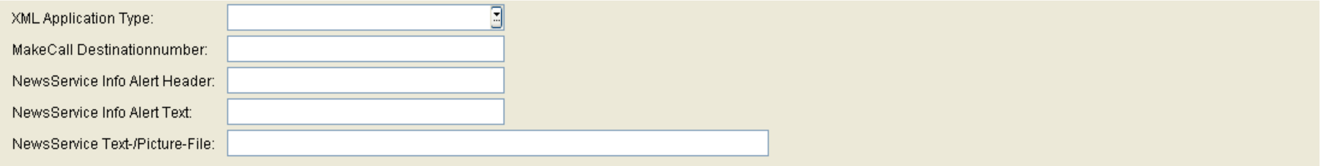
Indicates if the parameter has already been changed.

Status Info

Information on the job status.

14.1.4 "XML Application Data" Tab

Call: Main Menu > Job Coordination > Job Control > "XML Application Data" Tab



XML Application Type:	
MakeCall Destinationnumber:	
NewsService Info Alert Header:	
NewsService Info Alert Text:	
NewsService Text-/Picture-File:	

XML Application Type:

Type of XML application that has been started with this job.

Possible Options:

- **MakeCall**
- **NewsService File Display**
- **NewsService Info Alert**

MakeCall Destinationnumber:

Dialing number of the end device to which an automatic call has been initiated by the XML application 'MakeCall'.

NewsService Info Alert Header:

Header of the latest info alert message that has been sent to the end device by means of the XML application ’NewsService’.

NewsService Info Alert Text:

Text of the latest info alert message that has been sent to the end device by means of the XML application ’NewsService’

NewsService Text-/Picture File:

File name of the latest text (.txt) or picture file (.jpg, .bmp, .gif, .png) that has been sent to the end device by means of the XML application ’NewService’:

14.2 Daily Status

Call: Main Menu > Job Coordination > Daily Status

This area features the following components:

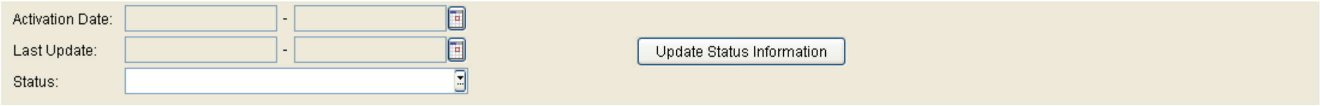
- General Data
- Possible Action Buttons
- "Status Information" Tab

This function gives you a clear display of all jobs in a table. Additionaly, you may search for Job Status or Job ID. In addition to the job found according to the requested Job Status, all jobs belonging to the same day will be displayed. In object view, you can switch between entire table view or individual table entries. The table can be sorted by Job ID, Job Status, Activation Time, or End Time.

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of jobs. The data associated with the jobs found is displayed in the Object view.



Activation Date:

Time for the activation of the deployment job (see Section 5.4.2.4, "Time field with calendar button").

Last Update

Date of the last status information update.

Status:

Possible action status:

- **active**
  The deployment job was entered in the job table but has not started running because the execution time, for example, has not yet been reached.
- **failed**
  The deployment job was started but could not be executed.
- **finished**
  The deployment job was executed correctly.
- **running**
  The deployment job is currently being executed.

Update Status Information

Set status information to the current state, including all jobs that have been created on the current day.

Possible Action Buttons

Search

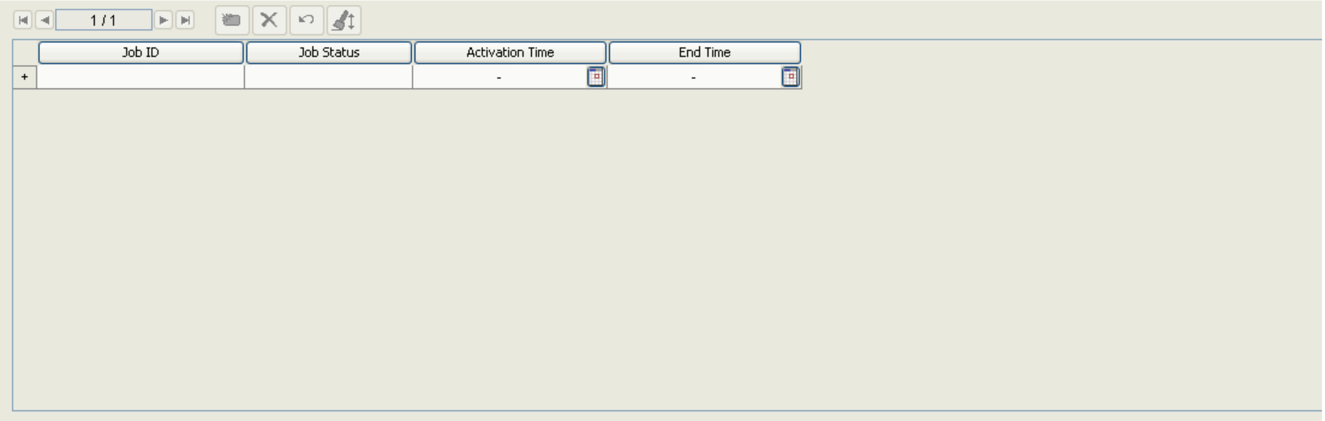
Searches for all statistical data that corresponds to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

14.2.1 "Status Information" Tab

Call: Main Menu > Job Coordination > Daily Status > "Status Information" Tab



	Job ID	Job Status	Activation Time	End Time
+			-	-

Job ID

Job ID (or the action number) of the deployment job.

Job Status

Status of the deployment job.

Activation Time

Time of activation for the deployment job.

End Time

For jobs with the status **finished**: time of end of execution.

14.3 Job Configuration

Call: Main Menu > Job Coordination > Job Configuration

This area features the following components:

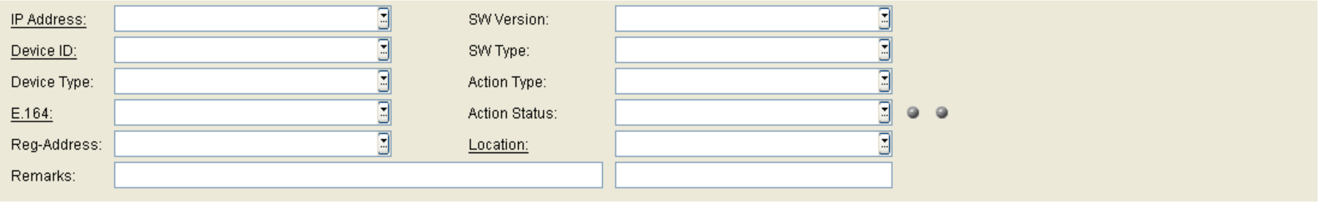
- General Data
- Possible Action Buttons
- "IP Phones" Tab
- "IP Clients" Tab
- "IP Gateways" Tab
- "Gateways" Tab

This function can be used to influence the behavior of a job. Some configuration data can be entered differently for IP phones and IP clients.

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

This part of the contents area is used for entering parameters which are valid for all tabs.



Limit of concurrent Jobs:

Maximum number of deployment jobs that can be performed simultaneously. If the number of jobs to be started according to the execution time is greater than number of jobs entered, retries would automatically be started for all jobs involved.

Default: 100.

Delete Finished Jobs after Days:

Number of days after which ended jobs should be deleted. Jobs with other statuses are not affected by this.

Default: 10.

Delete Cancelled Jobs after Days:

Number of days after which interrupted jobs should be deleted. Jobs with other statuses are not affected by this.

Default: 10.

Delete Expired Jobs after Days:

Number of days after which expired jobs should be deleted. Jobs with other statuses are not affected by this.

Default: 10.

Delete Failed Jobs after Days:

Number of days after which interrupted jobs should be deleted. Jobs with other statuses are not affected by this.

Default: 99999 (failed jobs are not deleted).

Default Job Execution Option:

Default value for the time of job execution.

Possible options:

- **Immediately**
  The job is started immediately.
- **Immediately or after registration**
  The job is started immediately. If it should fail, another attempt will be made on registration of the device.
- **After registration**
  The job is started on registration of the device.

Save Finished Jobs

Check box for activating the option that allows jobs to be left in the job table and displayed in the job statistics.

Default: **activated**

Possible Action Buttons

Save

Saves the changes you made under **Job Configuration**.

Discard

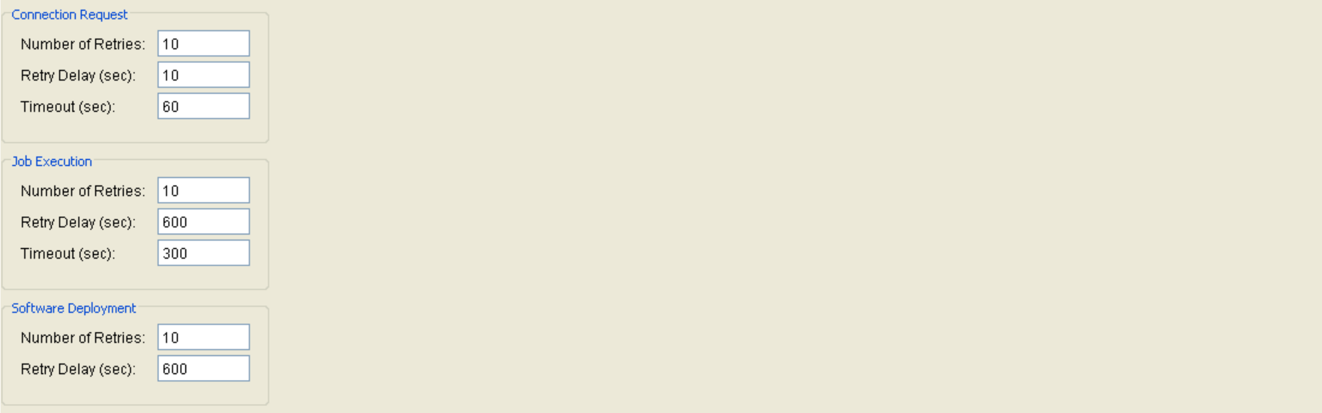
Discards the changes you made under **Job Configuration**.

Refresh

Refreshes the content of the relevant page.

14.3.1 "IP Phones" Tab

Call: Main Menu > Job Coordination > Job Configuration > "IP Phones" Tab



Connection Request

Number of Retries: 10

Retry Delay (sec): 10

Timeout (sec): 60

Job Execution

Number of Retries: 10

Retry Delay (sec): 600

Timeout (sec): 300

Software Deployment

Number of Retries: 10

Retry Delay (sec): 600

Connection Request

Number of Retries:

Number of retries permitted before the execution of a job for IP phones should be cancelled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP phones.

Default: **10** Value range: **1** - **3600**

Timeout (sec):

Time in seconds that the DLS waits for an IP phone answer for each attempt if a job is performed.

Value range: **1** - **3600**

Default: **60**

Job Execution

Number of Retries:

Number of retries permitted before the execution of a job for IP phones should be cancelled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP phones.

Value range: **1** - **3600**

Default: **600**

Timeout (sec):

Time limit for complete job execution, including all retries.

Value range: **30** - **3600**

Default: **300**

Software Deployment

Number of Retries:

Number of retries permitted before the software deployment for IP phones should be cancelled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two software deployment retries for IP phones.

Value range: **1** - **3600**

Default: **600**

Timeout (sec):

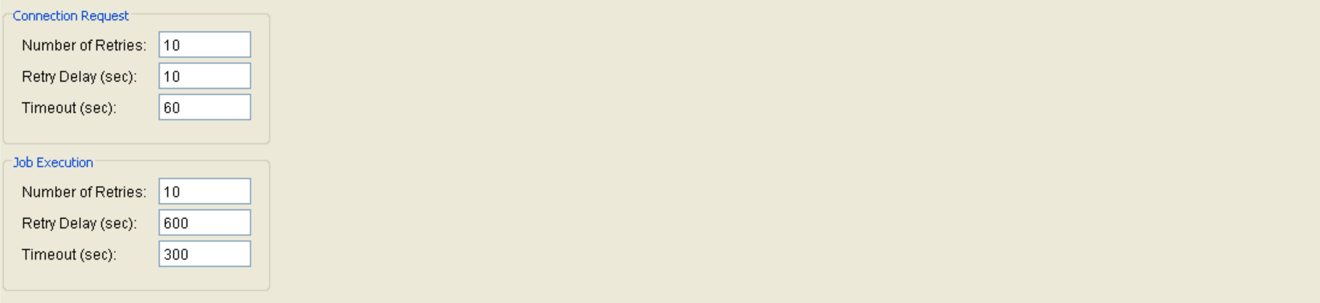
Time limit for complete Software Deployment, including all retries.

Value range: **30** - **3600**

Default: **300**

14.3.2 "IP Clients" Tab

Call: Main Menu > Job Coordination > Job Configuration > "IP Clients" Tab



Connection Request

Number of Retries: 10

Retry Delay (sec): 10

Timeout (sec): 60

Job Execution

Number of Retries: 10

Retry Delay (sec): 600

Timeout (sec): 300

Connection Request

Number of Retries:

Number of retries permitted before the execution of a job for IP phones should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP phones.

Value range: **1** - **3600**

Default: **10**

Timeout (sec):

Time in seconds that the DLS waits for an IP phone answer for each attempt if a job is performed.

Value range: **1** - **3600**

Default: **60**

Job Execution

Number of Retries:

Number of retries permitted before the execution of a job for IP phones should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP phones.

Value range: **1** - **3600**

Default: **600**

Timeout (sec):

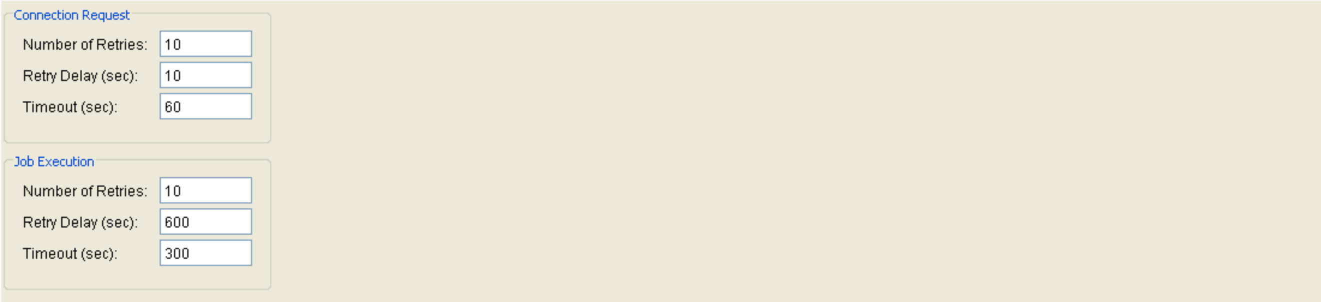
Time limit for complete job execution, including all retries.

Value range: **30** - **3600**

Default: **300**

14.3.3 "IP Gateways" Tab

Call: Main Menu > Job Coordination > Job Configuration > "IP Gateways" Tab



Connection Request

Number of Retries: 10

Retry Delay (sec): 10

Timeout (sec): 60

Job Execution

Number of Retries: 10

Retry Delay (sec): 600

Timeout (sec): 300

Connection Request

Number of Retries:

Number of retries permitted before the execution of a job for IP gateways should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP gateways.

Value range: **1** - **3600**

Default: **10**

Timeout (sec):

Time in seconds that the DLS waits for an IP gateway answer for each attempt if a job is performed.

Value range: **1** - **3600**

Default: **60**

Job Execution

Number of Retries:

Number of retries permitted before the execution of a job for IP gateways should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP gateways.

Value range: **1** - **3600**

Default: **600**

Timeout (sec):

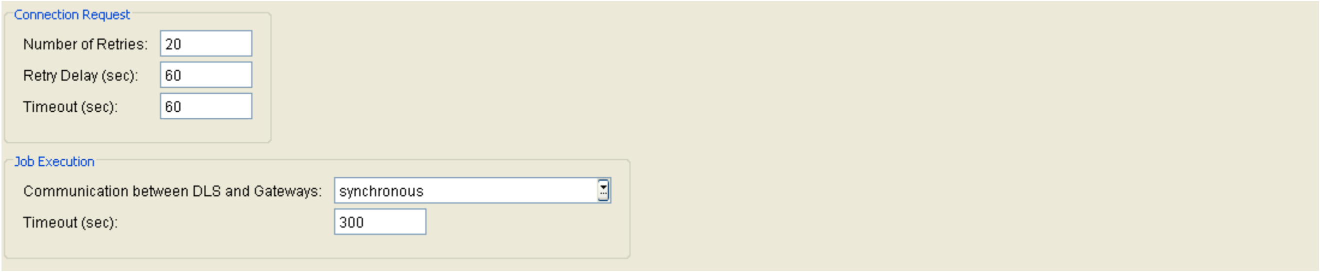
Time limit for complete job execution, including all retries.

Value range: **30** - **3600**

Default: **300**

14.3.4 "Gateways" Tab

Call: Main Menu > Job Coordination > Job Configuration > "Gateways" Tab



Connection Request

Number of Retries: 20

Retry Delay (sec): 60

Timeout (sec): 60

Job Execution

Communication between DLS and Gateways: synchronous

Timeout (sec): 300

Connection Request

Number of Retries:

Number of retries permitted before the execution of a job for gateways should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **200**

Default: **20**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for gateways.

Value range: **10** - **3600**

Default: **60**

Time that DLS waits for answer for each attempt if a job is performed:

Time in seconds that the DLS waits for a gateway answer for each attempt if a job is performed.

Value range: **1** - **3600**

Default: **60**

Job Execution

Communication between DLS and Gateways:

Possible options:

- **synchronous**
  The jobs are executed synchronously. The display on the DLS stops responding (the hourglass appears) until these actions are fully complete. Clicking **Refresh** always results in the current data record.

- **asynchronous**
  The jobs are executed in the background allowing you to continue working in parallel. To see the result, you must wait a little and then click **Refresh**. If you refresh too soon, the old data record is returned as a result.

Timeout (sec):

Time limit for complete job execution, including all retries.

Value range: **1** - **3600**

Default: **300**

15 Operating Sequences

This chapter contains the following practical sequences:

- First Steps: Changing IP Device Parameters

> This section provides fundamental operating information - also helpful for performing other functions.

- Changing the Element Manager Configuration and Creating Jobs
- Registering Workpoint Software and Files
- Editing Templates
- Workpoint Autoconfiguration (Plug&Play)
- Distribution of Workpoint Software
- Using Job Coordination
- Backup/Restore
- Importing and Exporting Plug&Play Data
- Copy Macro for P&P and Templates

For information on general interface operation, see Section 5.4.2, "Work Area".

> The sequence descriptions provided here are intended as examples. The actual sequence may vary from the description, depending on the particular DLS configuration, the servers or IP Devices used, and the ongoing development of the DLS.

15.1 First Steps: Changing IP Device Parameters

In many areas of the DLS (for example, **IP Devices**), you can use the database running in the DLS to select all or a subset of the total number of IP Devices available for subsequent administration.
This takes place in the working area using **Search** view (see Section 5.4.2.3).

Requirements for this example: the DLS, the servers and IP Devices are operational.

1. In the main menu, select an area where you would like to change something under **IP Devices**.
2. Select **Search** view (see Section 5.4.2.3) if it is not yet shown.
3. Indicate the IP Devices you want to select.
   Do this by choosing an entry in the selection list field, for example, beside **Device Type** (see Section 5.4.2.4) or enter an IP address range.

   > You can use the following wildcards in all text and selection list fields in **Search** view:
   >
   > - * (asterisk): Stands for any sequence of characters.
   > - ? (question mark): Stands for exactly one character.
   > - ^ (circumflex): Stands for an empty field.
   >
   > Partial inputs, such as, **192.168.***, are consequently possible for an IP address range from **192.168.0.0** to **192.168.255.255**.
   >
   > All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only those IP Devices that correspond to the specified device type and that also belong to the specified IP address range are selected.

   If you want to search through all available IP Devices, do not enter any information in the fields in Search view.
4. Click **Search** (see Section 5.4.2).
5. If no matching data was found, a message appears in the message window (see Section 5.4.2.6).
   If the search was successful, the display changes to **Object** view, which always shows the data for a single IP Device. You can use the navigation buttons (see Section 5.4.2.5) to scroll through all IP Device data that corresponds to the search filter.

6. Click **Table** in the view bar to change to List view. Click a column header to sort the entire table according to the value specified in the header (alternating between ascending and descending).

   Click between two column headers and drag the mouse right or left to change the width of the left-hand column.

   Click a column header and drag the mouse right or left to change the order of the columns.

7. Now you can change any fields that have not been dimmed. This is possible in both **Object** view and **Table** view.

8. To transmit the changes to a single IP Device, click **Save**. This sends the data directly to the IP Device.

   > If you would like to transmit the changes to multiple IP Devices simultaneously, change to **Table** view before you save the changes and mark additional IP Device entries in the list (see Section 5.4.2.4, "Multiple selection and data transfer in Table view" for information on how to do this).

   Click **Save**. This sends the data directly to the selected IP Devices.

15.2 Changing the Element Manager Configuration and Creating Jobs

Changes made in the Element Manager configuration under **Element Manager** > **Element Manager Configuration** (for example, E.164 prefix, gatekeeper ID, SIP server address, etc.) are forwarded to the relevant workpoints. The ID of this Element Manager is entered in the **Element Manager ID** field on these workpoints under **IP Devices** > **IP Device Management** > **IP Device Configuration** > **"EM Synchronization" Tab**. However, if a different Element Manager (or Element Manager ID) is entered under Referenced Element Manager, this one is valid.[1] A modification (of the E.164 prefix, for example) can take several minutes, depending on the number of workpoints.

Jobs are created for registered workpoints in the Element Manager configuration during modification. A dialog appears before the modifications are implemented, displaying the number of jobs and requesting confirmation of the action. You can save the configuration changes here without immediately creating jobs. The jobs are then automatically created (no confirmation required) during the next automatic or manual synchronization.

A synchronization that has been started but is not yet finished prevents the initiation of other synchronization operations for this Element Manager or Element Manager ID. A corresponding message appears in the window. The same message appears if you try to modify the Element Manager configuration while an (automatic) synchronization is running.

[1] This parameter is used when preparing to relocate a station to another system. Two data records exist during this operation with the same E.164 number and different device IDs. One of the data records is assigned to system A, the other to system B. The parameter defined here ensures that during synchronization between both systems, only the data record belonging to a particular system is updated.

15.3 Registering Workpoint Software and Files

This section explains how you can register software and files in the DLS so that the DLS can use them for the deployment.

The functions can be found under **Main Menu** > **Administration** > **Server Configuration** > **FTP Server Configuration**, ..> **HTTPS Server Configuration**, ... > **Network Drive Configuration**.

> The file that is to be registered is examined during registration.
>
> The following checks are made:
>
> - Whether the file exists at the source storage location.
> - If so and if this file contains software, whether the SPA is unknown, old, or new.
> - Any additional data available in the new format, such as, the **SW type** (HFA or SIP), **SW version**, etc. is read out.
>
> This process can take some time, depending on the network.

For an overview of all object types supported by the DLS, see Section 3.5, "Overview of Software and File Types".

For an overview of all IP Devices and platforms supported by the DLS, see Section 3.4, "Area of Application".

> You must also register IP client software installations in the DLS, but no license check is performed for IP client software in the DLS because this is done while it is running (at software startup).

Requirements

- A configured FTP server for IP phone software images or a configured Windows network drive for IP client software (see Section 6.2.4 or Section 6.2.6).
- The suitable files are available in the source storage location.

15.3.1 Automatic Registration

The only difference between the automatic registration of IP phone software and IP client installations involves the type of source storage location.

1. To register software and data on an FTP server, select an FTP server from the choice list under **Administration** > **Server Configuration** > **FTP Server Configuration** by means of the **Search** button. Then, click on **Start scan** to start the registration.

   To register an installation for IP Clients, use **Administration** > **Server Configuration** > **Network Drive Configuration** > **Scan Server**.

   To register softare and data on an HTTPS server, use **Administration** > **Server Configuration** > **Network Drive Configuration** > **Scan Server**.

   To configure FTP servers and network drives, see Section 6.2.4 or Section 6.2.6.

2. Click **Start**. Automatic registration starts and updates the status, and information is entered in the dialog window.

> You can go ahead and close the dialog window during this process. Automatic registration runs in the background without being affected.

15.3.2 Understanding License Information for IP Phone Software

Licensed IP phone software is not yet available. This means that as far as licensing is concerned, only data entered here for unlicensed software applies to IP phones.

When you register IP phone software, information is also read out of the software image's "license trailer".

The license trailer information consists of the following possible values:

- Device type (contains the device type designation)
- Software version (contains the software version number)
- Software type (contains the software type designation)
- License feature ID (contains the identification of the license feature)
- Licensed SW version (contains the software license version number)
- Expiry Date (contains the software expiration date)

15.4 Editing Templates

The DLS can create templates for all parameters in the **IP Devices** area. This provides a quick and easy option for reusing configurations that are frequently deployed.

You can also combine existing templates in profiles, which greatly simplifies the use of extensive workpoint configurations.

You can create a template for each interface in the contents area (see Section 5.4.2, "Work Area") and save it to use later. You can use buttons in addition to export and import all stored templates into an ZIP file (see Section 13.3, "Template Overview").

> ⚠ If data changes are made in configuration forms that have been generated using templates, these changes are not automatically applied to the templates.
> In order to be applied, the changes must be saved manually in the template; see below.

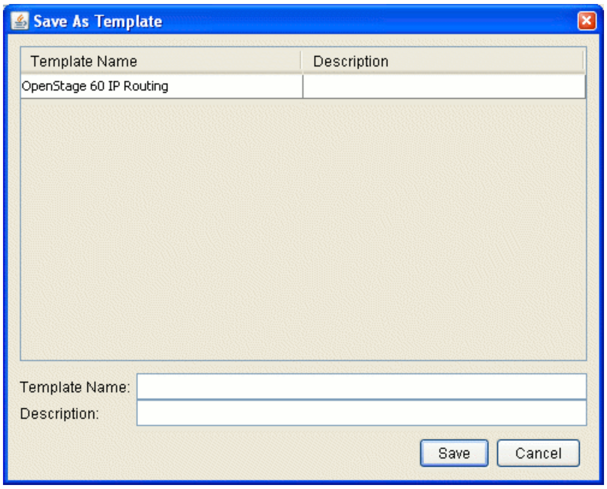
15.4.1 Creating a Template Manually

1. Select an area for which you want to create the template in the main menu under **IP Devices** > **IP Phone Configuration** or **IP Client Configuration**.
2. Select **Template** view (see Section 5.4.2.3, "View Bar").
3. Enter all the required data.
   A template always includes the contents of an interface under **IP Devices**, with all available tabs.

   > ℹ In many cases, it is useful to select the scope of a template so that it is not too large. For example, it may be advisable to create two separate templates instead of one for WAP and LDAP so that you can assign them more flexibly, that is, separately from one another, to different profiles.

4. Click **Save**.

5. The dialog window for saving the template appears.



Template Name	Description
OpenStage 60 IP Routing	

Template Name:
Description:

Enter a meaningful name under **Template Name**, such as, "QoS Configuration 1". Under **Description**, enter a text that explains this template.

6. Click **Save**.
   The name of the current template now appears after **Template** in the view bar.

You can also save multiple different templates for an area by using different template names.

You can export templates that you have saved (see Section 13.3, "Template Overview").

15.4.2 Creating a Template From an Existing Configuration

You can take configuration data that already exists in **Object** view and include it in a template.

1. In the main menu under **IP Devices**, select an area in **Object** view from which you want to copy the data into a template.
2. In the menu bar, select **Copy to template** under **Action**. **Template** view appears with the data that you copied.

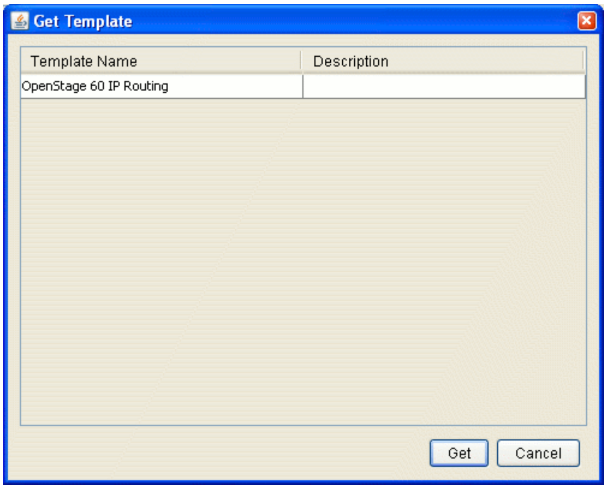
Save the template for later use as described above (see "Creating a Template From an Existing Configuration", starting with step 4).

15.4.3 Loading the Template

To change a template that has already been saved or to use such a template manually, you first have to load it into **Template** view.

1. Select the **Template** view for which you want to load a template that has already been saved in the area and click **Get**.

2. If there is at least one template for this area, the dialog for loading a template appears.



Get Template

Template Name	Description
OpenStage 60 IP Routing	

3. Select a template from the list and click **Get**.

4. The template contents are displayed in **Template** view and the template name appears in the view bar.
   To use the data for configuration or as a search criterion, select the appropriate view (**Object** or **Search**) and select the **Use template** entry under **Action** in the menu bar.

> When you use a template, only the contents defined in the template are applied. Empty fields or check boxes do not overwrite or delete any current values in the configuration.
>
> Use **Profile Management** > **Template Overview** to check which individual attributes are currently configured.

15.4.4 Additional Functions

By clicking **Rename Template** in **Template** view, you can rename a template that has already been saved and change the description of the template. With **Delete Template**, you can delete one or more saved templates.

15.5 Workpoint Autoconfiguration (Plug&Play)

The goal of Plug&Play in DLS is to automatically provide the workpoints supported with the parameters needed for registering at a gatekeeper or SIP server. This should always be done as soon as a workpoint is switched on or connected.

There are different types of Plug&Play:

- **Full plug&play**
  - Provision of the workpoint with IP base data and DLS address data using the DHCP server.
- **Limited plug&play**
  - Manual entry of IP base data and DLS address data at the workpoint.

> We recommend that you use a DHCP server in the DLS environment to
> - support full plug&play and
> - ensure the authenticity of the DLS server.
>
> For more information on how to configure a DHCP server, see Section 4.10.4, "DHCP Server in a Windows Environment" or Section 4.10.5, "DHCP Server in a Linux/Unix Environment".

15.5.1 Requirements

Requirements for full Plug&Play

- Functional DHCP infrastructure. Depending on the network topology, this consists of at least one DHCP server and, where applicable, multiple DHCP relay agents.
- The IP base data and the DLS address data is entered on the DHCP server so that it can be distributed automatically to the terminals. For information on configuring the DHCP server, see Section 4.10.4.3 (Windows) or Section 4.10.5 (Linux/Unix).

This ensures that an IP phone with factory settings receives its initial IP configuration when it is booted.

Requirements for limited plug&play

- Manual storage of the complete IP base data (IP address, subnet mask, default IP gatekeeper, DNS server, DNS domain suffix, etc.) and DLS address data on the IP phone.

This guarantees plug&play operation, albeit in a restricted form, in networks without DHCP infrastructure.

For IP clients, full plug&play looks a little bit different.
As IP clients usually run on a host with proper IP configuration, the IP client can be provided with missing DLS address data either using a "DHCP Inform" or with a "DNS Text Resource Request".

Both ways are considered full plug&play because in contrast to the exclusive use of a DNS with IP phones, manual configuration is not necessary.

15.5.2 Setting Up Plug&Play Registration

15.5.2.1 Assignment Procedure

There are two different procedures for plug&play registration. These differ in terms of the manner in which a workpoint’s plug&play data is assigned to a physical workpoint.

- **Assignment using Device ID**
  A specific device ID is entered here for an existing data record, that is, a virtual device (see Section 15.5.2.2, "Creating Plug&Play Data"). The DLS uses the device ID to identify which plug&play data it should send to the workpoint.
- **Assignment using E.164**
  Alternatively, the data record can be assigned an E.164 number which must be entered manually at the workpoint. The DLS then checks all familiar plug&play data sources based on phone numbers one after the other (for example, configured HiPath 4000 Assistant databases or HiPath 3000/5000) to see whether the phone number can be uniquely assigned to a system.
  If the workpoint responds during DLS installation, the DLS can use the E.164 number to identify which plug&play data it should send to the workpoint.

15.5.2.2 Creating Plug&Play Data

The are a number of different procedures for creating plug&play data:

- **Creation by synchronization with an Element Manager**
  Synchronizing DLS with an Element Manager creates a new data record for each station that is stored in the Element Manager but not yet in the DLS. For more information about connecting the Element Manager and the DLS, see **Element Manager** > **Element Manager Configuration**.
- **Plug&play data import**
  You can import plug&play data from a file via **IP Devices** > **IP Device Management** > **IP Device Configuration**.
- **Manual configuration of a station in the DLS**
  You can use the **IP Devices** > **IP Device Management** > **IP Device Configuration** area to create a new station data record in the DLS as a virtual device.
- **Configuration via a provisioning tool using the DLS API**

15.5.3 Registration

1. Connect the workpoint(s) (see the workpoint installation or administration manuals). If all requirements for full plug&play are met, the workpoint will receive the DLS address data from DHCP.

   The workpoint registers at the DLS with this data.

2. If the DLS can identify the unique plug&play data required by the workpoint performing registration, it automatically sends it to the workpoint.

   The DLS basically has two ways to determine plug&play data. For more information, see Section 15.5.2.1, "Assignment Procedure".

   - **Assignment using Device ID**

     In the first alternative, the DLS checks whether it can determine a set of plug&play data records from the device ID presented by the workpoint. However, this option currently requires that the device ID and plug&play data be linked manually.

   - **Assignment using E.164**

     Using the E.164 number that is manually entered at the workpoint, the DLS checks whether it can determine a corresponding data record.
     Example of a complete E.164 number: **498972212345**.

3. If configuration templates have been defined (see Section 15.4) and grouped as the standard template, data from the templates is transferred to the workpoint.

4. The plug&play sequence is completed when all assigned data has been sent successfully.

15.6 Distribution of Workpoint Software

This section explains how to perform manual software or file deployment and which configurations are necessary for automatic deployment.

Note the difference between **Software Deployment** and **File Deployment** in the DLS interface (see Section 10.1.1 and Section 10.1.2).

Software deployment refers to the distribution of workpoint software (IP phones and IP clients). In contrast, **file deployment** means the distribution of any binary or ASCII files that perform a certain task in the workpoint.

Both functions are combined in the DLS main menu under **Software Deployment**.

For automatic deployment, see Section 15.6.2, "Automatic Deployment".

A single software deployment operation can take place for each workpoint at the same time as a file deployment operation, but it is not possible for multiple software deployment operations or multiple file deployment operations to take place simultaneously.

If you want to update workpoint software using a netboot server, and the update is not possible with a crosslink cable (crossed LAN cable), the workpoint must be connected to the Netboot server via a hub.

When distributing software for optiPoint WL2 professional workpoints, ensure that the workpoints have sufficient battery capacity. If not, it may not be possible to operate the software successfully.

Software image properties

A distinction between software images can be made on the basis of the following properties:

- Type of hardware supported (device type, such as optiPoint 410 Standard).
- Software type (such as, Siemens HFA).
- Software version (such as, CLA, DHCP, DNS, and FTP servers).5.1.3).
- Integrated DLS interface
  (yes = new, no = old SPA).
- Requiring a license (yes or no).

Licensed IP phone software is not yet available. The IP phone software that is currently on offer does not require a license.

15.6.1 Manual Deployment

In principle, you can define the following parameters during manual deployment:

- Which workpoints should be provided with the software.
- Which software should be used for the distribution.
- When the distribution should occur.

Requirements

- A working DLS infrastructure (such as
- The workpoints to be supplied have automatically registered at the DLS or were found by the DLS during a manual scan (see Section 7.4.4, "Scan IP Devices").
- The software to be distributed was either automatically or manually registered at the DLS (see Section 15.3, "Registering Workpoint Software and Files").

Performing distribution

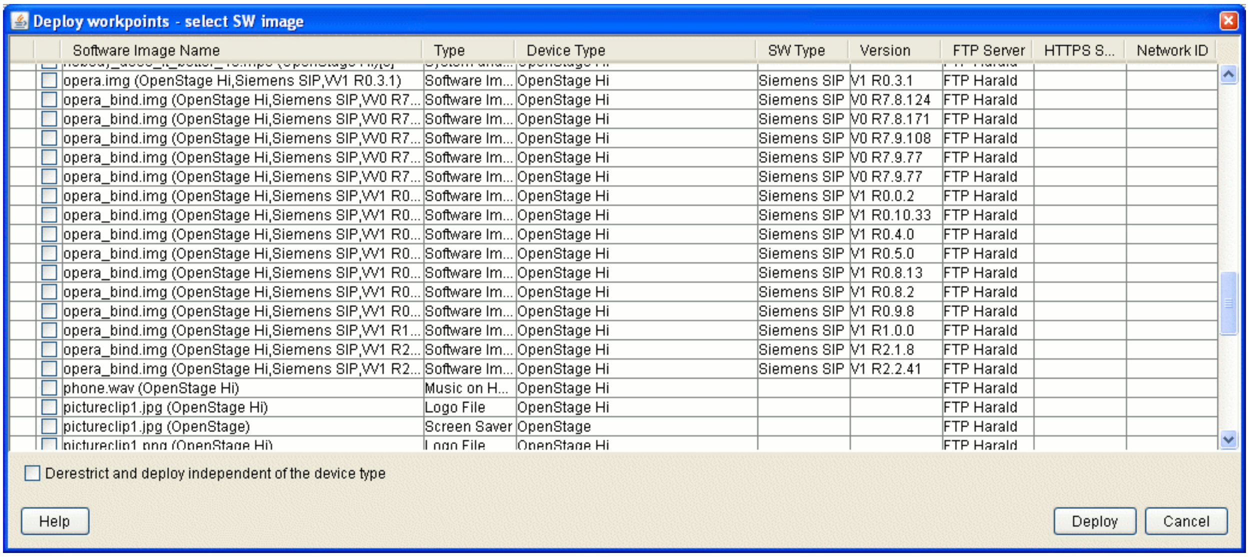
1. First decide which workpoints you want to provide with the software.
   Do this by choosing the **Software Deployment** > **Deploy Workpoints** area and, if necessary, enter search criteria in **Search** view. Click **Search** to start the search.

2. If one or more workpoints were found, the first entry is shown in **Object** view.
   To select multiple workpoints, change to **Table** view and hold down the `<CTRL>` key to select a number of individual workpoints or hold down the `<SHIFT>` key to select workpoint ranges.

3. Click **Deploy**.

> When you click **Deploy**, the system checks whether suitable software is available, that is, registered, for the selected workpoints.
> If this is not the case, an appropriate message is displayed. This is also true if you have selected both IP clients and different IP phones (optiPoint, OpenStage) in a multiple selection.

If suitable software was found, the following dialog appears (example):



Deploy workpoints - select SW image

	Software Image Name	Type	Device Type	SW Type	Version	FTP Server	HTTPS S...	Network ID
☐	opera.img (OpenStage Hi,Siemens SIP,V1 R0.3.1)	Software Im...	OpenStage Hi	Siemens SIP	V1 R0.3.1	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V0 R7...	Software Im...	OpenStage Hi	Siemens SIP	V0 R7.8.124	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V0 R7...	Software Im...	OpenStage Hi	Siemens SIP	V0 R7.8.171	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V0 R7...	Software Im...	OpenStage Hi	Siemens SIP	V0 R7.9.108	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V0 R7...	Software Im...	OpenStage Hi	Siemens SIP	V0 R7.9.77	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V0 R7...	Software Im...	OpenStage Hi	Siemens SIP	V0 R7.9.77	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R0...	Software Im...	OpenStage Hi	Siemens SIP	V1 R0.0.2	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R0...	Software Im...	OpenStage Hi	Siemens SIP	V1 R0.10.33	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R0...	Software Im...	OpenStage Hi	Siemens SIP	V1 R0.4.0	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R0...	Software Im...	OpenStage Hi	Siemens SIP	V1 R0.5.0	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R0...	Software Im...	OpenStage Hi	Siemens SIP	V1 R0.8.13	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R0...	Software Im...	OpenStage Hi	Siemens SIP	V1 R0.8.2	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R0...	Software Im...	OpenStage Hi	Siemens SIP	V1 R0.9.8	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R1...	Software Im...	OpenStage Hi	Siemens SIP	V1 R1.0.0	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R2...	Software Im...	OpenStage Hi	Siemens SIP	V1 R2.1.8	FTP Harald		
☐	opera_bind.img (OpenStage Hi,Siemens SIP,V1 R2...	Software Im...	OpenStage Hi	Siemens SIP	V1 R2.2.41	FTP Harald		
☐	phone.wav (OpenStage Hi)	Music on H...	OpenStage Hi			FTP Harald		
☐	pictureclip1.jpg (OpenStage Hi)	Logo File	OpenStage Hi			FTP Harald		
☐	pictureclip1.jpg (OpenStage)	Screen Saver	OpenStage			FTP Harald		
☐	pictureclip1.png (OpenStage Hi)	Logo File	OpenStage Hi			FTP Harald		

☐ Derestrict and deploy independent of the device type

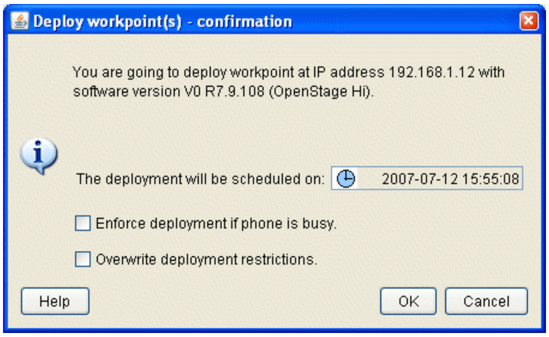
If a software image is not suitable for this workpoint type, the entry is displayed with a yellow triangle and dimmed. If you hover the mouse pointer over this icon, a ToolTip appears with the reason for this.
For example, the ToolTip "Software not applicable for this device type" states that a specific registered HFA software package cannot be distributed on Siemens HFA workpoints.

> ⚠ You can use the check box **Derestrict and deploy independent of the device type** to perform software deployment even for a workpoint that does not match the other workpoints because of the software license information (see Section 15.3.2, "Understanding License Information for IP Phone Software").
> In general, this is only necessary if you want to perform deployment for a new device type unknown to the DLS.
>
> The result can involve the loss of the entire workpoint functionality.
>
> If this check box is selected, all entries in the list (including ones that were previously dimmed) are available for selection.

4. Select an **Execution Time** in the toolbar. To do this, click the calendar symbol 📅 and select one of the time options and the conditions for the deployment. For more information on the calendar button, see Section 5.4.2.4, "Time field with calendar button".

5. Choose the entry that you want and click **Deploy** to stipulate the performance time.

6. A dialog window where you can start software distribution appears. By default, the software is set on the basis of the configured restrictions (see Section 6.2.2.6, ""SW Deployment Restrictions" Tab"). If you activate **Overwrite deployment restrictions**, these restrictions are ignored.



You are going to deploy workpoint at IP address 192.168.1.12 with software version V0 R7.9.108 (OpenStage Hi).

The deployment will be scheduled on: 2007-07-12 15:55:08

□ Enforce deployment if phone is busy.

□ Overwrite deployment restrictions.

7. Activating **Force deployment if device is busy** forces the deployment procedure to be carried out without delay even if a workpoint is busy (active call). You should only use this option in exceptional cases because it interrupts a telephone connection on the workpoint.

8. Activating **Overwrite deployment restrictions** forces deployment regardless of any restrictions that may be configured.

9. Click **OK**. If the license check was successful, individual jobs are generated for distribution to the selected workpoints and carried out at the specified time. A progress bar shows job generation progress (see Section 5.4.2.6, "Message Windows").

For more information on job coordination, see Section 15.7, "Using Job Coordination".

15.6.2 Automatic Deployment

As the name suggests, in addition to manual distribution (see Section 15.6.1, "Manual Deployment"), you can also distribute workpoint software automatically, that is, without user intervention.

If a workpoint is registered at the DLS, either during a manual scan (see Section 7.4.4, "Scan IP Devices") or as a result of first-time registration of a workpoint with software in the new format (with DLS interface), a deployment procedure will be initiated on the DLS that complies with the deployment rules.

The following describes how to configure the rules that control this procedure.

Requirements

- A working DLS infrastructure (such as CLA, DHCP, DNS and FTP servers).
- The workpoints to be supplied have automatically registered at the DLS or were found by the DLS during a manual scan (see Section 7.4.4, "Scan IP Devices").
- The software to be distributed was either automatically or manually registered at the DLS (see Section 15.3, "Registering Workpoint Software and Files").

Reconfiguring deployment rules

1. Select the **Software Deployment** > **Manage Rules** area and click **New**.
2. In the **Device Type** field, select the workpoint type to which the rule should apply.

> You can only configure one rule per combination of location, device type, software type, and software version.

3. In the **Location** field, select the location to which the rule should apply.
4. In the **Software Type** field, select the type of software type which is currently installed on the workpoints to which the rule should apply.
5. In the **WP SW Version** field, select the version of the software which is currently installed on the workpoints to which the rule should apply.
6. If applicable, activate **Deploy Newest SW Version** if only you want software deployment to be performed when there is a version available for distribution that is newer than the version installed at the time.
   Example: Version 5.1.9 is distributed to workpoints with version 5.1.1, while version 5.2.0 is left on the workpoint.

7. To distribute a very specific software version, you must deactivate **Deploy Newest SW Version**. You must make this setting to force a change in the workpoint software type. In this case, go to the **SW Image** and **Software Version** fields and select the required software image in the available software version from the lists or enter the image and version.
8. Click **Save** to save the new rule.
9. Click **Apply** to obtain a listing of all workpoints to which the rule applies. A dialog window opens up in which you can select the workpoints to which the rule shall apply effectively. After this, confirm by pressing **Apply** in the dialog window.

Repeat the procedure for each rule that you want to set up.

Automatic distribution sequence

Automatic software distribution is always initiated at the workpoint.

When registering a workpoint, the DLS first checks if there is a rule for the workpoint device type. If there is no rule or if the rule has been deactivated by deselecting **Deploy Default Software**, no further processing takes place.

If the distribution of the newest software is activated across the board, the newest software (software with the highest software version number) is distributed to all workpoints with the same software type. Workpoints with other software types do not receive new software.

If **Deploy newest version** is deactivated, each workpoint receives the software entered, without taking the software type into consideration.

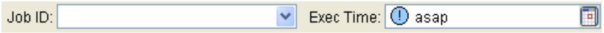
15.7 Using Job Coordination

In the DLS, all tasks are planned, processed, and logged with the help of jobs. Individual jobs can consist of a number of actions.

You can set up jobs in the following areas:

- Location
- Workpoint Interface Configuration
- Automatic SPE Configuration
- IP Phone Configuration
- IP Client Configuration
- IP Gateway Configuration
- IP Device Interaction
- SIP Mobile User Configuration
- SIP Mobile User Interaction
- Gateways
- Software Deployment
- Voice over IP Security V1

You can assign specific configuration, deployment, and interaction tasks to particular jobs in these areas by entering a name with **Job ID** and stipulating the execution time and execution option in the toolbar (see Section 5.4.2.4, "Time field with calendar button").



Job ID:

Exec Time: asap

If a name was defined before the object was saved, this then appears later in **Job Control** in addition to the action number. You can group individual actions into jobs to achieve greater clarity by manually entering a **Job ID**.

> Switching from daylight saving time to regular time (one hour back) will not lead to a second execution of a job that has been started in the time interval hereby doubled. When switching from regular time to daylight saving time (one hour advance), a job which is scheduled for this skipped time will not be executed.

You can configure properties for executing and logging jobs (see Section 14.3, "Job Configuration").

15.7.1 Defining a Job

A job is defined by entering a **Job ID** in the tool bar. You can enter a time in the future to the right of **Job ID**. In this case, the required action (such as, changes to IP Device parameters) is performed at the specified time instead of immediately.

To avoid assigning further actions to the specified job, simply select the empty entry from the selection list under **Job ID**. You can remove a defined time in the calendar dialog by clicking **Delete**.

15.7.2 Viewing Job Properties and Status

There are two tools available for checking and logging jobs.

Job Control

This function lets you view a large volume of information on the individual jobs and discard, delete, or reactivate existing jobs.

1. Click the **Job Coordination** > **Job Control** area.
2. If necessary, enter filter criteria to narrow the search to only jobs with certain properties. For example, this lets you search for jobs that are currently active, that is, they have not been processed yet.
3. Click **Search** to start the search.
   The search result shows all relevant data on each job or action that was found (see Section 14.1, "Job Control").
4. You can delete (completely remove) selected jobs or actions in **Object** and **Table** views. You can do this either before or after the job has executed.
   You can use **Discard job** to prevent a job from executing. This job remains in the list of all jobs, however, and is also still shown under **Daily Status**.

> You can discard any job regardless of its status. If the job's status is **done**, you can discard it and enter a new execution time. This allows you to reactivate jobs, that is, you can execute them again.

Daily Status

This function gives you a clear display of all jobs in a table and lets you filter them according to time frame and job status. You can also delete the jobs that are displayed here.

1. Click the area **Job Coordination** > **Daily Status**.
2. If necessary, restrict the statistics by entering an activation date and job status so that the search includes only jobs with these properties.
3. Click **Search** to start the search.
   The search results shows a table containing the job ID, job status, activation time and end time (see Section 14.2, "Daily Status").
   If several actions have been combined into one job ID and if at least one action has the status **time exceeded**, **discarded**, or **failed**, this status is shown for the entire job.
4. Click **Delete** to remove the job completely. If several actions have been combined into one job ID, all of these actions are deleted.

15.8 Backup/Restore

The DLS client interface provides enhanced options for automatically saving DLS data and restoring backups.

15.8.1 Automatic Data Backups

You can create and restore automatic backups of the entire DLS database. You can also view backup logs.

15.8.1.1 Configuring Automatic Backups

1. Click the **Administration** > **Backup/Restore** > **"Backup" Tab** area.
2. If you have not already done so, enter the path for saving the backup (without the file name) under **Backup Path** or select a suitable path by clicking **Browse**. Click **Test** once to check the availability of this path.
3. If necessary, change the maximum number of backup file types that should be backed up under **Max. Number of Backups**. The oldest backup file is deleted once this value is exceeded.
4. You can perform the following types of backups:
   – A single backup performed immediately.
   Click **Start Backup Now**.
   – A single backup performed at a specific time in the future.
      1. Enter a time in **Start Backups at** (for a calendar, see Section 5.4.2.4, "Time field with calendar button").
      2. Click **Save**.
   – A backup performed periodically on one, multiple or all weekdays.
      1. Enter a time in **Start Backups at** (for a calendar, see Section 5.4.2.4, "Time field with calendar button").
      2. Activate **Enable Daily Backups** .
      3. Activate or deactivate **Execute daily Backups on,** depending on your requirements.
      4. Click **Save**.

The backup file is created with the name `DLS_YYYYMMDD_HHMMSS.bak` in the directory you selected.

15.8.1.2 Restoring Backups

> A DLS database restore assumes that a database backup already exists, see Section 15.8.1.1, "Configuring Automatic Backups".
>
> If the database to be restored is older (modified database definition), please perform a migration instead of a restore (see Section 15.8.2.3, "Migrating DLS Database Data"). A migration should also be performed if you are not sure if the database backup is still compatible.
> There are some basic server configuration data which will never be restored as e.g.
> - the account the Deployment Service is running with
> - the license settings
> in order to guarantee a proper working after any restore.

1. Click the **Administration** > **Backup/Restore** > **"Restore" Tab** area.
2. Enter the name of the backup you want to restore under **Backup File** or select a suitable file by clicking **Browse**. Click **Test** to check the availability of this file.
3. Click **Restore** to start backup recovery.
4. A dialog window asks if Plug&Play shall be disabled after restore. When Plug&Play has been disabled, it can be enabled again via **Administration** > **Server Configuration** > **P&P Settings** > **Plug&Play enabled**. For this, it must be ensured that all IP Devices are registered in the DLS database.

15.8.1.3 Monitoring Backups

1. Click the **Administration** > **Backup/Restore**> **"Protocol" Tab** area.
2. Click **Refresh** to display the backup log. The log provides information on the time the backups and recoveries were created and their statuses, as well as the backup files used. Possible values for the backup/recovery status: **Backup OK**, **Backup failed**, **Deleted**, **Restore OK**, **Restore failed**.

15.8.2 Manual Database Manipulation

This section explains how you can manually manipulate data in the DLS SQL database. The data is stored on the PC on which the deployment service is also running (the DLS server).

> We strongly urge you to use the automatic DLS Backup/Restore function as this is a simpler and more secure procedure (see Section 15.8.1, "Automatic Data Backups").

You can:

- perform a backup of all data, see Section 15.8.2.1,
- restore saved data, see Section 15.8.2.2,
- migrate a database backup with a current database definition (combine), see Section 15.8.2.3,
- reset the database (delete all database data), see Section 15.8.2.4.

15.8.2.1 Backing Up DLS Database Data

To back up the DLS server SQL database, proceed as follows:

1. Close all browser windows connected to the DLS.
2. End *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. End the SQL server. Do this by right-clicking the SQL server icon in the system tray and selecting **MSSQLServer - Stop** in the context menu.
   The icon in the system tray changes from ▶ to ■.
4. Save the directory **[installation path]\DeploymentService\DB\** with all subdirectories by executing the following command:
   ```
   [Installation path]\DeploymentService\webapps\
   DeploymentService\database\dbexport.bat <filename>.zip
   ```
5. Start *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

15.8.2.2 Restoring DLS Database Data

A DLS database restore assumes that a database backup already exists, see Section 15.8.2.1, "Backing Up DLS Database Data".

If the database to be restored is older (modified database definition), please perform a migration instead of a restore (see Section 15.8.2.3, "Migrating DLS Database Data"). A migration should also be performed if you are not sure if the database backup is still compatible.

There are some basic server configuration data which will never be restored as e.g.
- the account the Deployment Service is running with
- the license settings
in order to guarantee a proper working after any restore.

The procedure for restoring a saved database is similar to the one already described for a backup.

1. Close all browser windows connected to the DLS.
2. End *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. Restore the the DLS data by executing the following command:
   ```
   [Installation path]\DeploymentService\webapps\
   DeploymentService\database\dbimport.bat <filename>.zip
   ```
4. Start *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

15.8.2.3 Migrating DLS Database Data

"Migration" here means that you can restore a saved database even if the database definition has been changed in the meanwhile. The database definition can change over time, for example, if IP Device configuration parameters are added .

1. Close all browser windows connected to the DLS.
2. End *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. To migrate the DLS data, execute the following command:
   ```
   [Installation path]\DeploymentService\webapps\
   DeploymentService\database\migrate.bat <exportfilename>.zip
   ```
   The file `<exportfilename>` must be created by a backup of DLS data (see Section 15.8.2.1, "Backing Up DLS Database Data").

4. Start *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

15.8.2.4 Resetting the DLS Database

You can reset the DLS database, which means that you can delete all data. As far as the data in the database is concerned, this produces the same result as the uninstallation (Section 4.12, "Uninstalling the Deployment Service") and renewed installation of the complete DLS application.

> ⚠ A reset deletes all data in the DLS database.
> To avoid data loss, create a backup of the database before you carry out the reset (see Section 15.8.2.1, "Backing Up DLS Database Data").

1. Close all browser windows connected to the DLS.
2. End *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. Delete the database by executing the following command:
   ```
   [Installation path]\DeploymentService\webapps\
   DeploymentService\database\dbinstall.bat delete
   ```
4. Create a new database by executing the following command:
   ```
   [Installation path]\DeploymentService\webapps\DeploymentService\database\dbinstall.bat update create <passwort>
   ```
   `<passwort>` defines the password for the user "admin".
5. Start *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

15.8.2.5 Troubleshooting: Lizenzagent is unreachable

If the DLS cannot be called due to a deficient connection to the license agent, a different license agent can be entered in the DLS database. This is accomplished by the following steps:

1. Close all browser windows that are connected to the DLS.
2. On the DLS server, terminate the service "Deployment service" by clicking on **Programs** > **Deployment Service** > **Stop Service** in the Windows start menu.
3. Execute the command that is appropriate for the desired action:
   - to change the license agent:
     ```
     [Installation path]\DeploymentService\webapps\
     DeploymentService\database\dbinstall.bat setcla <hostname>
     <port>
     ```
   - to change the license manager:
     ```
     [Installation path]\DeploymentService\webapps\
     DeploymentService\database\dbinstall.bat setclm <hostname>
     <port>
     ```
   - if multiple DLS share one license agent:
     ```
     [Installation path]\DeploymentService\webapps\
     DeploymentService\database\dbinstall.bat setmaxbasicdevices
     <Number of Devices>
     [Installation path]\DeploymentService\webapps\
     DeploymentService\database\dbinstall.bat setmaxmobileusers
     <Number of Mobile Users>
     ```

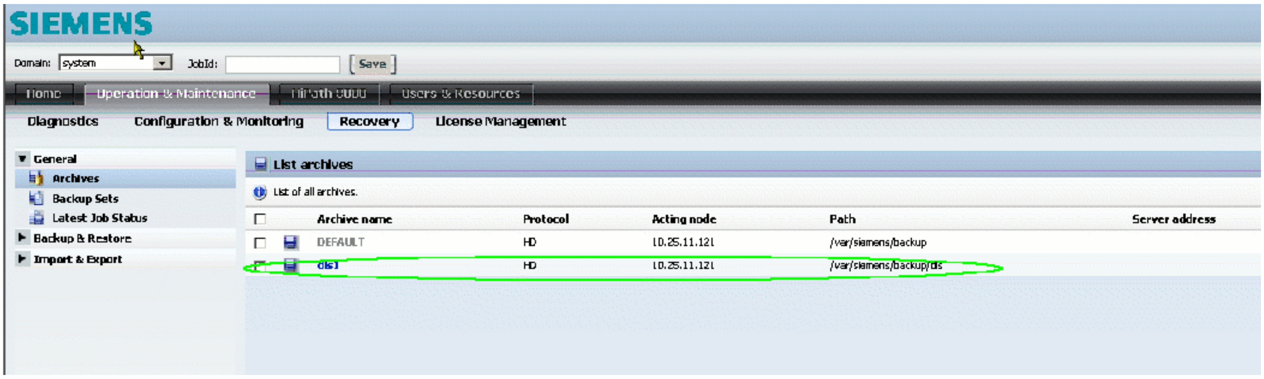
4. Start the service "Deployment service" on the DLS server by clicking on **Programs** > **Deployment Service** > **Start Service** in the Windows start menu.

15.9 Backup & Restore On OpenScape Voice Integrated and Linux Standalone Installations

This chapter describes DSL database backup and recovery for the OpenScape Voice onboard version and the Linux Standalone version.

15.9.1 Backup

1. Log on at the Common Managament Portal. The management portal is reached under `https://<IP of server>`
2. Navigate to **Operation & Mainentance** > **"Recovery" Tab**. Create an archive for DLS backups, e. g. in `/var/siemens/backup/dls`.

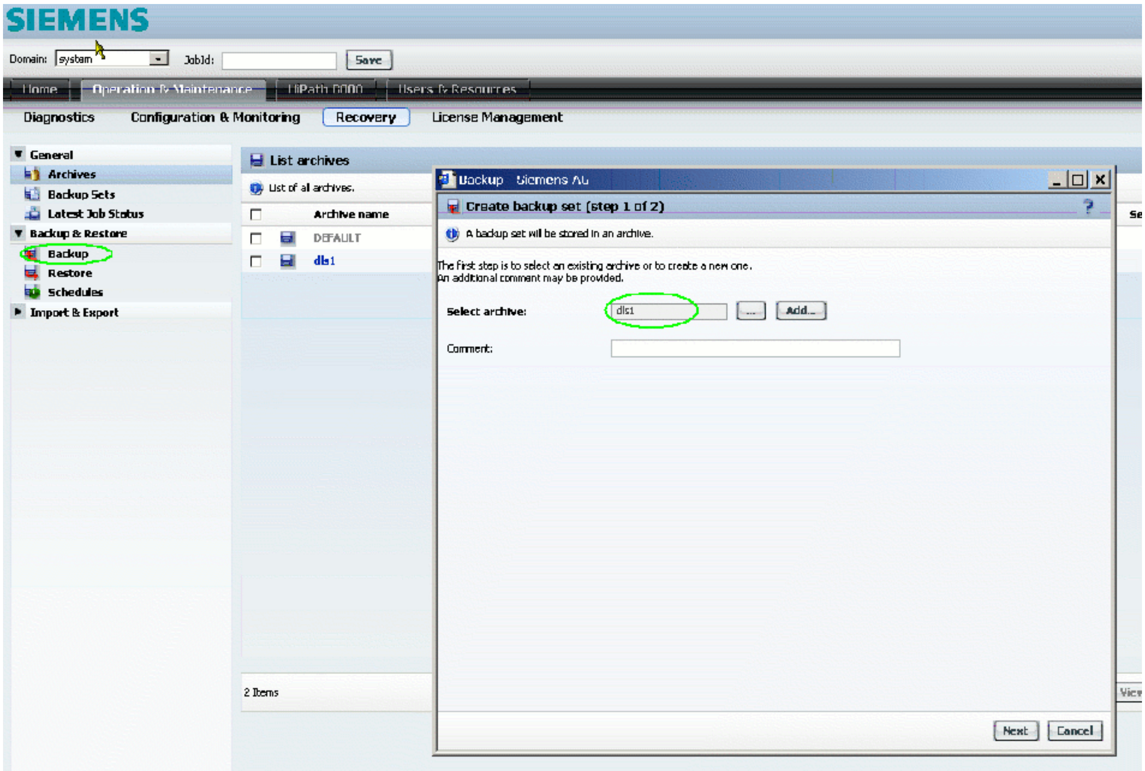


List archives

List of all archives.

□		Archive name	Protocol	Acting node	Path	Server address
□		DEFAULT	HD	10.25.11.121	/var/siemens/backup	
□		dls1	HD	10.25.11.121	/var/siemens/backup/dls	

3. To create a backup, firstly open the folder **Backup & Restore** and click **Backup**. In the **Backup** window, in the **Select archive** field, select the newly created archive.



List of all archives.

□	Archive name
□	DEFAULT
□	dls1

2 Items

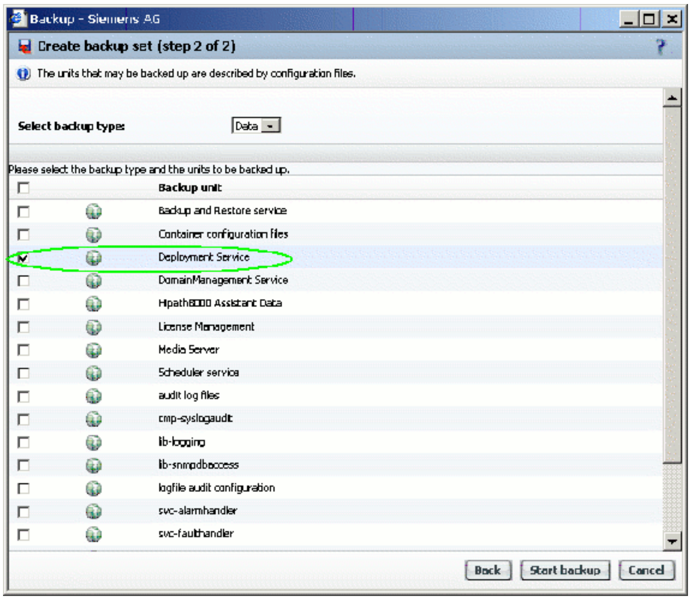
A backup set will be stored in an archive.

The first step is to select an existing archive or to create a new one.
An additional comment may be provided.

Select archive: dls1

Comment:

4. As **Backup unit**, select **Deployment Service**. Afterwards, click **Start backup**.



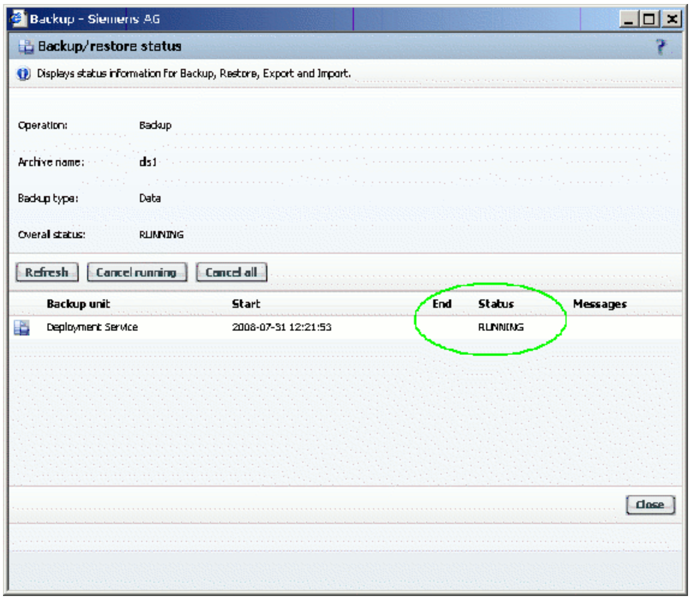
The units that may be backed up are described by configuration files.

Select backup type: Data

Please select the backup type and the units to be backed up.

□	Backup unit
□	Backup and Restore service
□	Container configuration files
☑	Deployment Service
□	DomainManagement Service
□	Hipath8000 Assistant Data
□	License Management
□	Media Server
□	Scheduler service
□	audit log files
□	cmp-syslogaudit
□	lib-logging
□	lib-snmpdbaccess
□	logfile audit configuration
□	svc-alarmhandler
□	svc-faulthandler

5. Wait until **Status** changes from **RUNNING** to **OK** (this screen refreshes automatically).



Displays status information for Backup, Restore, Export and Import.

Operation: Backup

Archive name: ds1

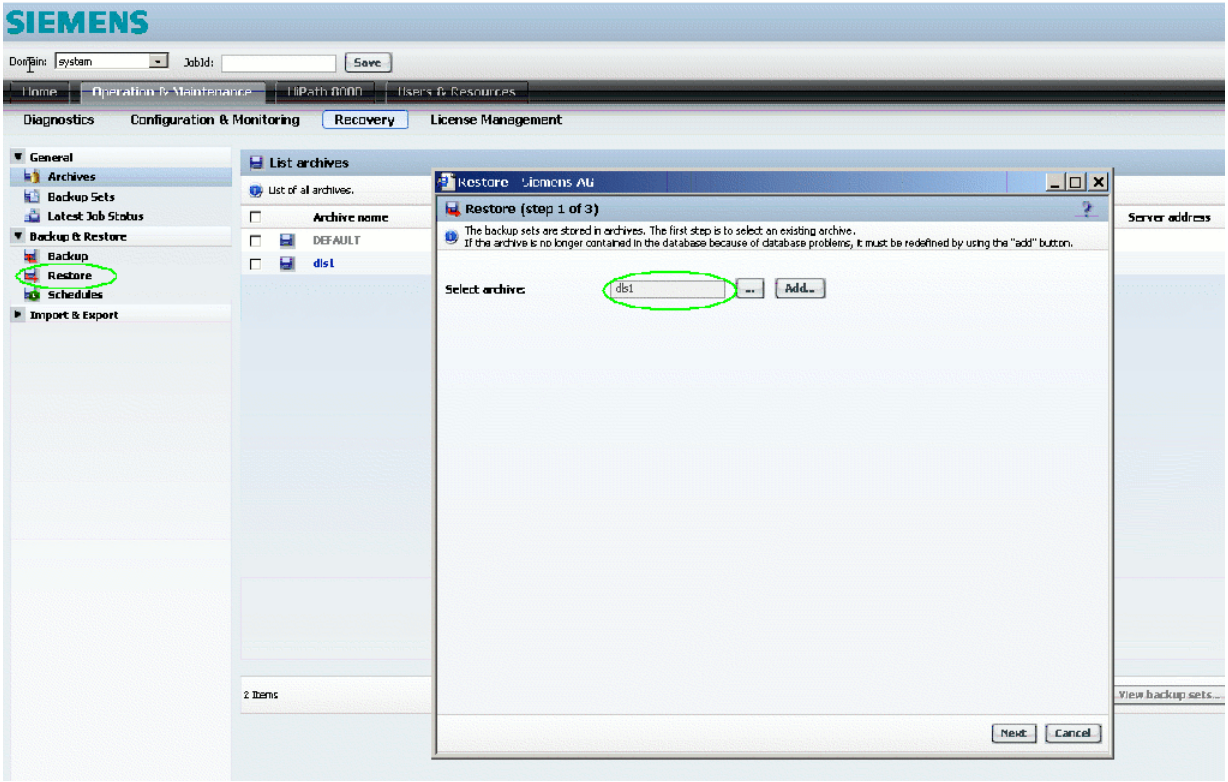
Backup type: Data

Overal status: RUNNING

Backup unit	Start	End	Status	Messages
Deployment Service	2008-07-31 12:21:53		RUNNING	

15.9.2 Restore

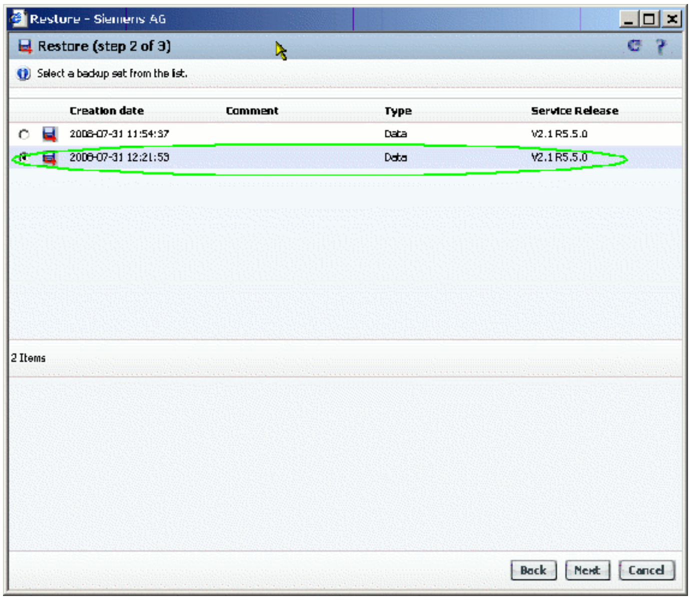
1. To restore a database, firstly open the folder **Backup & Restore** and click **Restore**. In the **Restore** window, in the **Select archive** field, select the archive containing the desired backup, and click **Next**.



The backup sets are stored in archives. The first step is to select an existing archive.
If the archive is no longer contained in the database because of database problems, it must be redefined by using the "add" button.

Select archive: dls1

2. Select the desired backup from the list. The backups are identified by a time stamp or optional comment. Click **Next**.



Restore - Siemens AG

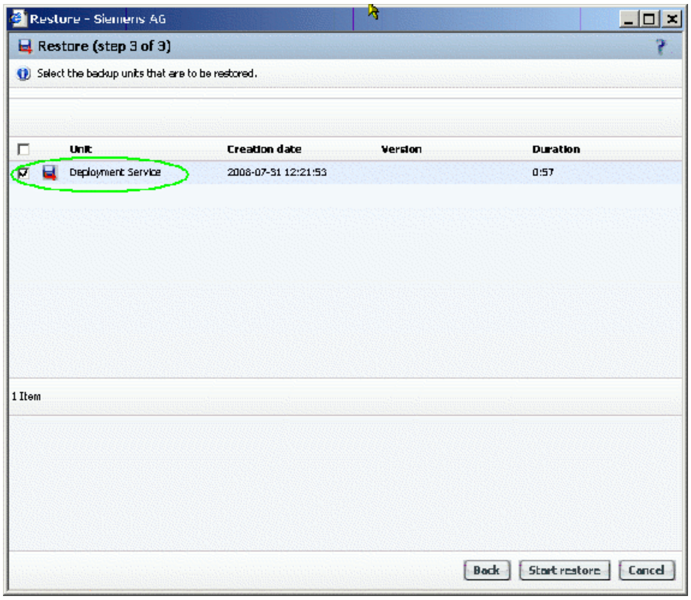
Restore (step 2 of 3)

Select a backup set from the list.

	Creation date	Comment	Type	Service Release
○	2008-07-31 11:54:37		Data	V2.1 R5.5.0
●	2008-07-31 12:21:53		Data	V2.1 R5.5.0

2 Items

3. As backup **Unit**, select **Deployment Service**, and click **Start restore**.



Restore - Siemens AG

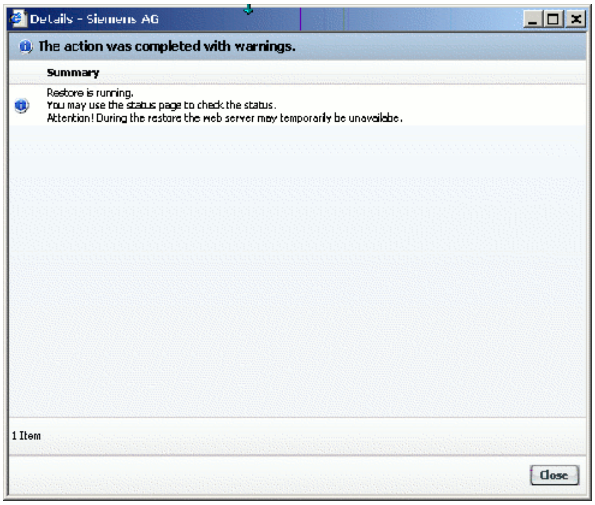
Restore (step 3 of 3)

Select the backup units that are to be restored.

□	Unit	Creation date	Version	Duration
☑	Deployment Service	2008-07-31 12:21:53		0:57

1 Item

4. You will be presented with a confirmation window. As this window will not refresh automatically, you can close it any time.



Details - Siemens AG

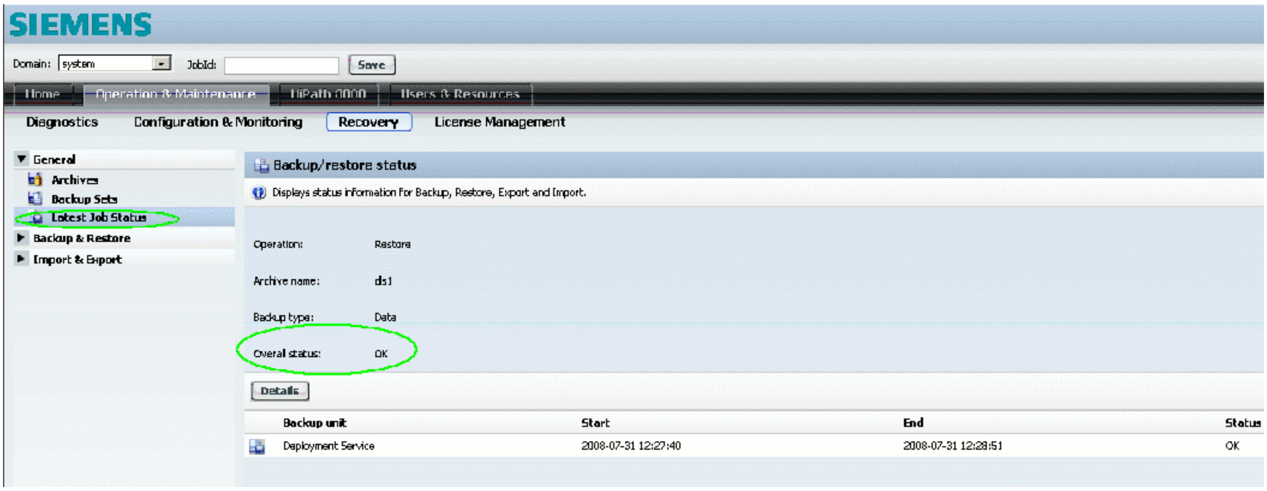
The action was completed with warnings.

Summary

Restore is running.
You may use the status page to check the status.
Attention! During the restore the web server may temporarily be unavailabe.

1 Item

5. To check the state of the restore process, use the **Latest Job Status** screen.



Domain: system JobId:

Backup/restore status

Displays status information for Backup, Restore, Export and Import.

Operation: Restore

Archive name: ds1

Backup type: Data

Overal status: OK

Backup unit	Start	End	Status
Deployment Service	2008-07-31 12:27:40	2008-07-31 12:28:51	OK

15.9.3 Post-Restore Procedures

After the database has been restored successfully, the following manual steps must be performed, using shell commands on the server.

1. Log in as root at the Linux server or OpenScape Voice (for OpenScape Voice cluster: at both nodes).
2. Stop DeploymentService:
   ```
   sh /etc/init.d/symphoniad stop TomcatServletContainer
   ```
   On OpenScape Voice Cluster: Perform this step at both nodes.
3. Adopt the DLS database to the current layout. The command paths vary according to the platform.
   On Linux Standalone:
   ```
   cd /opt/siemens/share/tomcat/webapps/DeploymentService/database
   sh dbinstall.sh update
   ```
   On OpenScape Voice:
   ```
   cd /enterprise/share/tomcat/webapps/DeploymentService/database
   sh dbinstall.sh update
   ```
   On a OpenScape Voice cluster, you need to perform this step only on that node where the PRIMARY database is located. You can check the result with the following command:
   ```
   su - srx -c "RtpSolid -l"
   ```
4. Start DeploymentService:
   ```
   sh /etc/init.d/symphoniad start TomcatServletContainer
   ```
   On OpenScape Voice cluster, perform this step on both nodes.

15.10 Importing and Exporting Plug&Play Data

The following section describes how to import and export workpoint plug&play data as files in CSV format.

15.10.1 Exporting Plug&Play Data

The following steps explain how to store plug&play data from a particular workpoint as a CSV file on the DLS server.

> A file that already exists with the name you enter will be overwritten.

1. Click the **IP Devices** > **IP Device Management** > **IP Device Configuration** area.
2. Locate and select the workpoints from which you want to export plug&play data and click **Export File**.
3. In the subsequent dialog, enter the name of the export file on the server and click Save.
4. A window appears confirming that the export was successful or displaying an error message.

15.10.2 Importing Plug&Play Data

The following steps explain how to import plug&play data from a CSV file on the DLS server. Detailed import results documenting which workpoints were newly created, which were modified and on which errors occurred, for instance, can be found in the log file. It is displayed under **Administration** > **Display Logging Data** > **P&P Import Protocols**.

1. Click the **IP Devices** > **IP Device Management** > **IP Device Configuration** area.
2. Click **Import File** in Search view.
3. Enter the name of the CSV file you wish to import in the next dialog. In this dialog, you can also specify whether workpoints created during the import should be created as IP phones and/or IP clients. Confirm the next dialog by clicking **Open**.
4. A window appears on the client confirming that import was executed and giving the location of the log file containing the import results.

15.10.3 Syntax of the .csv Files

The .csv file used for import and export has following format:

- 1st row: Description of content of columns
- 2nd and following rows: command and parameters

If a parameter is not needed, a ';' must be included to mark an empty parameter.

Empty lines and lines starting with a '#' will be ignored.

If a virtual ID is used (no MAC address), a second trial is ignored, and will be documented in the protocol file. As long as different MAC addresses are in use, it is possible to create multiple devices with a common E.164 number.

> Prior to changing keys or keysets, a device must be created.

> This format is supported by DLS version V2R2 onwards. Older formats are supported further on; in such cases, all devices are imported als IP phones. If IP clients are to be imported, a conversion to the previously described format is necessary.

You can find a list of parameters under Section 15.10.3.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

15.10.3.1 Create a SIP Phone (CreateSIPPhone)

Command syntax for creating a SIP phone:

```
CreateSIPPhone;<DeviceID>;<e164 number>;<IP Phone Type>;<Software Ty-
pe>;<Software Version>;<Device Profile>;<Remark>;<Basic Profile>;<Re-
store Basic Profile after Workpoint Reset>;<Terminal Name>;<Display
ID>;<SIP User ID>;<SIP Password>;<SIP Realm>;<SIP Server Addr.>;<SIP
Server Port>;<SIP Registrar Addr.>;<SIP Registrar Port>;<SIP Rou-
ting>;<SIP Gateway Addr.>;<SIP Gateway Port>;
```

You can find a parameter list under section Section 15.10.3.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateSIPPhone;02:00:00:00:00:05;4989925000005;OpenStage 80;Siemens
SIP;0.0.0;;;;fal-
se;;;;b6589fc6ab0dc82cf12099d1c;;139.21.93.205;5060;0.0.0.0;0;;
```

15.10.3.2 Create an HFA Phone (CreateHFAPhone)

Command syntax for creating a SIP phone:

```
CreateHFAPhone; <DeviceID>;<e164 number>;<IP Phone Type>;<Software
Type>;<Software Version>;<Device Profile>;<Remark>;<Basic Profi-
le>;<Restore Basic Profile after Workpoint Reset>;<Subscriber Num-
ber>;<Gatekeeper>;<Gatekeeper Password>;<Subscriber Number (Stand-
by)>;<Gatekeeper (Standby)>;<Gatekeeper Password (Standby)>
```

You can find a parameter list under section Section 15.10.3.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateHFAPhone;00:01:E3:25:E2:19;498972221456;OpenStage 80;Siemens
HFA;V1 R0.0.93;;;;false;21456;218.1.16.211;;;;;
```

15.10.3.3 Create a SIP Client (CreateSIPClient)

Command syntax for creating a SIP phone:

```
CreateSIPClient;<DeviceID>;<e164 number>;<IP Client Type>;<Software
Type>;<Software Version>;<Device Profile>;<Remark>;<Basic Profi-
le>;<Restore Basic Profile after Workpoint Reset>;<Terminal Name>;<SIP
User ID>;<SIP Password>;<SIP Realm>;<SIP Server Addr.>;<SIP Registrar
Addr.>;<SIP Registrar Port>;<SIP Gateway Addr.>;<SIP Gateway Port>;
```

You can find a parameter list under section Section 15.10.3.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateSIPClient;00:19:99:03:5B:0E;498972221458;optiClient 130;
Siemens oC-Bundle;5.1.182.0000;;;;;;;;218.1.16.211;218.1.16.211;5060
;;5060;;
```

15.10.3.4 Create an HFA Client (CreateHFAClient)

Command syntax for creating an HFA Client:

```
CreateHFAClient; <DeviceID>;<e164 number>;<IP Client Type>;<Software
Type>;<Software Version>;<Device Profile>;<Remark>;<Basic Profi-
le>;<Restore Basic Profile after Workpoint Reset>;<Subscriber Num-
ber>;<Gatekeeper>;<Gatekeeper Password>;<Subscriber Number (Stand-
by)>;<Gatekeeper (Standby)>;<Gatekeeper Password (Standby)>
```

You can find a parameter list under section Section 15.10.3.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateHFAClient;00:19:99:03:5B:0E;498972221458;optiClient 130;
Siemens oC-Bundle;5.1.182.0000;;;;;21458;;;;;;
```

15.10.3.5 Create an IP Gateway (CreateIpGateway)

Command syntax for creating an IP Gateway:

```
CreateIpGateway;<DeviceID>;<IP Gateway Type>;<Software Type>;
<Software Version>;<Device Profile>;<Remark>
```

You can find a parameter list under section Section 15.10.3.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateIpGateway;139.21.93.205;HG1500;Siemens CGW;HXG_V7_R0.215.4;;;
```

15.10.3.6 Modify Key

This command enables enables to create or change the configuration of a particular device key. You can set any device key, depending on the type, software and version of the IP phone. With the reset parameter, all key functions can be deleted before setting them newly. If this field is empty, the existing keys remain unchanged.

Syntax:

```
ModifyKey;<reset>;<e164 number>|deviceId=<deviceId>;
<key function>;<level>;<module>;<key-number>[;<name>=<value>]+
```

> The default value is `e164`. If a device ID is to be used, `deviceId=<deviceId>` must be written.

You can find a list of parameters under Section 15.10.3.11, "Parameter Description for ModifyKey, ModifyKeyset".

Examples

1. An OptiPoint 410 advance shall be equipped with a control key for a headset:
   `ModifyKey;false;218116231;024;001;0;1;locked-function-keys=false;`
   As an alternative, the UI term "headset" can be used for defining the key function, instead of the function number (here: 024).

2. For setting up a direct station select (DSS) key, 2 steps are required:
   1. Set up a primary line
   `ModifyKey;false;218116230;line;000;0;1;`
   `line-sip-uri=49897223500;line-primary=true;`
   2. Set up the direct station select key
   `ModifyKey;false;218116230;dss;000;0;3;line-sip-uri=498972233439`

3. To delete a function key, set the key function to "Key Unused". In this example, key #3 is deleted:
   `ModifyKey;false;218116232;Key Unused;0;0;3`

15.10.3.7 Modify Keyset

The values of a keyset can be modified. With the reset parameter, all key functions can be deleted before setting them newly. If the field is empty, the existing keyset vaues remain unchanged.

Syntax:

```
ModifyKeyset;<reset>;<e164 number>|deviceId=<deviceId>[;<attribute-name>=
<attribute-value>]+
```

> The default value is `e164`. If a device ID is to be used, `deviceId=<deviceId>` must be written.

You can find a parameter list in Section 15.10.3.11, "Parameter Description for ModifyKey, ModifyKeyset".

Example

In the following example, multiple parameters are set:

1. Rollover volume is set to 2 (line-rollover-volume).

2. Show focus is reset (keyset-use-focus => 0; true/false can also be used for activating/ deactivating.

3. LED on registration is set (line-registration-leds, 0/1 can be used as well).

```
ModifyKeyset;false;218116230;line-rollover-volume=2;
keyset-use-focus=0;line-registration-leds=true;
```

15.10.3.8 Modify Device Attributes (ModifyDevice)

This command enables to create or change device attributes, dependent on type, software and version of the IP phone. The allowed device attributes are described under:

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_Device_EN.html
```

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_SIPRegistration_EN.html
```

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_HFARegistration_EN.html
```

Syntax:

```
ModifyDevice;<e164>|deviceId=<deviceId>[;<attribute-name>=<attribu-
te-value>]+
```

> The default value is `e164`. If a device ID is to be used, `deviceId=<deviceId>` must be written.

You can find a parameter list under Section 15.10.3.12, "Parameter Description for ModifyDevice".

Example:

```
ModifyDevice;218116230;remark=Testdeviceconfiguration;
display-id=6230;display-id-unicode=6230;
```

15.10.3.9 Modify OpenScape Data (ModifyOpenScape)

This command enables modification of OpenScape Data.

The allowed attributes and their values are described under:

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_OpenScapeParam_EN.html
```

Syntax:

```
ModifyOpenScape;<reset>;<e164 number>|<deviceId=anyDeviceId>
[;<attribute-name>=<attribute-value>]+
```

> The default value is `e164`. If a device ID is to be used, `deviceId=<deviceId>` must be written.

Example:

```
ModifyOpenScape;false;498972231234;osc-connection-userid=31234;
osc-connection-port=4709;osc-connection-use-standardproxy=true;
osc-connection-use-https=true;osc-xmp-port=5222;
osc-xmp-use-https=false;osc-rules-port=8443;
```

15.10.3.10 Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway

Unless otherwise stated, it is about parameters in the menu IP Devices> IP Phone Configuration > Gateway/Server.

Parameter	optional/required	DLS Parameter	Description
Device ID	optional	Device ID	MAC address. If not specified, a virtual ID is created by the DLS.
e164 number	required	E.164	Unique E.164 number, max. 24 characters.

Table 15-1

Parameter	optional/required	DLS Parameter	Description
IP Phone Type, IP Client Type, IP Gateway Type	optional	Device Type	Device type or virtual device. Alphanumeric, max. 50 characters. Possible values: IP Phone Type: "Possible Values for IP PhoneType". IP Client Type: Possible Values for IP Client Type: IP Gateway: Possible Values for IP Gateway Type:
Software Type	optional	SW Type	Alphanumeric, max. 30 characters.
Software Version	optional	SW Version	Alphanumeric, max. 30 characters.
Device Profile	optional	Device Profile	Alphanumeric, max. 30 characters.
Remark	optional	Remark	Alphanumeric, max. 256 characters.
Basic Profile	optional	IP Devices > IP Device Management > IP Device Configuration > "Profile" Tab > Basic Profile	Alphanumeric, max. 40 characters.
Restore Basic Profil after Workpoint Reset	optional	Apply Basic Profile at IP Device Registration	Possible values: true / false or 1/ 0
Terminal Name	optional	Terminal Name	Alphanumeric, max. 255 characters.
Display ID	optional	Display ID	Alphanumeric, max. 24 characters
SIP User ID	optional	UserID	1st part of SIP URL, alphanumeric, max. 20 characters

Table 15-1

Parameter	optional/required	DLS Parameter	Description
SIP Password	optional	Password	Password, max. 25 characters
SIP Realm	optional	SIP Realm	Alphanumeric, max. 93 characters.
SIP Server Addr	optional	Reg-Adr	IP Address, max. 25 characters
SIP Server Port	optional	Reg-Port	Port number, numeric, max. 5 Zeichen, default: 5060.
SIP Registrar Addr	optional	SIP Registrar Adr	IP Address, alphanumeric, max. 255 characters
SIP Registrar Port	optional	SIP Registrar Port	Portnumber, numeric, max. 5 characters
SIP Routing	optional	SIP Routing	Poss. Values: Server, Gateway, Direct
SIP Gateway Addr	optional	SIP Gateway Addr	IP Address, alphanumeric, max. 255 characters
SIP Gateway Port	optional	SIP Gateway Port	Portnumber, numeric, max. 5 characters, default: 5060
Subscriber Number	optional	Registration Subscriber Number	HFA parameter, E.164 number, max. 24 characters
Gatekeeper	optional	Gatekeeper ID	HFA parameter, domain-ID, max. 255 characters
Gatekeeper Password	optional	Subscriber Password	HFA parameter, password, max. 24 characters
Subscriber Number (Standby)	optional	Registration Subscriber Number (Standby)	HFA parameter, E.164 number, max. 24 characters

Table 15-1

Parameter	optional/required	DLS Parameter	Description
Gatekeeper (Standby)	optional	Gatekeeper ID (Standby)	HFA parameter, domain ID, max. 255 characters
Gatekeeper Password (Standby)	optional	Subscriber Password (Standby)	HFA parameter, password, max. 24 characters

Table 15-1

15.10.3.11 Parameter Description for ModifyKey, ModifyKeyset

Parameter	optional/required	DLS Parameter	Description
Device ID	optional	Device ID	MAC address. If not specified, a virtual ID is created by the DLS.
e164 number	required	E.164	Unique E.164 number, max. 24 characters.
key function	optional	IP Devices > IP Phone Configuration > Keysets/Keylayout > "Destinations" Tab > Key function	For possible values, see table "Possible Values for Key Function".
level	optional	IP Devices > IP Phone Configuration > Keysets/Keylayout > "Destinations" Tab > Level	Poss. Values: 0 = 1st Level,1= 2nd Level, 2 = 3rd Level, 3 = 4th Level
module	optional	Module	Poss. Values: 0 ... 4
key-number	optional	IP Devices > IP Phone Configuration > Keysets/Keylayout > "Destinations" Tab > Key number	Numeric. For possible values, please see table "Possible Values of name for ModifyKey".
attribute-name	optional	----	For possible values, please see table "Possible Values of name for ModifyKey".
name	optional	----	For possible values, please see table "Possible Values of name for ModifyKey".
reset	optional	No DLS parameter	Poss. values: true/ false, 1/ 0

15.10.3.12 Parameter Description for ModifyDevice

Parameter	optional/required	DLS Parameter	Description
Device ID	optional	Device ID	MAC address. If not specified, a virtual ID is created by the DLS.
e164 number	required	E.164	Unique E.164 number, max. 24 characters.
attribute-name	optional	----	For possible values, see the table "Possible Values for attribute-name in ModifyDevice".

Possible Values for attribute-name in ModifyDevice

- `...\DeploymentService\api\doc\v200\dlsapi\device\index_Device_EN.html`
- `...\DeploymentService\api\doc\v200\dlsapi\device\index_SIPRegistration_EN.html`
- `...\DeploymentService\api\doc\v200\dlsapi\device\index_HFARegistration_EN.html`

Possible Values for IP PhoneType

- Mobile User SIP60
- OpenStage 15
- OpenStage 20
- OpenStage 20E
- OpenStage 40
- OpenStage 60
- OpenStage 80
- optiPoint 410 advance
- optiPoint 410 economy
- optiPoint 410 economy plus optiPoint 420 advance
- optiPoint 410 entry
- optiPoint 420 economy
- optiPoint 420 economy plus
- optiPoint 420 standard

Possible Values for IP Client Type

- **optiPoint 130**
- **Siemens OpenScape Desktop Client**
- **AC-Win 2Q IP**
- **AC-Win MQ IP**

Possible Values for IP Gateway Type

- **HG1500**
- **HG3500**
- **HG3575**
- **HOOEE**
- **HOOME V1**
- **HP2K V2.0**

Possible Values for Key Function

Function	Code
Key Unused	000
Selected Dialing	001
Abbreviated Dialing	002
Repeat Dialing	003
Missed Calls	004
Voice Messages	005
Forwarding	006
Loudspeaker	007
Mute	008
Ringer Off	009
Hold	010
Alternate	011
Blind Transfer	012
Join (optiPoint)	013
Transfer Call (OpenStage)	013
Deflect	014
Setup Menu	015

Table 15-2

Function	Code
Room Echoing	016
Room Muffled	017
Shift	018
Notebook	019
Settings	020
Phone Lock	021
Conference	022
Local Conference	023
Headset	024
Do Not Disturb	025
Group Pickup	029
Repertory Dial	030
Line	031
Feature Toggle	032
Show Phone Screen	033
Swap Screen	041
Mobility	042
Call Park	044
Call Pickup	045
Cancel/Release	046
Ok Confirm	047
Callback Request	048
Cancel Callback	049
consultation transfer	050
DSS	051
State Key	052
Call Waiting Toggle	053
Immediate Ring	054
Preview Key	055
Call Recording	056

Table 15-2

Function	Code
AICS Zip	057
Server Feature Key	058
BLF	059
start application	060
send url	063
built-in forwarding	064
built-in release	065
built-in voice dial	066
built-in redial	067
start phonebook	068

Table 15-2

Possible Values of name for ModifyKey

Name	DLS Parameter	DLS description	Type
key-destination	Destination	Destination data to be dialed. This can be a digit string or a URL.	Alphanumeric, max. 255 characters
state-key-uri	Feature-URI	URI used to control this feature on the server.	Alphanumeric, max. 48 chars
line-primary	Primary Line	Specifies whether the line operates as a primary line.	Poss. values: true/ false
line-sip-uri	Address of record	Line’s phone number and address of record.	E.164 number
line-sip-realm	Realm	SIP realm for the line's address of record.	Alphanumeric, max. 48 characters
line-sip-user-id	UserID	User ID	Alphanumeric, max. 48 characters
line-sip-pwd	Password	Password	Alphanumeric, max. 48 characters

Table 15-3

Name	DLS Parameter	DLS description	Type
line-ring	Ring	Ring	Poss. values: true/ false
line-hunt-sequence	Hunt Ranking	Hunt Ranking	0 ... 10
line-shared-type	Shared type	Shared type	Poss. Values: • Private • Shared • Unknown
feature-toggle-description	Toggle text	Label for the "Feature Toggle" key function.	Alphanumeric, max. 24 characters
feature-toggle-code-description-unicode	Toggle text (Unicode)	Label for the "Feature Toggle" key function in unicode.	Alphanumeric, max. 24 characters
state-key-description-text	State Key Description	Description text for the state key.	Alphanumeric, max. 22 characters
state-key-description-text-unicode	State Key Description (Unicode)	Description text for the state key in unicode.	Alphanumeric, max. 22 characters
key-label	Key Label	A key label can be entered here for every key in the case of Self labeling Keys workpoints (for example, optiPoint 420 standard).	Alphanumeric, max. 24 characters
key-label-unicode	Key label (Unicode)	You can enter the key label in unicode characters for devices in the OpenStage family.	Alphanumeric, max. 24 characters
line-hidden	Show on APM/DSM	Check box for activating the line display on the optiPoint Application Module/Display Module	Poss. values: true/ false
line-int-allow	Line intrusion allowed	Check box for enabling line intrusion	Poss. values: true/ false
line-hld-active	Line Hotline Dest. active	Check box for activating a line hotline.	Poss. values: true/ false

Table 15-3

Name	DLS Parameter	DLS description	Type
line-hld	Line Hotline Destination	Subscriber number that is used as a destination for the line hotline.	Alphanumeric, max. 60 characters
line-mlo-pos	Overview Position on APM/DSM	Overview Position on APM / DSM	Number, length 2
line-short-desc	Line Description	Description of Line	Alphanumeric, max. 10 characters
line-hot-line-warm-line	Hot/Warm Line Type		Poss. Values: • Normal • Hot Line • Warm Line
line-ring-delay	Ringing Delay	Time before ringing starts for an alerting call.	Number, length: 5
forwarding-type	Forwarding Type	Forwarding Type	Poss. Values: • on busy • on no reply • unconditionally
locked-function-keys	Lock Key	Check box for locking the function key	Poss. values: true/ false
dss-sip-line-type	Line Type	Line Type	Poss. values: • normal • direct
dss-sip-line-action	Line Action	Line Action	Poss. Values: • Consultation • Transfer • No Action

Table 15-3

Possible Values of name for ModifyKeyset

Internal name	DLS display label	DLS description	Type
dss-sip-deflect	Deflect Alerting Call	active: Deflect Alerting Call by pressing key	Poss. values: true/ false

Table 15-4

Internal name	DLS display label	DLS description	Type
dss-sip-detect-timer	Call Pickup Detect Timer (sec)	Specifies how long group pickup is signaled by the key	Number
dss-sip-refuse	Allow Pickup to be refused	active: Allow Pickup to be refused by pressing key	Poss. values: true/ false
line-key-operating-mode	Line Key Operating Mode	Defines what should happen to a line (call) when a connection is established over another line. Call hold: The original call is put on hold. Release: The connection to the original call is cleared	Poss. Values: • Call hold • Release
originating-line-preference	Originating Line Preference	Defines the preferred line to be used for outgoing calls	Poss. Values: • Idle line preference • Primary line preference • Last line preference • No preference
line-registration-leds	Registration LEDs	Activates display when restarting the IP phone indicating whether the IP Device was registered successfully	Poss. values: true/ false
keyset-remote-forward-ind	Remote Forward Indication	Activates alerting on a line key when call forwarding is active for its destination	Poss. values: true/ false
keyset-reservation-timer	Reservation Timer	Time in seconds indicating how long a line reservation can be maintained	Number

Table 15-4

Internal name	DLS display label	DLS description	Type
line-rollover-type	Rollover Type	Type of alerting when busy	Poss. Values: • No ring • Alert Ring • Standard • Alerting
line-rollover-volume	Rollover Ring Volume	Volume of alerting when busy	Number
terminating-line-preference	Terminating Line Preference	Defines the preferred line to be used for incoming calls	Poss. Values: • Ringing line preference • Calling line preference with prime line preferred • Ringing line preference • Ringing line preference with prime line preferred • No preference
keyset-use-focus	Show Focus	Activates display showing which line is currently active (line has the focus)	Poss. values: true/ false
line-button-mode	Line Button Mode	Mode of line button	Poss. Values: • Single button • Preselection
line-preselection-timer	Line Preselection Timer (sec)	Time in seconds before Line Preselection is cancelled	Number
line-preview-period	Line Key Preview Period	Time in seconds before preview mode is cancelled	Number
shift-key-timeout	Shift Key Timeout	Time in seconds before shift mode is cancelled	Number
stimulus-dtmf-sequence	DTMF Sequence	DTMF Sequence	Alphanumeric, max. 255 chars

Table 15-4

Internal name	DLS display label	DLS description	Type
blf-audible	BLF audible alert	BLF audible alert	Poss. values: true/ false
blf-popup	BLF popup alert	BLF popup alert	Poss. values: true/ false
fpk-app-name	Application name	Application name	Alphanumeric, max. 48 chars
send-url-address	Web server address	Host name, domain name, or IP address of web server	Alphanumeric, max. 255 chars
send-url-protocol	Protocol	Protocol	Poss. values: 0: HTTP 1: HTTPS
send-url-port	Port	Port number of web server	Number
send-url-path	Path	Directory path and name of the program or web page. Examples: "servlet/IppGeneric-Servlet" or "webpage/checkin.html"	Alphanumeric, max. 255 chars
send-url-query	Parameters	Parameters (e.g.: parameter1=value1&amp;parameter2=value2)	Alphanumeric, max. 255 chars
send-url-method	HTTP method	HTTP method	Poss. values: 0: Get 1: Post
send-url-user-id	Web server user ID	User identity known by web server	Alphanumeric, max. 48 chars
send-url-passwd	Web server password	Password known by web server	Alphanumeric, max. 48 chars

Table 15-4

Internal name	DLS display label	DLS description	Type
key-functionality	Key functionality	Key functionality	Poss. Values: 0: Toggle call forwarding 1: Unspecified call forwarding 2: Unspecified

Table 15-4

15.11 Copy Macro for P&P and Templates

This function enables copying field values to another field automatically. For example, copy registration data for HFA phones to standby configuration by means of a macro command.

To copy a value or parts of it from one field to another, provides a template containing the macro command.

As an example, you can define a template to use the registration subscriber number of the main gateway to be copied to the registration subscriber number (standby): In order to do this, enter the following string in the **Standby Reg** field: `%reg-number%`

When the template is applied, the macro command will be executed and the result will be written to the field and sent to the device.

It is also possible to enter a macro command for a virtual device directly. It will be executed when P&P is applied. For an already registered device, the macro command will be executed immediately via a job.

15.11.1 Macro Command Syntax

The syntax of the macro command

```
%<item name >[begin index, end index]%
```

consists of the following parts:

- `%` marks the begin and the end of the macro command.
- `item name` names the field whose values are to be copied.
- `begin index` to `end index` (optional): only parts of the value are copied. `$` represents the last index.

  Example: Macro command `%e164%` copies the whole E.164 number; `%e164[1,5]%` copies the first 5 digits of the E.164; `%e164[$-4,$]%` copies the last 5 digits of the E.164.

15.11.2 Available <item name>s

The feature is available for dedicated fields only. The source item `<item name>` has to be part of the same screen as the destination item.

The following fields are supported:

Screen	Field	Item name
IP Devices > IP Phone Configuration > Gateway / Server	E.164	`e164`
	Reg address	`reg-addr`
	Registration Subscriber Number	`reg-number`
	Gatekeeper ID	`reg-id`
	H.235 Security Mode	`h235securitymode`
IP Devices > IP Client Configuration > Gateway / Server	System Type	`hfa-pbx-type`
	E.164	`e164`
	Reg address	`reg-addr`
	Registration Subscriber Number	`registration-phone-no`
	Gatekeeper ID	`gatekeeper-id`
	H.235 Security Mode	`h235securitymode`

Table 15-5

15.11.3 Available Destination fields

Screen	Field
IP Devices > IP Phone Configuration > Gateway / Server	E.164
IP Devices > IP Phone Configuration > Gateway / Server > Gateway Tab	Registration Subscriber Number
IP Devices > IP Phone Configuration > Gateway / Server > Gateway (Standby) Tab	Reg address
	Registration Subscriber Number
	Gatekeeper ID
	H.235 Security Mode

Table 15-6

Screen	Field
IP Devices > IP Phone Configuration > Gateway / Server > SIP Terminal Settings Tab	Display ID
	Display ID (Unicode characters)
	Terminal Name
IP Devices > IP Phone Configuration > Miscellaneous > Display/Phone Settings Tab	Handset Name
IP Devices > IP Phone Configuration > IP Routing > DNS Server Tab	Terminal Hostname
IP Devices > IP Client Configuration > Gateway / Server	E.164
IP Devices > IP Client Configuration > Gateway / Server > Gateway Tab	Registration Subscriber Number
IP Devices > IP Client Configuration > Gateway / Server > Gateway (Standby) Tab	System Type
	Reg address
	Registration Subscriber Number
	Gatekeeper ID
	H.235 Security Mode
IP Devices > IP Client Configuration > Gateway / Server > SIP Connection Tab	Terminal Name

Table 15-6

16 Administration Scenarios

This chapter contains the following administration scenarios:

- Workpoint Reinstallation with HiPath 4000
- Workpoint Reinstallation with HiPath 3000
- Configuring a Gateway in DLS
- Replacing an IP Device
- Replacing an Old Workpoint (TDM) with a New One (IP)
- Replacing HFA with SIP Software and Vice Versa with Identical Device IDs
- Configuring an IP Client 130 in the DLS
- Changing the IP Address and/or Port Number of the DLS
- Using an EWS with DLS in a Customer Network Without Permanent DLS
- Operating the DLS via the Program Interface (DlsAPI)
- Security: Pre-Shared Secret for SRTP Security Domains
- Security: Administering Certificates
- Configuring and Administrating Mobility
- Data Structures for DLS-hosted XML applications
- Use Multi-Tenancy

> The sequence descriptions provided here are intended as examples. The actual sequence may vary from the description, depending on the particular DLS configuration, the servers or IP Devices used, and the ongoing development of the DLS.

16.1 Workpoint Reinstallation with HiPath 4000

Requirements

- A working DLS infrastructure (such as, DHCP and DNS server).
- A HiPath 4000 Assistant with deactivated access block[1]configured in the DLS (see Section 12.1.4).

Performing reinstallation

1. Configure the stations in the system, for example, with the help of HiPath 4000 Manager or AMOs. For more information refer to the relevant documentation.
2. Select the **Element Manager** > **Element Manager Configuration** > **"HiPath 4000 Assistant" Tab** area.
3. Click **Synchronize**. This transmits all data for the stations configured in the system to the DLS.
4. Click the area **IP Device Management** > **IP Device Configuration**.
   Click **Search** to find all configured workpoints. The first of the workpoints found is displayed in **Object** view.
5. Change to **Table** view and sort the table by **E.164**.
6. Select the desired, pre-configured virtual device from the table. The **device ID** generated by the DLS for a virtual device is prefixed by "@".
7. Enter the **device ID** of the workpoint.
8. Click **Save**.
9. Connect the workpoint.

This completes reinstallation.

[1] To deactivate the access block, select **Access Management** > **Password Management** > **System Password Management** > Password **uas_read** in the HiPath 4000 Assistant and deactivate the option **Block password**. Enter the password and save your changes.

16.2 Workpoint Reinstallation with HiPath 3000

Requirements

- A working DLS infrastructure (such as DHCP- and DNS server).
- A HiPath 3000/5000 configured in the DLS (see Section 12.1.5).

Performing reinstallation

1. Configure the stations in the system. For more information refer to the relevant documentation.
2. Select the **IP Devices** > **IP Device Management** > **IP Device Configuration** area to create an station, that is, a virtual device, in the DLS. Instead of a device ID, the virtual device receives a placeholder generated by the DLS beginning with "@".
3. Enter the **E.164** of the new station.
4. Click the **Element Manager** > **Element Manager Configuration** > **"HiPath 3000/5000" Tab** area.
5. Click **Synchronize**. If the E.164 already exists in one of the configured HiPath 3000/5000 DB Feature Servers, the relevant gatekeeper address is added to the data record.
6. Enter the device ID of the workpoint in **IP Devices** > **IP Device Management** > **IP Device Configuration**.
7. Click **Save**.
8. Connect the workpoint.

This completes reinstallation.

16.3 Configuring a Gateway in DLS

Requirements

- A working DLS infrastructure.
- A configured gateway (HG1500, HG3530, HG3550, HG3570, HG3575 or RG2700).

16.3.1 Adding Gateways

1. Click the **Gateways** > **Gateway Configuration** area.
2. Click **New**.
3. Select the gateway you want under Gateway Type. Once you have made this selection, all unnecessary fields are deactivated (dimmed).

   If a gateway of the same category is already configured, you can copy the data from this and modify it to meet your requirements. Find the gateway you want to copy data from and select **New**.

4. If necessary, add a description of this gateway under **Remark**.
5. Enter the necessary data in the "Gateway Connection" Tab. The following is a list of entries required for the various gateway types.
   - **HG1500** (for HiPath 3000/5000, direct connection), **RG2700**

     Gateway IP Address: IP address of the gateway.

     Account: Gateway access ID (as configured in the gateway, default ID: **31994**).

     Password: Password for accessing the gateway (configured on the gateway as described above for the account).
   - **HG3550** (for HiPath 4000, connection via the HiPath 4000 Assistant)

     Gateway IP Address: IP address of the gateway.

     Gateway Proxy IP Address: IP address of the relevant HiPath 4000 Assistant.

     Gateway Proxy Port: 443.

     Account: Access ID for HiPath 4000 Assistant (as configured on the Assistant). You must use an ID in the HiPath 4000 Assistant that contains user rights for HG3550Mgr. For information on creating IDs and assigning rights with this tool, refer to "Access Management" in the HiPath 4000 Assistant online help.

     Password: Password for accessing HiPath 4000 Assistant (configured on HiPath 4000 Assistant as described above for the account).

- **HG3530**, **HG3570**, **HG3575** (for HiPath 4000, connection via SNMP proxy - an integral part of the DLS server)

  Gateway IP Address: IP address of the gateway.

  SNMP Community: Community string (for authenticating SNMP communication to the gateway). Default community string: **nbcs**.
  The community string must be set to the same value as the relevant gateway in HiPath 4000 (AMO HFAB: TYP=SNMP, parameter: CS2).

> During DLS installation, the SNMP proxy is also installed at the same time and automatically started as a local service on the DLS server PC. You can stop and start the SNMP proxy manually on this PC.
>
> To access this service, select: Start > Settings > Control Panel > Administrative Tools > Services > DeploymentServiceSNMPProxy

6. Click **Save** to apply the entries.

16.3.2 Release Information (QDC and VoIP Security)

QoS Data Collection

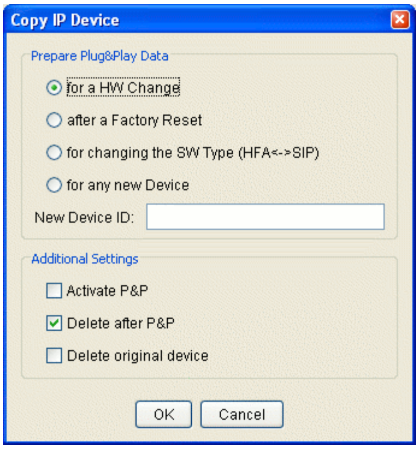
- HG1500: V5.0
- HG3550: V2.0
- HG3530: V2.0
- HG3570: V2.0
- HG3575: V2.0
- RG2700: V1.0

VoIP Security

- HG1500: V6.0
- HG3550: V3.0 (may still "officially" be V2.0)
- HG3530: V3.0 (may still "officially" be V2.0)
- HG3570: No VoIP security
- HG3575: No VoIP security
- RG2700: No VoIP security

16.4 Replacing an IP Device

1. Click the **IP Device Management** > **IP Device Configuration** area. Click **Action** in the menu bar and select **Copy IP Device**.
2. The following dialog window opens:



Copy IP Device

Prepare Plug&Play Data

● for a HW Change

○ after a Factory Reset

○ for changing the SW Type (HFA<->SIP)

○ for any new Device

New Device ID:

Additional Settings

□ Activate P&P

☑ Delete after P&P

□ Delete original device

OK Cancel

Select **for a HW Change** under **Prepare Plug&Play Data.**

If you wish to leave configuration data as it is, select **Activate P&P**. The data record is then released for transfer to the workpoint.

3. Disconnect the defective workpoint and connect the replacement workpoint.
4. If full plug&play is supported for the workpoint, the replacement workpoint is automatically registered and configured (as in the case of reinstallation, Section 16.1 or Section 16.2).

   If plug&play is not supported, workpoint registration must be performed manually in the DLS. Registration depends on the presence of a DHCP server:

   - If a **DHCP server is not present**:

     The following data must be configured on the workpoint in the *Configuration* menu:

     1. DHCP must be set to *off*.
     2. The IP address of the workpoint must be entered.
     3. The network mask of the workpoint subnet must be entered.
     4. The IP address of the default router must be entered.
     5. The *Fully qualified Subscriber Number* must be entered.

     After saving changes and restarting the IP phone, DLS can be used to perform a scan to register the IP phone in the DLS (see Section 7.4.4, "Scan IP Devices"). The DLS address must also be sent when performing scanning.

   - If a **DHCP server is present**:

If the DHCP does not send DLS address data to the workpoint, start the workpoint scan. In the scanning dialog box, activate **Register IP Devices** and **New IP Devices from Scan Results** (see Section 7.4.4, "Scan IP Devices") to register the new workpoint in the DLS.

If the DLS address data is sent automatically from the DHCP to the workpoint, registration in the DLS is automatic.

For information on configuring a DHCP server to transfer DLS access data to the workpoints, see Section 4.10.4.3, "Configuring the DHCP Server for DLS".

> ⓘ You should not delete the old workpoint data from the DLS database until after the new workpoint is functioning.

This completes replacement.

16.5 Replacing an Old Workpoint (TDM) with a New One (IP)

Requirements

- A working DLS infrastructure (such as CLA, DHCP, DNS and FTP servers).

Performing the replacement

1. Reconfigure the stations in the system by deleting them and then recreating them, for example, with the help of the HiPath 4000 Manager or AMOs. For more information refer to the relevant documentation.
2. For the remaining procedure, follow the instructions for the reinstallation of a workpoint (see Section 16.1, "Workpoint Reinstallation with HiPath 4000").

This completes replacement.

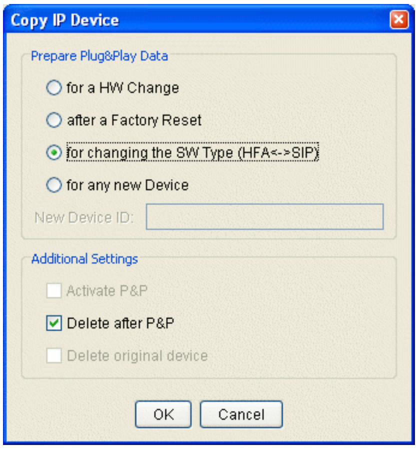
16.6 Replacing HFA with SIP Software and Vice Versa with Identical Device IDs

Requirements

- A working DLS infrastructure (such as CLA, DHCP, DNS and FTP servers).

16.6.1 Replacing HFA with SIP Software

1. Prepare the SIP software in the DLS (see Section 15.3, "Registering Workpoint Software and Files").
2. Click **Action** in the menu bar and select **Copy IP Device**.
3. The following dialog window opens:



Copy IP Device

Prepare Plug&Play Data

○ for a HW Change
○ after a Factory Reset
● for changing the SW Type (HFA<->SIP)
○ for any new Device

New Device ID:

Additional Settings

□ Activate P&P
☑ Delete after P&P
□ Delete original device

Select **changing the SW Type (HFA<->SIP)** under **Prepare Plug&Play Data**.
If you wish to leave the configuration data unchanged, select **Activate P&P**. The data record is then released for transfer to the workpoint.

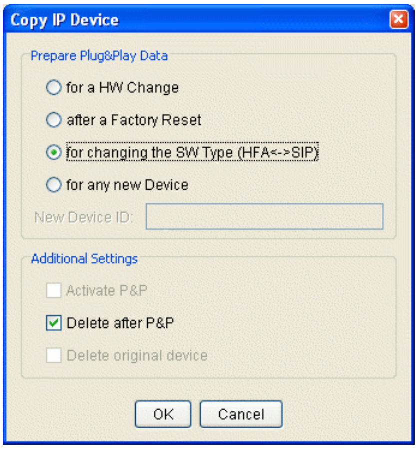
4. Define the required registration data. This configuration is dependant on the SIP server used. In the case of OpenScape Voice, this is for a minimum configuration:
IP Devices > **IP Phone Configuration** > **Gateway/Server**
   – **"Gateway (HFA) / SIP Server" Tab**:
   Reg-Addr., **Reg-Port**.
   – **"SIP Registering 1" Tab**:
   SIP Routing, SIP Registrar Addr., **SIP Registrar Port**, **SIP Phone Port**, **RTP Base Port**.

   We recommend managing configuration data using templates. For more information, see Section 15.4.1, "Creating a Template Manually".
   If necessary, you can also transfer registration data via synchronization with the system. For more information, see Section 12.1, "Element Manager Configuration".

5. Start software deployment (see Section 15.6.1, "Manual Deployment").
   The workpoint is restarted once the software is loaded to the phone. This completes the software replacement operation.

16.6.2 Replacing SIP with HFA Software

1. Prepare the HFA software in the DLS (see Section 15.3, "Registering Workpoint Software and Files").
2. Click **Action** In the menu bar and select **Copy IP Device**.
3. The following dialog window opens:



Copy IP Device

Prepare Plug&Play Data

○ for a HW Change
○ after a Factory Reset
● for changing the SW Type (HFA<->SIP)
○ for any new Device
New Device ID:

Additional Settings

□ Activate P&P
☑ Delete after P&P
□ Delete original device

   Select **changing the SW Type (HFA<->SIP)** under **Prepare Plug&Play Data**.
   If you wish to leave the configuration data unchanged, select **Activate P&P**. The data record is then released for transfer to the workpoint.

4. Define the access data for the gateway.
   You can also use templates to manage configuration data. For more information, see Section 15.4.1, "Creating a Template Manually".
   If necessary, you can also transfer access data via synchronization with the system. For more information, see Section 12.1, "Element Manager Configuration".
5. Start software deployment (see Section 15.6.1, "Manual Deployment").
   The workpoint is restarted once the software is loaded to the phone. This completes the software replacement operation.

16.7 Configuring an IP Client 130 in the DLS

The following describes how to configure an optiClient 130 V5.0 as a HFA client in a HiPath 4000 environment.

Requirements

- A live DLS infrastructure (including existing connection to the HiPath 4000).

Procedure

1. Creating Templates
2. Settings at the optiClient 130

16.7.1 Creating Templates

Template: Gateway/Server

The data for system type (including standby), program update, telephone type, and licensing are entered in this template.

1. Click the **IP Devices** > **IP Client Configuration** > **Gateway/Server** > **"Gateway" Tab** area.
2. In the view bar (see Section 5.4.2.3, "View Bar"), select **Template**..
3. Select **HiPath 4000** in the **System Type** list.
4. Switch to the **"Gateway (Standby)" Tab.**
5. Select **No standby system** in the **System Type** list.
6. Switch to the **"SW Deployment" Tab**.
7. Select the **DLS Deployment** check box and enter the **Directory** and the **SW Update Mode**.
   The meaning of the entries in **SW Update Mode** are as follows:
   – **Start**: the system checks for a new version when starting optiClient 130.
   – **Interval**: the system checks for a new version every X minutes based on the value set under **Update Mechanism Interval.**
8. Switch to the **"HFA Settings" Tab**.
9. Select the telephone (including add-on devices) used to represent the optiClient 130 from the **Device Phonetype** list. For example: **Device Phonetype:** optiPoint 420 standard, **Device Modules Type:** optiPoint 420 Key Module and **Device Modules Count:** 2.
10. Switch to the **"Licenses" Tab**.

11. Enter the IP address and the port number of the license server under **Server** and **Port** in the **HFA License** tab.
12. Click **Save** and define the name for the template, for example, **oC130 Gateway/DLS HP4000**.
13. Click the **IP Devices** > **IP Client Configuration** > **Dialing Properties** > **"HFA Dialing Properties" Tab** area.
14. Select **Template** in the view bar and set the template name.
15. Enter the necessary data here for the main network access, for example, **49** for the local country code.
16. Click **Save** and define the name for the template, for example, **oC130 dialing properties HP4000**.
17. Create more templates as needed, for example, if an LDAP server is available, the relevant data is in the **LDAP** section.

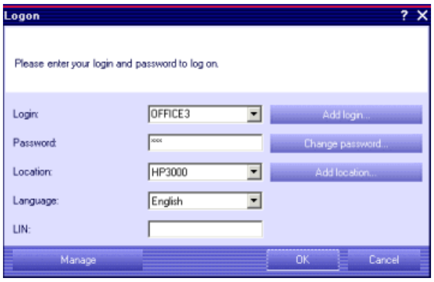
16.7.2 Creating a Profile from the Template

1. Click the **Profile Management** > **Device Profile** area.
2. Click **New** in the view bar to create a new profile.
3. Enter a suitable name for your profile, such as, **oC 130 device** in the **Name** field and enter a brief description in the **Description** field.
4. If you wish the profile to be the default profile for a particular **Location** (see Section 6.2.2, "Location"), activate **Default Profile**.
5. Group the templates that you wish to use to form the profile under **Profile Management** > **Device Profile** > **"Templates" Tab**. To do this, click □ for each template you wish to add and then select a template from the choice list.
6. Enter the correct **Device Type**, **SW Type**, and **SW Version** under **Profile Management** > **Device Profile** > **"Templates" Tab**.
7. Click Save to save the profile.

16.7.3 Settings at the optiClient 130

Certain additional data must be entered at the optiClient 130 so that the optiClient 130 can operate with the DLS.

Login (same as for the optiClient 130 extension), Password, and Location:

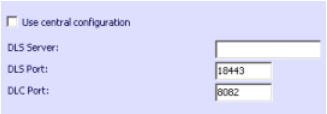


Logon

Please enter your login and password to log on.

Login: OFFICE3
Password: xxx
Location: HP3000
Language: English
LIN:

Under **Settings...** the data for the DLS server:



☐ Use central configuration

DLS Server:
DLS Port: 18443
DLC Port: 8082

For more information on configuring the optiClient 130, refer to the online help or the optiClient 130 Administration Manual.

16.7.4 OptiClient in Call Centers

In call centers, it is necessary that optiClient users are enabled to work with their own call number. With every first login at a specific PC, P&P is executed. For this purpose, the Activate Plug&Play flag must be set.

1. Configure the optiClient for the first time, using the E.164 relevant to the user (e. g. 497224711), and the corresponding profile.

   Please ensure that the DLS address is defined in the optiClient, and that the data is stored in the home drive within the network.

2. Now create a corresponding participant, that is, a virtual device, in the DLS. For this purpose, select **IP Devices** > **IP Device Management** > **IP Device Configuration** und click on the action button **New**.

3. Enter the E.164 number.

4. Enter the E.164 number once again, as **Device ID**, and end with a ’.’ (dot; e. g. ’497224711.’).

5. Click on **Save**.

16.8 Changing the IP Address and/or Port Number of the DLS

If you need to change the address data (IP address and port number) of the DLS while it is running, for example, because you want to move it to an alternative computer, you must perform all changes in a specific sequence.

The current DLS installation is called "old" and the DLS with the modified data is called "new" in the following.

1. First put the new DLS into operation. Do this by installing all necessary components and starting the new DLS.

   The new DLS is now already running with a new IP address and port number, but the workpoints are not yet using it.

2. You must change the DLS IP address data in the workpoints so that the workpoints can contact the new DLS. How you change this data depends on how the workpoints are supplied with the DLS IP address and port number.

   - With DHCP (full plug&play):

     Change the data in the DHCP server's "vendor class" (see Section 4.10.4.3).

   - Without DHCP (limited plug&play):

     a) In the DLS, select the **IP Devices** > **IP Device Management** > **IP Device Configuration** > **"DLS Connectivity" Tab** area with all available workpoints (see also Section 15.1, "First Steps: Changing IP Device Parameters").

     b) Enter the IP address data of the new DLS under **DLS Server Address** and **DLS Port** and apply it to all workpoints (see Section 5.4.2.4, "Multiple selection and data transfer in Table view").

     c) Send the DLS IP address data to the workpoints by clicking **Save**.

3. Restart all relevant workpoints (**IP Devices** > **IP Device Interaction** > **Reset IP Devices**).

   > Note that the workpoints will communicate only with the new DLS after a restart. This means that there is no message indicating whether this action was successfully executed for the old DLS.

   The workpoints register with the new DLS.

4. Deactivate the old DLS (to uninstall the DLS, see Section 4.12, "Uninstalling the Deployment Service").

16.9 Using an EWS with DLS in a Customer Network Without Permanent DLS

Requirements

- DLS CV45 and higher.
- An FTP server installed on the TAP. For information on installation, see Section 4.10.1, "FTP Server".
- The workpoint software to be deployed must be located on the EWS and registered in the DLS (see Section 6.2.4, "FTP Server Configuration", Section 6.2.5, "HTTPS Server Configuration" or Section 6.2.6, "Network Drive Configuration").
- The EWS must be connected to the customer LAN and assigned a free IP address from the customer LAN. The IP address can be modified using the IP changer.

Restriction

DHCP can be activated or deactivated at the workpoint (*DHCP=ON* or *DHCP=OFF*). However, no DLS info may be sent from the DHCP to the workpoint. "Vendor Class" must not be configured in the DHCP as described under Section 4.10.4.3. If the workpoint has already received the DLS info from the DHCP, this value can only be reset with a *Factory Reset*.

16.9.1 Installation and Initial Configuration of DLS on the EWS

1. Install Java 2 Runtime Environment 1.4.2.
2. Install the current version of DLS.
3. Perform initial configuration on the DLS (see Section 4.8, "Initial Configuration"). You must configure the data for the FTP server(s) here.
4. The IP address range containing the workpoint must be configured before the workpoint can be transferred from the customer network to the DLS (**IP Devices** > **IP Device Interaction**> **Scan IP Devices** > **"IP Ranges" Tab**).

   In addition, the current IP address of the EWS must be entered as the **DLS Address** (the current IP address is displayed, for example, by entering *ipconfig/all* in the DOS shell). The **Send DLS Address** option must be activated (**IP Devices** > **IP Device Interaction**> **Scan IP Devices** > **"Configuration" Tab**). This IP address range is then scanned with **Scan Workpoints**.

16.9.2 Manipulating the DLS Database for Using the TAP at Different Customer Facilities

The database used by the DLS must be modified to facilitate working with multiple databases on the TAP.

16.9.2.1 Configuring a Database at a new Customer Facility

1. If the DLS database already contains data, save it on the EWS. See Section 15.8.1, "Automatic Data Backups".
2. Create a new database on the EWS. See Section 15.8.2.4, "Resetting the DLS Database".

16.9.2.2 Database Change Between Customers A and B

1. Save the currently active database associated with **customer A** on the EWS. See Section 15.8.1, "Automatic Data Backups".
2. Restore the saved DLS database associated with **customer B**. See Section 15.8.1, "Automatic Data Backups".

16.10 Operating the DLS via the Program Interface (DlsAPI)

In addition to standard GUI-based operation, the DLS can also be operated by external applications over a web service interface. An account with authorization to access the Dls API must first be configured for this (see Section 6.1, "Account Management").

DLS V2 provides both DlsAPI v100 (as released with DLS V1) and new methods as part of DlsAPI v200. While DlsAPI v100 methods support IP Phones only, DlsAPI v200 methods also support IP Clients and IP Gateways.

16.10.1 DLS API Web Service Interface

The DLS API is included in the DLS installation and is stored in the following directory:

`<DLS installation directory>\Programs\DeploymentService\api`

The following data is included:

1. `dlsapiv100.wsdl`
   Describes the DlsAPI v100 in WSDL (Web Services Description Language).
2. `dlsapiv100.jar`
   Generated by WSDL2JAVA. This JAR file contains Client Stubs and the Service Locator and may be used by JAVA clients as an interface to the DlsAPI v100.
3. `dlsapiv200.wsdl`
   Describes the DlsAPI v200 in WSDL (Web Services Description Language).
4. `dlsapiv200.jar`
   Generated by WSDL2JAVA. This JAR file contains Client Stubs and the Service Locator and may be used by JAVA clients as an interface to the DlsAPI v200.
5. `doc`
   This subdirectory contains a description of the DLS API interface in Javadoc format.

The WSDL descriptions are stored on the DLS server at the following URLs:

```
https://<DLS server>:10444/DeploymentService/services/
DlsAPIv100?wsdl
```

```
https://<DLS-Server>:10444/DeploymentService/services/
DlsAPIv200?wsdl
```

Online documentation for the DLS API is stored at the following URL:

`https://<DLS server>:10443/DeploymentService/dlsapidoc`

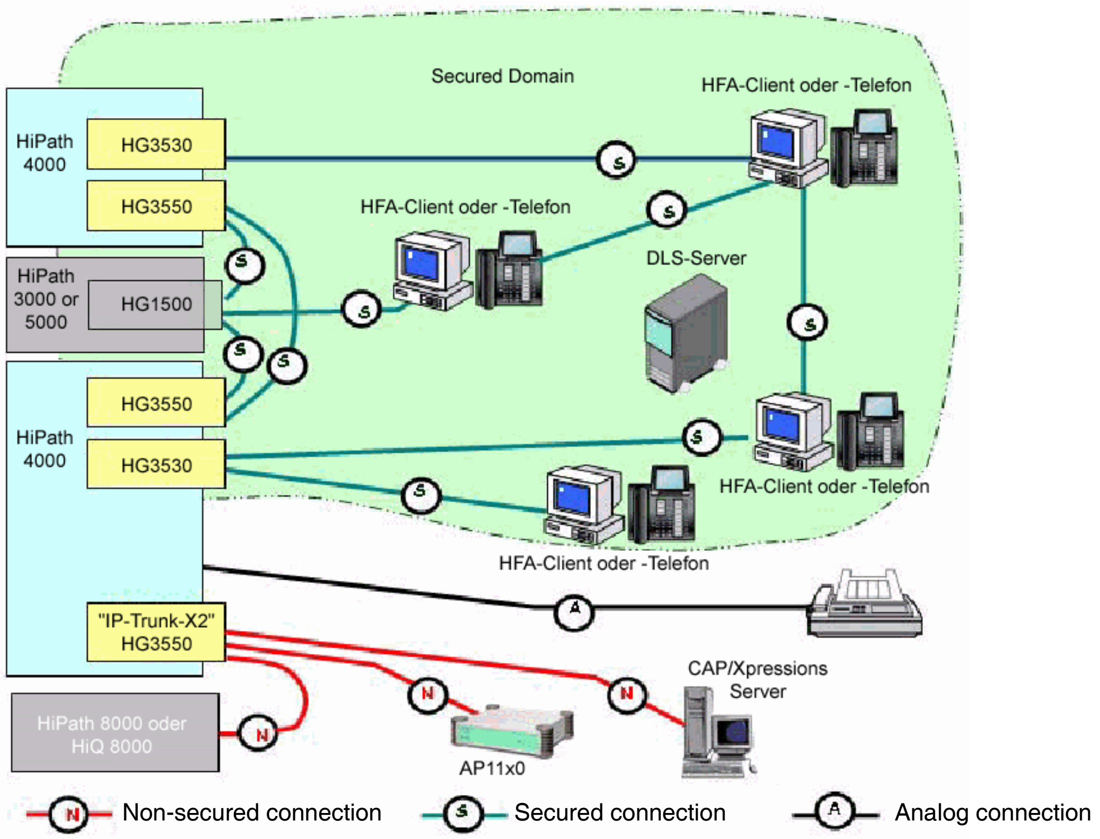
> If the DLS HTTP port is not deactivated, it can be used as an alternative to the HTTPS port. In this case, the URLs will change:
> `https://<DLS server>:10443/DeploymentService/...`

A PHP test script is available for the DLS API. Among other things, this enables you to monitor SOAP communication, query particular IP phones in the DLS database, and modify configuration parameters for a selected IP phone. For more information, see the DLS ReleaseNote.

16.11 Security: Pre-Shared Secret for SRTP Security Domains

This section describes initial configuration of a pre-shared secret (PSS) for an SRTP security domain.

The following figure shows an overview of an SRTP security domain (green background) and the components involved.



A PSS (Pre-Shared Secret) is used by gateways and workpoints to encrypt and transmit payload and signaling data in HiPath 3000 V6.0 or HiPath 4000 V3.0 and between two platforms via the HG3550 gateway.

The DLS is the central tool for creating and distributing the PSS during this procedure. As an administrator, the DLS enables you to easily distribute keys. You do not have to worry about dependencies between gateways and workpoints because the DLS performs various tests before automatically distributing keys to all relevant workpoints.

> Pre-shared secrets can only be administered via the DLS and not via the deployment tool, the WBM or directly at a telephone.

16.11.1 Initially Configuring a PSS

Requirements

- The DLS must be permanently available.
- The gateway (HG3530 or HG1500) must support PSS security encryption. For more information on gateway configuration, see Section 9.1, "Gateway Configuration".
- The workpoints connected to the gateway in question must support PSS security encryption.

Preparation

Before starting key distribution, configure the relevant workpoints as follows:

1. Select **IP Devices** > **IP Phone Configuration** (or **IP Client Configuration**) > **Gateway/Server** > **"Gateway (HFA) / SIP Server" Tab** (if necessary, also **"Gateway (Standby)" Tab**).
2. If you have not already done so, set the **H.235 Security Mode** to **Full** and enter the **subscriber password**.
3. If you have not already done so, enter the Gateway ID in the relevant workpoints.

> The Gateway ID corresponds to the GLOBID parameter in the AMO HFAB for HiPath 4000 resp. der H.323 ID with HiPath 3000.

Check that the gateway is correctly configured for encryption. You can do this as follows:

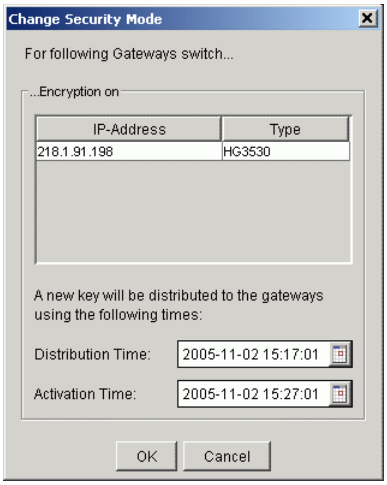
1. Click the **Gateways** > **Gateway Configuration** area.
2. Select Read Gateway Data for the gateway in question.
Configuration of VoIP Security Data enabled should be active.
3. Click the **Voice over IP Security V1** > **Key Distribution** area. The gateway should be entered in the **Distribute to** list. **Encryption off** should be entered in the **CurrentSecurity Mode** column, and **yes** should be entered in the **License** column.

> The gateway is unable to send any license information if **unknown** is entered in the **License** column. In this case the security mode is still activated for the gateway.

Distributing a key

1. Click the **Voice over IP Security V1** > **Key Distribution** area.
2. In the **Distribute to** list, select the gateway(s) for encrypted communication in an SRTP security domain via PSS (for more information on making selections, see Section 5.4.2.4, "Multiple selection and data transfer in Table view").

3. Click **ChangeSecurity Mode**.



Change Security Mode

For following Gateways switch...

...Encryption on

IP-Address	Type
218.1.91.198	HG3530

A new key will be distributed to the gateways using the following times:

Distribution Time: 2005-11-02 15:17:01

Activation Time: 2005-11-02 15:27:01

This dialog displays the IP address and type of the gateway(s) you selected.

4. If necessary, change the **Distribution Time** (default: current time + 10 minutes) and the **Activation Time** (default/minimum: distribution time + 10 minutes).
 For information on the calendar, see Section 5.4.2.4, "Time field with calendar button".

> The period between the last activation and the next distribution must be at least 30 minutes. This means that there must be at least forty minutes between two distributions.

5. Click **OK**.
This creates a PSS. The PSS is then distributed to the gateway(s) and the connected workpoints and activated at the time specified in step 4.

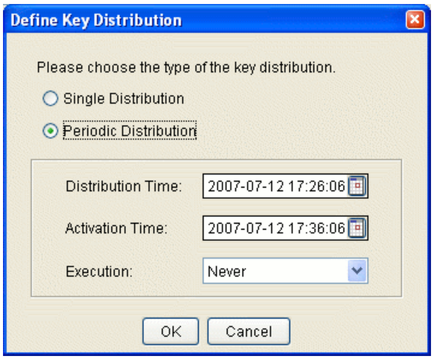
6. In **Single Distribution**, select **Job ID** to view this job in the **Job Coordination** > **Job Control** area.
As PSS jobs are handled like all other deployment jobs, these jobs also appear in the area **Job Control**.
PSS job IDs (a job for every gateway and workpoint) have the following syntax: **PSS**[job ID].

> Before distribution, the system checks gateway availability. The PSS is not distributed if a gateway cannot be reached. In this case, the ⚠ icon is displayed next to the Distribution Time field. A ToolTip appears if you hold your cursor over this icon. For information on other icons, see Section 5.4.2.4, "Icons beside entry fields".

16.11.2 Distributing a PSS

To further increase security, you can configure a PSS for automatic distribution after a preset time. In this scenario, a PSS is distributed to all gateways and workpoints with an activated security mode.

1. Click the **Voice over IP Security V1** > **Key Distribution** area.
2. Click **Key Distribution** and select **Periodic Distribution**.



Define Key Distribution

Please choose the type of the key distribution.

○ Single Distribution

● Periodic Distribution

Distribution Time: 2007-07-12 17:26:06

Activation Time: 2007-07-12 17:36:06

Execution: Never

Now edit the **Distribution Time** and the **Activation Time** (for a calendar, see Section 5.4.2.4, "Time field with calendar button").

Select the period between two distributions in the **Execution** choice list (**Daily** to **Every 4 Weeks**).

3. Click **OK**.
   You have now created a job for the periodic distribution of a PSS.
4. In **Periodic Distribution**, select **Job ID** to view this job in the **Job Coordination** > **Job Control** area.

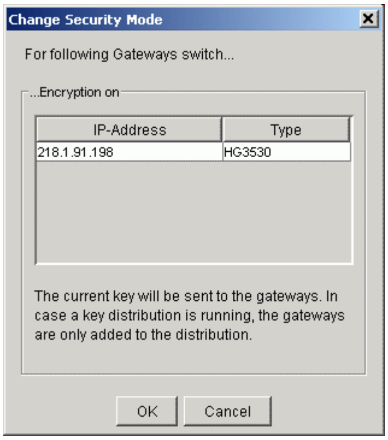
> You can also configure single distribution instead of periodic distribution. This procedure is similar to the one described above.

> For information on configuring an alarm in the event of incorrect key distribution, see Section 6.5, "Alarm Configuration".

16.11.3 Changing Security Mode

PSS encryption is easy to activate and deactivate.

1. Click the **Voice over IP Security V1** > **Key Distribution** area.
2. Select the relevant gateway(s) in the **Distribute to** list (for information on making selections, see Section 5.4.2.4, "Multiple selection and data transfer in Table view").
3. Click **Change Security Mode**.
   Different dialogs are displayed depending on the current status of the gateways you have selected.
   If the security mode is deactivated for all gateways, the following dialog appears:



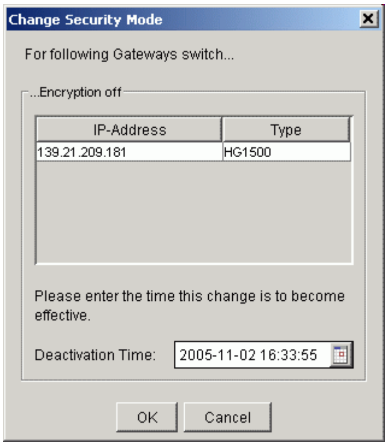
For following Gateways switch...

...Encryption on

IP-Address	Type
218.1.91.198	HG3530

The current key will be sent to the gateways. In case a key distribution is running, the gateways are only added to the distribution.

If the security mode is activated for all gateways, the following dialog appears:



For following Gateways switch...

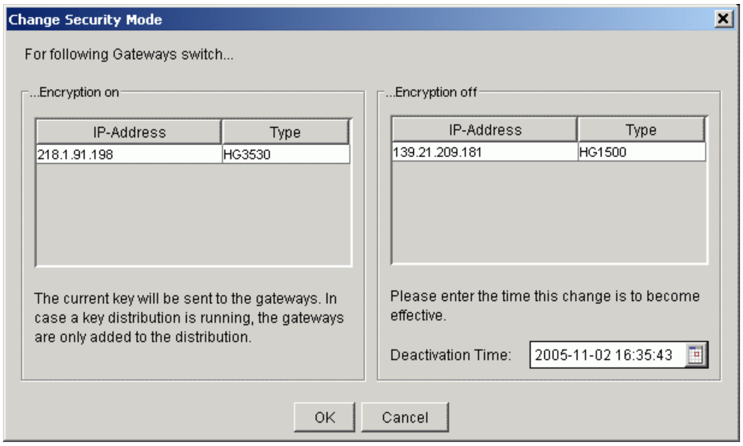
...Encryption off

IP-Address	Type
139.21.209.181	HG1500

Please enter the time this change is to become effective.

Deactivation Time: 2005-11-02 16:33:55

If the security mode is deactivated for some gateways and activated for others, the following dialog appears:



Change Security Mode

For following Gateways switch...

...Encryption on

IP-Address	Type
218.1.91.198	HG3530

The current key will be sent to the gateways. In case a key distribution is running, the gateways are only added to the distribution.

...Encryption off

IP-Address	Type
139.21.209.181	HG1500

Please enter the time this change is to become effective.

Deactivation Time: 2005-11-02 16:35:43

4. If you have selected gateways with activated security modes, you can change their deactivation time (for information on making selections, see Section 5.4.2.4, "Multiple selection and data transfer in Table view").

5. Click **OK**.

6. In **Distribute to**, select **Job ID of Change Security Mode** to view this job in the **Job Coordination** > **Job Control** area.

Current and, if applicable, future security mode statuses of different components are displayed in the following areas:

- For IP phones:
  IP Devices > **IP Phone Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE CA Certificates" Tab**
- For IP clients:
  IP Devices > **IP Client Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE CA Certificates" Tab**
- For gateways:
  IP Devices > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE CA Certificates" Tab**

16.11.4 Assign AC-Win in DLS

The following guideline describes the integration of an AC-Win as IP Client, exemplified for an HiPath 4000 V3 environment. Only key distribution is supported, not signalling and payload encryption.

A running DLS infrastructure with connection to the HiPath 4000 is required.

16.11.4.1 Settings at AC-Win

1. In ACConfig, for **Signalling and Payload Encryption**, change the value of **Type of Connection** to **TLS**.
2. Enable the **DLS Deployment Connection** and enter the IP address of the DLS.

16.11.4.2 Settings in DLS

1. Select **IP Devices** > **IP Device Interaction** > **Scan IP Devices** > **IP Ranges**. Enter the appropriate IP Addresses and start the scan. In the dialogue window appearing afterwards, select the actions: **Scan IP Devices**, **Register IP Devices**, **All IP Devices from Scan Results**, **Execute Autoconfiguration**, and **Execute AutoDeployment**.
2. Switch to **IP Devices** > **IP Device Interaction** > **Scan IP Devices** > **"Scan Results" Tab**. The scanned AC-Wins are found here.
3. Switch to **IP Devices** > **IP Client Configuration** > **Gateway/Server** > **"Gateway" Tab** and enter the **Registration Subscriber Number** and **Subscriber Password**.
4. The key distribution and the setting of the appropriate security mode will be performed automatically depending on the settings in **IP Devices** > **IP Client Configuration** > **VoIP Security V1** > **"HFA Key Distribution" Tab**.

16.12 Security: Administering Certificates

Certificates are used for secure authentication between the server and clients. A certificate is comparable to a digital ID card issued by an authorized body - the Certification Authority (CA).

You can administer certificates in the DLS for the following server/client configurations:

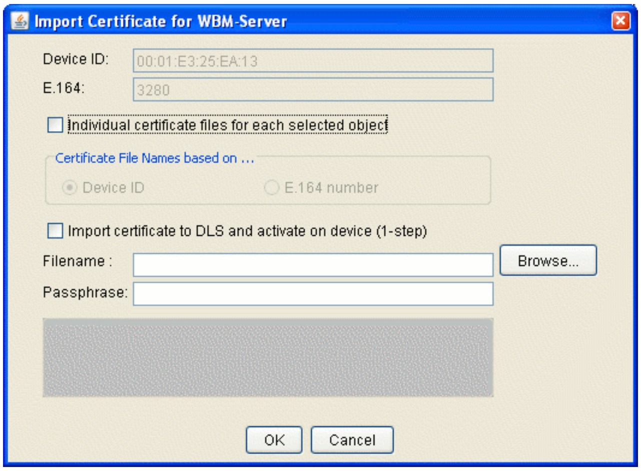
- **Server**: WBM server in the IP phone
  Client: Web browser for administering IP phones (see Section 16.12.1, "Importing WBM Server Certificates")
  For an interface description, see Section 7.1.7.4, ""WBM Server Certificate" Tab".
- **Server**: DLS
  Client: IP phone (see Section 16.12.2, "Importing Phone and RADIUS Certificates")
  For an interface description, see Section 7.1.23.2, ""Phone Certificate" Tab".
- **Server**: RADIUS server
  Client: IP phone (see Section 16.12.2, "Importing Phone and RADIUS Certificates")
  For an interface description, see Section 7.1.23.3, ""RADIUS Server CA Certificate 1" Tab" and Section 7.1.23.4, ""RADIUS Server CA Certificate 2" Tab".
- **Server**: SIP server
  Client: IP phone (see Section 16.12.3, "Importing SPE CA Certificates for IP Phones")
  For an interface description, see Section 7.1.21.1, ""SPE CA Certificates" Tab".
- **Server**: SIP server
  Client: IP client (see Section 16.12.4, "Importing SPE CA Certificates for IP Clients")
  For an interface description, see Section 7.2.12.1, ""SPE CA Certificates" Tab".
- **Server**: SIP Server
  Client: IP Gateway (see Section 16.12.5, "Importing SPE Certificates and SPE CA Certificates for IP Gateways")
  For an interface description, see Section 7.3.3.3, ""SPE CA Certificates" Tab".

> ⓘ Certificates can only be administered via DLS and not via the deployment tool, the WBM or directly at a telephone.

16.12.1 Importing WBM Server Certificates

1. Select **IP Devices** > **IP Phone Configuration** > **Security Settings** > **"WBM Server Certificate" Tab**. Search for and select the IP phone that you want to import a certificate for to enable communication with the WBM client (Web browser).

2. Click **Import Certificate**. An import dialog appears:



Import Certificate for WBM-Server

Device ID: 00:01:E3:25:EA:13

E.164: 3280

☐ Individual certificate files for each selected object

Certificate File Names based on ...

● Device ID ○ E.164 number

☐ Import certificate to DLS and activate on device (1-step)

Filename :

Passphrase:

This dialog contains the device ID of the IP phone you have selected.

3. In the **File name** entry field, enter the entire local path including the name of the certificate or click **Browse** to enter the path via the browser.
   The certificate should be in `PKCS#12` format.

4. Enter the key used to encrypt the PKCS#12 file you want to import in the **Passphrase** field.

5. Activate **Import certificate to DLS and activate on device (1-step)**, if the certificate should be activated immediately.

6. Click **OK** to import the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.

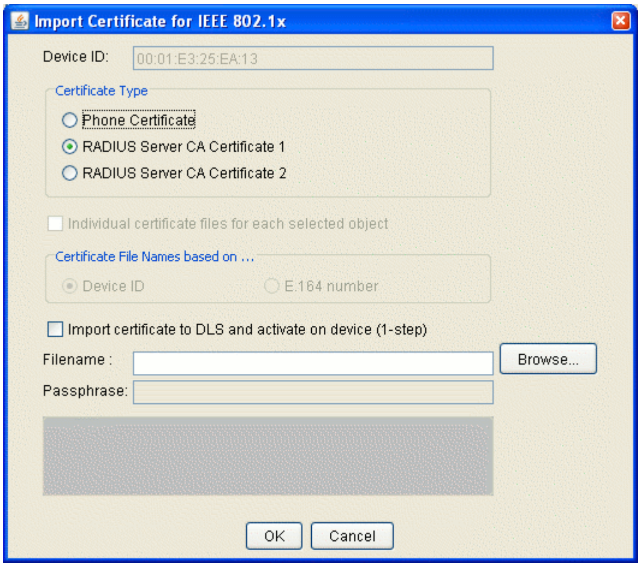
7. For activating the imported certificate, click **Activate** certificate and **Save** afterwards, if **Import certificate to DLS and activate on device (1-step)** is not activated.

16.12.2 Importing Phone and RADIUS Certificates

1. Click the **IP Devices** > **IP Phone Configuration** > **IEEE 802.1x** area.

2. Select the tab for the relevant certificate **"Phone Certificate" Tab, "RADIUS Server CA Certificate 1" Tab** or **"RADIUS Server CA Certificate 2" Tab**. Search for and select the IP phone that you want to import the certificate for.

3. Click **Import Certificate**. An import dialog appears:



Import Certificate for IEEE 802.1x

Device ID: 00:01:E3:25:EA:13

Certificate Type

○ Phone Certificate
● RADIUS Server CA Certificate 1
○ RADIUS Server CA Certificate 2

□ Individual certificate files for each selected object

Certificate File Names based on ...

● Device ID ○ E.164 number

□ Import certificate to DLS and activate on device (1-step)

Filename :

Passphrase:

This dialog contains the device ID of the IP phone you have selected.

4. Select the relevant certificate in the **Certificate Type** field. The option that corresponds to the tab is already selected.

5. Activate the check box
Individual certificate files for each selected object to import an individual certificate for every IP phone (for more information, see step 6).

6. In the **File Name** entry field (or **Directory** if the check box in step 5 is activated), enter the entire local path including the certificate name (without the name if the check box in step 5 is activated) or click **Browse** to enter the path via the browser.

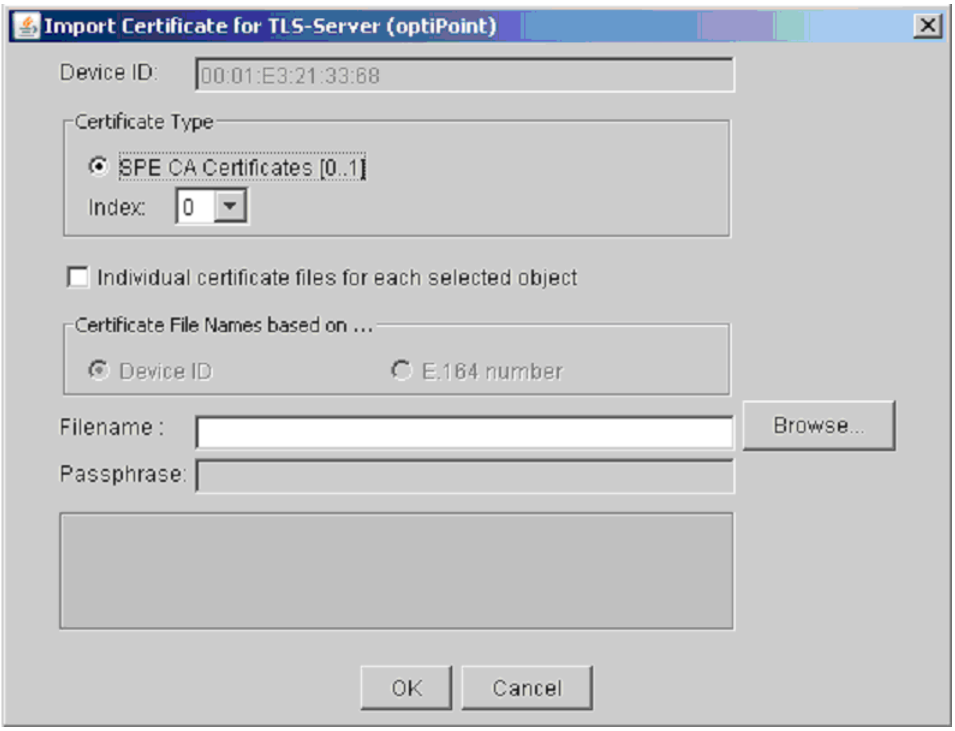
> If you decided to import individual certificated for each IP phone in step 5, these certificates must already be available as follows:
> All certificate file names must be based on:
> - The device IDs of the telephones or
> - The phones' E.164 numbers
>
> Select the appropriate option in **Certificate File Names based on ....**

Phone certificates should be in `PKCS#12` format and RADIUS certificates in `.pem` format.

7. For phone certificates only: Enter the key used to encrypt the PKCS#12 file you want to import in the **Passphrase** field (not necessary for RADIUS certificates).
8. Activate **Import certificate to DLS and activate on device (1-step)**, if the certificate should be activated immediately.
9. Click **OK** to import the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.
10. For activating the imported certificate, click **Activate certificate** and **Save** afterwards, when **Import certificate to DLS and activate on device (1-step)** is not activated.

16.12.3 Importing SPE CA Certificates for IP Phones

1. Select **IP Devices** > **IP Phone Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE CA Certificates" Tab**. Search for and select the IP phone that you want to import a certificate for to enable communication with the SIP server.
2. Click **Import Certificate**. An import dialog appears:



Import Certificate for TLS-Server (optiPoint)

Device ID: 00:01:E3:21:33:68

Certificate Type

● SPE CA Certificates [0..1]

Index: 0

☐ Individual certificate files for each selected object

Certificate File Names based on ...

● Device ID ○ E.164 number

Filename :

Passphrase:

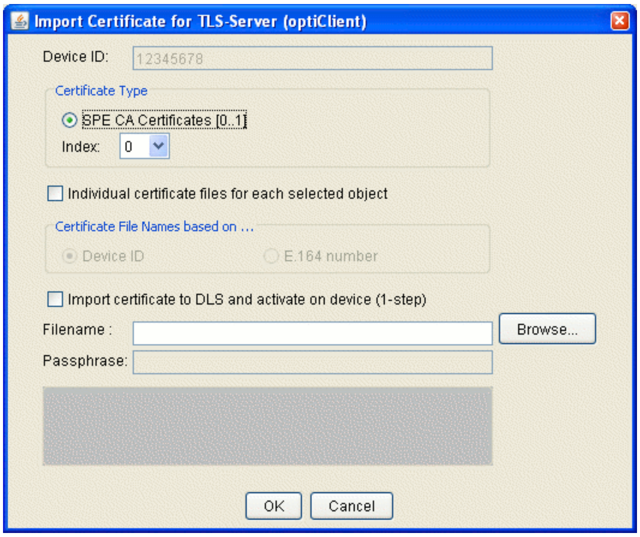
This dialog contains the device ID of the IP phone you have selected.

3. You must enter the according **Index**, because the CA certificate is indexed.
4. In the **File name** entry field, enter the entire local path including the name of the certificate or click **Browse** to enter the path via the browser.
   The certificate should be in `.pem` format.
5. Enter the key used to encrypt the PKCS#12 file you want to import in the **Passphrase** field.
6. Click **OK** to import the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.
7. For activating the imported certificate. click **Activate certificate** and **Save** afterwards.
8. To import a second certificate, proceed as described for the first certificate.

16.12.4 Importing SPE CA Certificates for IP Clients

1. Select **IP Devices** > **IP Client Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE CA Certificates" Tab**. Search for and select the IP client that you want to import a certificate for to enable communication with the SIP server.

2. Click **Import Certificate**. An import dialog appears:



Import Certificate for TLS-Server (optiClient)

Device ID: 12345678

Certificate Type

● SPE CA Certificates [0..1]

Index: 0

□ Individual certificate files for each selected object

Certificate File Names based on ...

● Device ID ○ E.164 number

□ Import certificate to DLS and activate on device (1-step)

Filename :

Passphrase:

This dialog contains the device ID of the IP phone you have selected.

3. In the **File Name** entry field, enter the entire local path including the name of the certificate or click **Browse** to enter the path via the browser.

   The certificate should be in `.pem` format.

4. Activate **Import certificate to DLS and activate on device (1-step)**, if the certificate should be activated immediately.

5. Click **OK** to import the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.

6. For activating the imported certificate, click **Activate certificate** and **Save** afterwards, if **Import certificate to DLS and activate on device (1-step)** is not activated..

7. To import a second certificate, proceed as described for the first certificate.

16.12.5 Importing SPE Certificates and SPE CA Certificates for IP Gateways

If Signaling and Payload (SPE) certificates are to be used, the IP phones must be connected to an IP gateway. The IP gateway has to be be pre-configured as virtual device.

1. Select **IP Devices** > **IP Device Management** > **IP Device Configuration**. Enter the IP address of the IP Gateway in the **Device ID** field and select "IP Gateway" in the **Device Family** field.

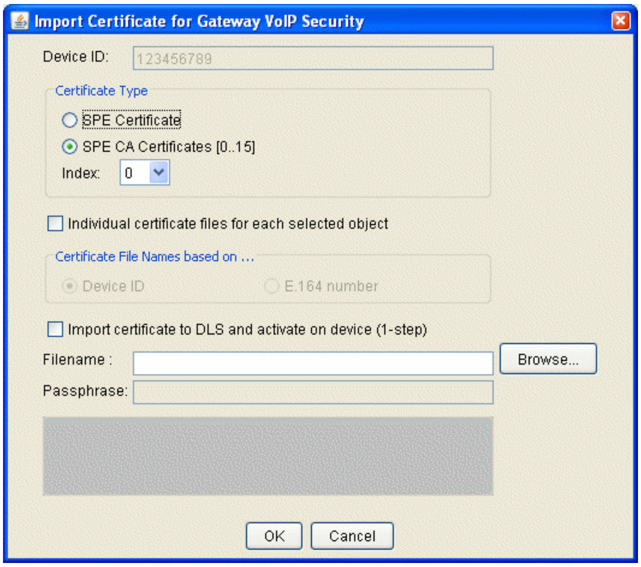
2. When configuring IP Gateways for the first time, enter the **DLS Server Address** and the **DLS Port** (Default: 18443) in the tab **DLS Connectivity**. If you want to configure further IP Gateways, these values will be used internally by the DLS.

3. **Secure mode required** is activated automatically, because IP Gateways may operate in this mode only. Select **PIN Mode**.

> If **Default PIN** has been chosen, this PIN might be administered by means of **Administration** > **Workpoint Interface Configuration**.
> The PIN must be declared to the IP Gateway board before the registration. This is done by the CLI interface (activate dls pin <pin>).

4. When pressing the **Scan** button, the registration including bootstrapping will be executed.

5. Switch to **IP Devices** > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE Certificate" Tab** and click on **Import Certificate**. An import dialog appears:



Import Certificate for Gateway VoIP Security

Device ID: 123456789

Certificate Type

○ SPE Certificate

● SPE CA Certificates [0..15]

Index: 0

□ Individual certificate files for each selected object

Certificate File Names based on ...

● Device ID ○ E.164 number

□ Import certificate to DLS and activate on device (1-step)

Filename :

Passphrase:

> The imported certificates must be created by means of a customer PKI.
> It is recommended to deploy an individual certificate for each gateway to which the own IP address is assigned in **Owner field (CN)**. This is absolutely neccessary if **Owner check** is activated. If DNS is used, the host name of the gateway may be entered instead of its IP address.

6. Choose whether you want to import a SPE certificate or a SPE CA certificate. For SPE CA certificates, you must enter the according **Index**, because this certificate is indexed.

7. In the **File name** entry field, enter the entire local path including the name of the certificate or click **Browse** to enter the path via the browser.
   The SPE certificate should be in PKCS#12 format, and the SPE CA certificate should be in `.pem` format.

8. For SPE certificate only: In the **Passphrase** field, enter the key used to encrypt the PKCS#12 file you want to import.

9. Activate **Import certificate to DLS and activate on device (1-step)**, if the certificate should be activated immediately.

10. Click **OK** to import the certificate. If you have selected several objects (see Section 5.4.2.4, "Multiple selection and data transfer in Table view"), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.

11. For activating the imported certificate, click **Activate certificate** and **Save** afterwards, if **Import certificate to DLS and activate on device (1-step)** is not activated.

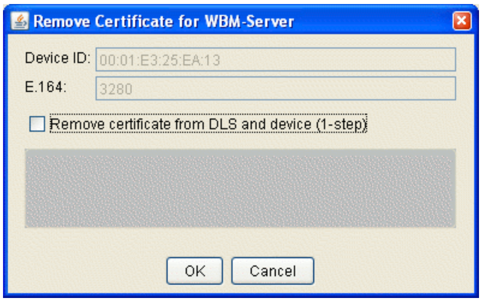
12. SPE Certificate as well as SPE CA certificate for IP Gateway must be imported.

13. Afterwards, the SPE Certificates for IP Phones / IP Clients must be imported as described in chapter Section 16.12.3, "Importing SPE CA Certificates for IP Phones" / Section 16.12.4, "Importing SPE CA Certificates for IP Clients".

14. Switch to **IP Devices** > **IP Phone Configuration** > **Signaling and Payload Encryption (SPE)** > **"SIP Settings" Tab** or **"HFA Settings" Tab** and set "TLS" in the entry fields **SIP Transport Protocol** resp. **HFA Transport Protocol**. For IP Clients the values have to be entered the same way.

16.12.6 Remove Certificate (IEEE 802.1x Phone as an example)

1. Select the area you require under **IP Devices** > **IP Phone Configuration** (see Section 16.12.1 to Section 16.12.5).
2. Search and select the IP phone whose certificate you want to remove or switch to **Template** view to delete a certificate from a template.
3. Click **Remove Certificate**. A dialog appears (see the following example):



Remove Certificate for WBM-Server

Device ID: 00:01:E3:25:EA:13

E.164: 3280

☐ Remove certificate from DLS and device (1-step)

4. For IEEE 802.1x certificates, select the certificate to be removed (if applicable). The option that corresponds to the tab is already selected.
5. Activate **Remove certificate from DLS and device (1-step)**, if the certificate should be remoced immediately.
6. Click **OK** to remove the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to remove certificates for all of these objects.
7. Click **Activate certificate** and **Save** to delete the certificate on the phone, if **Remove certificate from DLS and device (1-step)** is not activated.

16.12.7 Replace IP Phone

1. Click the **IP Devices** > **IP Device Management** > **IP Device Configuration** area. Click **Action** in the menu bar and select **Copy IP Device** (see Section 16.4, "Replacing an IP Device").
2. Please check if the copy contains all certificates as imported certificates, or the certificates are part of a default profile. If only activated certificates are available, they are not used any more with Plug&Play.

16.13 Configuring and Administrating Mobility

With the Mobility function, call numbers can be assigned to specific persons instead of devices. In addition to their call numbers, a user’s settings, such as, the key layout, can be transferred from one device to another. To enable this, users must log on to the device in question with their call number and a password. Once the user has logged off, the previous device used is reassigned its basic profile, and as a result, a different call number to that of the mobile user.

> For basic information on mobility in DLS, see Section 3.7, "DLS Mobility - General Information".

16.13.1 Configuring the Mobility Function on the Device

Select the **Mobility** tab in the area **IP Devices > IP Phone Configuration > SIP Mobility** and activate the option **Device available for Mobile User**.

16.13.2 Programming the "Mobility" Button

Configure a template with a key layout that provides a mobility key:

1. Select **Template** view in the area **IP Devices >** IP Phone Configuration > Keysets/Keylayout and click the icon in the **Destinations** tab. A new line is displayed in the table, in which you can make the required entries.
2. As the key function **Mobility** is on the first level, select "1. Level" in the **Level** column.
3. In the **Key number** column, select the key to which the new function should be assigned. For more information, see Section 7.1.19.2, ""Destinations" Tab".
4. Select "Mobility" in the **Key function** column.
5. You can now enter a key label in the final column. This is only displayed with optiPoint 420 telephones that provide LCD key labeling.
6. If you click **Save**, a dialog window opens where you can enter a name and a description for the template. Save the template by clicking **Save**.

   For more information on creating templates, see Section 15.4.1, "Creating a Template Manually".
7. Assign the template to a profile and load this profile to the required workpoint.

16.13.3 Creating a Mobile User Profile

1. Create templates containing the required mobile user configurations. Select the **Templates** view in the area to be configured, for example in **Mobile Users** > **SIP Mobile User Configuration** > **Miscellaneous**.
2. If you click **Save**, a dialog window opens where you can enter a name and a description for the template. Save the template by clicking **Save**.
3. Click **New** in the area **Profile Management** > **User Data Profile** to create a new profile. Click the icon . In the choice list that now opens, select the required template.
4. In the **Name** field, enter the name for the new profile. In the **Description** field, enter a short description of the profile if required.
5. Click **Save** to save the profile.

16.13.4 Creating Mobile Users

Requirements

- A working DLS infrastructure.
- The Mobile Users must already be configured in OpenScape Voice.

16.13.4.1 Adding New Mobility Users

1. Select the area **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User > "Mobile / Basis User" tab**.
2. Click **New**.

   Click the button to the right of the **New Mobile User IDs** field. A dialog window appears. The list shows all call numbers registered in the telephone system that are still available, i.e. that have not yet been assigned to a workpoint or mobile use. Clicking **OK** applies the data. In addition to the choice list, you also have the option of entering the call number of the mobile user into the field by hand. Multiple numbers must be comma-separated.
3. Under **Mobile User Password**, enter the password for the Mobile User accessing the Mobility Phone.
4. Under **Mobile User Profile**, select the profile (see Section 16.13.3, "Creating a Mobile User Profile") that should be applied for the Mobile User to be created.
5. If necessary, activate the **Get SIP Data from Virtual Devices** to automatically apply the SIP data entered in the device profile (**Profile Management** > **Device Profile**) for the Mobile User.
6. Click **Save**.

16.13.4.2 Creating Mobile Users via Migration

1. Go to **Mobile User > Mobile User Interaction > Mobile User**. If you select "Mobility enabled Device" in the **User Type** field and then click **Search**, a list of all devices available for a mobile user is shown in the **Table** view.
2. Click **Migration to Mobile User**. A dialog window opens.
3. Enter a new basic call number in the field **New Basic E.164** for the currently-selected device for which the basic profile is to be migrated. This must be registered on the SIP server. A new basic number is necessary so that the device is ready for use, even if a mobile user is not logged on. As soon as migration has been completed, the previous basic call number is assigned to the mobile user. The mobile user call number is also known as the **Mobility ID**.

> The SIP access data assigned to the basic call number must be included in the plug&play configuration.

4. A new profile must be entered for the basic user (basic call number) in the **Basic Mobile User Profile** field. The mobile user transfers the data and the call number of the device; this data automatically forms this user’s new individual profile. In the field **Mobile User Profile**, the mobile user call number is automatically entered with the prefix "@". This represents a wildcard for the mobile user’s individual profile.
5. Start the migration via **Start Migration**.
6. In the Field **Mobile User Password**, enter a new passwort for the Mobile User. (the default password is "000000").
7. To complete, confirm with **Save**.

16.13.5 Create a Home Phone

A home phone is an end device assigned to a SIP mobile user. The mobile user is logged on to the home phone by default. Setting up of a home phone is optional. However, when a home phone has been set up, the mobile user is automatically logged on to it after having been logged off from another phone, and thus, he is accessible. When the mobile user logs off from the home phone, he is not accessible any more.

1. Navigate to **Mobile Users > SIP Mobile User Interaction > SIP Mobile User**. If you choose "Mobility enabled Device" in the field **User Type** and click on **Search** afterwards, you get a list in **table** view that contains all end devices which are available to a mobile user. For mobile users with status "Mobile User Logged Off", the fields under **Mobile User Home Phone** are available.
2. Activate **Allow automatic Logon at Home Phone**, so that logging on the mobile user at the home phone is activated immediately.
3. For **Home Phone**, choose the call number of the end device from the selection list. The Home **Phone Status** field shows the status of the home phone selected.
4. Finally, confirm by **Save**.

16.13.6 Logging On Mobile Users (Forced Logon)

A mobile user can be logged on not only at the device but also via DLS.

1. In the area **Administration > SIP Mobile User Interaction > Logon/Logoff** use **Search** > **Table** view **> Object** view to find the mobile user you want to log on. Alternatively, you can also select the device where you want to log the mobile user on.
2. Click **Logon Mobile User**.
3. A dialog window opens. If you had already selected a mobile user, enter the Basic E.164 number now for the device where you want to log the mobile user on. If you have selected a device, you must enter the mobile user's mobility ID.

16.13.7 Logging Off Mobile Users (Forced Logoff)

Using the DLS, the administrator can implement a forced logoff for a Mobile User that is logged on to a workpoint. This interrupts ongoing calls.

1. In the area **Administration > SIP Mobile User Interaction > Logon/Logoff** use **Search** > **Table** view **> Object** view to find the mobile user that you wish to log off. Alternatively, you can also select the device where the mobile user is logged on.
2. You can use **Logoff Mobile User** to log the Mobile User off the relevant device.

16.13.8 Troubleshooting for Mobile User Logon/Logoff

The **History** tab in the area **Mobile User > Mobile User Interaction > Logon/Logoff** contains information regarding actions. This information is available for the Mobile User and for devices that are available for the Mobile User.

You can find a survey of all mobile user related actions in the are **Mobile Users** > **Mobility Statistics**.

A multitude of reasons can lead to a situation where a mobile user is logged on at two phones (A and B) simultaneously. This will not cause an error in OpenScape Voice. However, the DLS provides a special error handling which tries to clear this situation by logging off the mobile user at phone A, as soon as it is reachable again.

Possible reasons for unsuccessful logoff:

1. Phone A is not available, is restarting, is plugged off, has a broken network, or a hardware problem. These are the most probable reasons.
2. Phone A has a software problem and cannot complete the protocol for exectuing the logoff. In most of these cases, the DLS is able to tell the phone to start a logoff, but the phone does not execute it.

3. Phone A is DCMP-enabled. SIP Mobility and DCMP do not work together. Therefore, DCMP has to be disabled when using SIP Mobility.
4. Phone A is not accepted by the DLS, because it is in Secure Mode, but does not have a valid certificate of this DLS.
5. Phone A does not have the correct DLS-Address.
6. Phone A is in a phone call (see time before doing a Logoff while a Phone Call is ongoing: **Main Menu** > **Mobile Users** > **SIP Mobile User Configuration** > **SIP Mobility** > **"Mobility Logon/Logoff" Tab**).

16.13.9 Default Setting for the Key Layout in Mobility Telephones

For each device type, default key layouts can be defined for the four basic key functions "Prime Line", "Mobility", "Cancel" and "Shift". These defaults overwrite the key layout defined in each Mobile User's profile.

1. Select the area **Mobile Users** > **SIP Mobile User Interaction** > **SIP User Keylayout**.
2. Select the required **Device Type**.
3. Activate **Use following Defaults for Mobile User Logon**.

16.13.10 Data Backup to a .zip Archive

All mobile user data can be saved in a .zip archive. The data within the .zip archive is saved in XML format which is the format used for data exchange between workpoints and DLS.

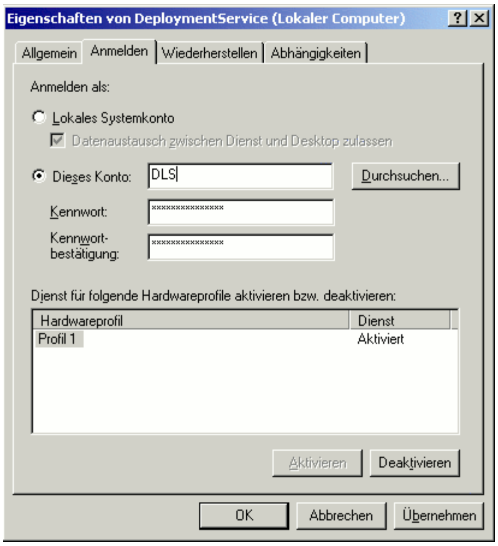
16.13.10.1 Preparation

Data backup should normally be performed on a network drive. Only one specific directory should be released for mobile user data storage. The following steps are required for this:

1. Stop the DeploymentService, that is the DLS Web service. To do this, click **Programs** > **DeploymentService** > **Stop Service** in the Windows Start menu.
2. As the DeploymentService runs after installation with the localadmin account for which no drives are normally mapped, it can only access local drives at first. You should therefore assign the DeploymentService an account which contains privileges for the network drive to be mapped.

> ⚠ **Make sure that the DeploymentService account has administrator rights. Restrictions can lead to problems with DLS.**

To assign a new account to the DeploymentService, select **Settings** > **Administrative Tools** > **Services** or **Settings** > **Control Panel** > **Administrative Tools** > **Services** in the Windows Start menu. Double-click the **DeploymentService** entry to open a window where you can change the properties of the service. Now activate the **This account** check box in the **Log On** tab and click **Browse** to select the relevant user account.



Anmelden als:

○ Lokales Systemkonto

☑ Datenaustausch zwischen Dienst und Desktop zulassen

● Dieses Konto: DLS

Kennwort: ***************

Kennwort-bestätigung: ***************

Dienst für folgende Hardwareprofile aktivieren bzw. deaktivieren:

Hardwareprofil	Dienst
Profil 1	Aktiviert

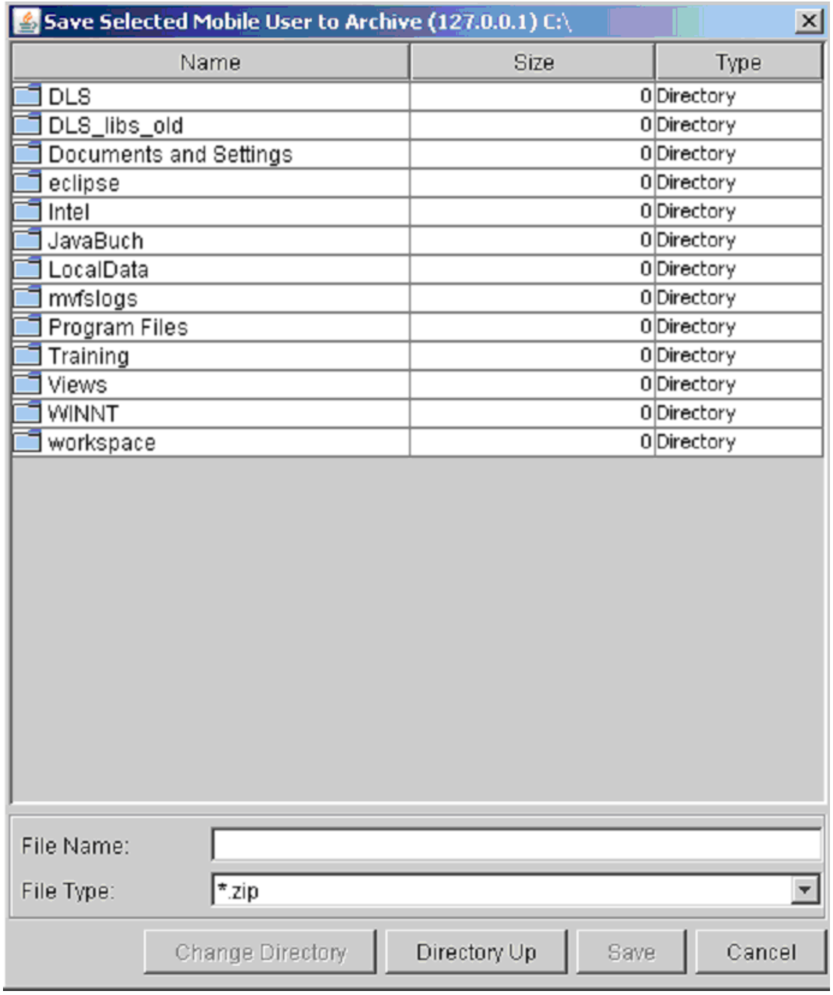
3. Rename the following files in the folder
`"C:\Program Files\DeploymentService\Tomcat5\bin"`:
`initdlsservice.template` > `initdlsservice.bat`
`releasedlsservice.template` > `releasedlsservice.bat`

4. Enter the network drive connection or release command as described in the files `"initdlsservice.bat"` and `"releasedlsservice.bat"`.

5. Select **Programs** > **DeploymentService** > **Start Service** to restart the service.

16.13.10.2 Saving Mobile User Data

1. Select the area **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User**.
2. Click **Search** to find all available mobile users.
3. Select the option **Table** under **Views**. Mark the mobile user whose data you want to save.
4. Now, select the entry **Save Selected Mobile User to Archive** in the menu bar under **Action**. A dialog window opens where you can select the storage location.



Name	Size	Type
DLS	0	Directory
DLS_libs_old	0	Directory
Documents and Settings	0	Directory
eclipse	0	Directory
Intel	0	Directory
JavaBuch	0	Directory
LocalData	0	Directory
mvfslogs	0	Directory
Program Files	0	Directory
Training	0	Directory
Views	0	Directory
WINNT	0	Directory
workspace	0	Directory

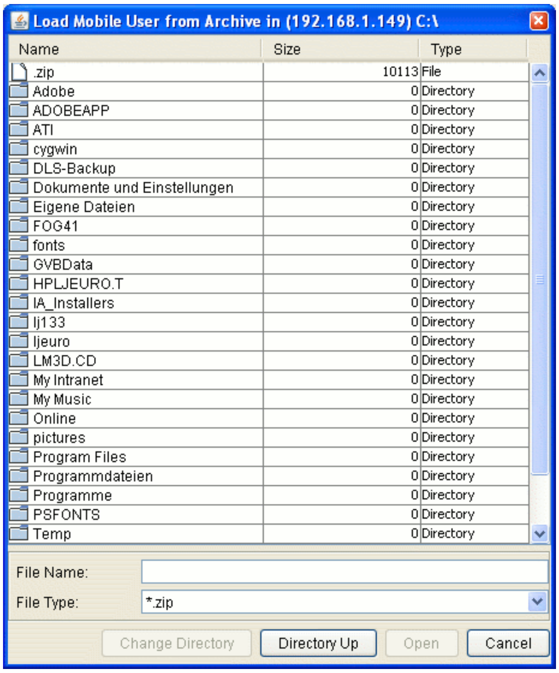
File Name:
File Type: *.zip

5. The contents of the drive where the DLS is installed are displayed by default. Mark a directory name and then click **Directory Change** or double-click the directory name to select the required destination directory. Click **Directory Up** to move to a higher directory level.
6. Enter a file name for the ZIP archive and confirm with **Save**. Alternatively, you can mark an existing archive in the list with a simple click and then press **Save**. In the ensuing selection window, you can choose if you want to save the mobile user data to the existing archive (**Write Data to existing Archive**) or overwrite the existing archive (**Create new Archive**).

16.13.10.3 Loading Mobile User Data

> You can only load mobile user data if the relevant mobile users are logged off. Data associated with a mobile user who is logged on will not be overwritten.

1. Select the area **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User**.
2. Now, select the entry **Import Mobile User** in the menu bar under **Action**. A dialog window opens for selecting the directory path. Mark a directory name and then click **Directory Change** or double-click the directory name to select the required destination directory. Click **Directory Up** to move to a higher directory level.



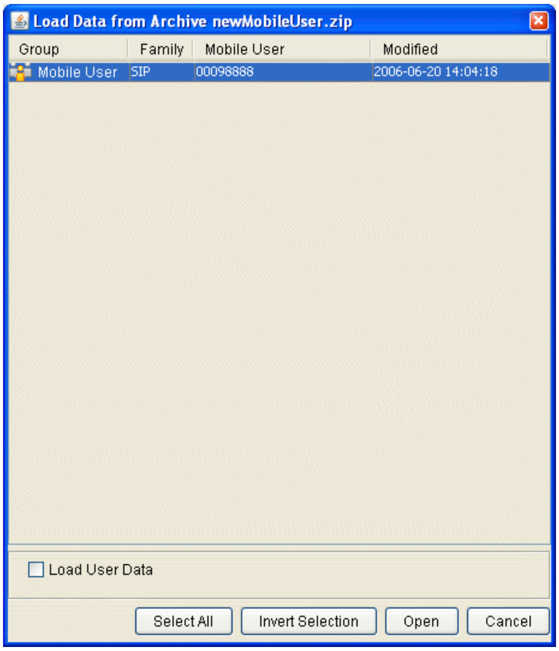
Load Mobile User from Archive in (192.168.1.149) C:\

Name	Size	Type
.zip	10113	File
Adobe	0	Directory
ADOBEAPP	0	Directory
ATI	0	Directory
cygwin	0	Directory
DLS-Backup	0	Directory
Dokumente und Einstellungen	0	Directory
Eigene Dateien	0	Directory
FOG41	0	Directory
fonts	0	Directory
GVBData	0	Directory
HPLJEURO.T	0	Directory
IA_Installers	0	Directory
lj133	0	Directory
ljeuro	0	Directory
LM3D.CD	0	Directory
My Intranet	0	Directory
My Music	0	Directory
Online	0	Directory
pictures	0	Directory
Program Files	0	Directory
Programmdateien	0	Directory
Programme	0	Directory
PSFONTS	0	Directory
Temp	0	Directory

File Name:

File Type: *.zip

3. Mark a .zip archive in the list and click **Open**. A list of all mobile user data records saved in this archive is displayed.



Load Data from Archive newMobileUser.zip

Group	Family	Mobile User	Modified
Mobile User	SIP	00098888	2006-06-20 14:04:18

□ Load User Data

4. Mark the data records you want or, where applicable, click **Select All**. You can also select **Reset selection**. Use the **Load User Data** check box to specify whether or not non-configurable user data, such as, call lists or phone book data, should be loaded to the DLS database.

> Call lists and phone book data must be saved in encrypted format.

5. If you click **Open** now, the selected mobile user data is loaded to the DLS database.

> It may take some time to load all user data depending on the data volume.
> The size of the non-configurable user data can be requested over **Mobile Users** > **User Data Administration**.

16.13.11 Import Mobile User Data

It is possible to import a manually created csv file with Mobile User Data. An export of Mobile User Data is not allowed due to data security reasons.

The file must have following format:

1. row: Description of columns content:

<E.164>	Required ,valid E.164 number
<Mobile User Password>	Required
<Mobile User Profile>	Required
<Get SIP Registration Data from Virtual Devices>	optional
<Home Phone>	optional
<Allow automatic Logon at Home Phone>	Required, possible values: true, false

Table 16-1

2. and following rows: Columns content separated by ';'

Import-File example:

```
<E.164>;<Mobile User Password>;<Mobile User Profile>;<Get SIP Regist-
ration Data from Virtual Devices>;<Home Phone>;
<Allow automatic Logon at Home Phone >
12345;000000;@profile;;;false
33333;000000;@profile;;;false
4411594311111;000000;MobUser;;;false
4411594312334566789;000000;MobUser;;12345;true
```

To import a file with mobile user data, proceed as follows:

1. Switch to **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User** and click **Import Mobile User**. An import dialog appears, brows for valid filename.
2. Click on **Save** to save the imported mobile user.

16.13.12 Mobility between optiPoint and OpenStage

Mobility between optiPoint and OpenStage is possible, but with restrictions only. For additional information see
http://wiki.siemens-enterprise.com/images/7/72/SIP_Mobility_User_-_optiPoint_and_OpenStage_Regression_Test.pdf

16.14 HFA Mobility with HiPath 3000

This feature allows for using the HiPath 3000 IP Mobility feature in a networked (TDM or IP trunks) environment with a closed numbering range.

> Technically, only a matching HiPath 3000 LCR dial plan entry is required for the IP Clients on other nodes, while LCR routing is irrelevant. Without a matching LCR dial plan entry, it will only be possible to enter local E.164 subscriber numbers when using the feature. The network trunks are not used for this feature.

On HiPath 3000 systems, the DLS is responsible for sending the correct registration information to IP Clients that are not logging-on at their home location.

HFA Mobility with HiPath 3000 systems works as follows: A subscriber from a different HiPath 3000 system logs on at an IP Phone, which results in the phone being unable to communicate with the gateway because of modified registration data. The IP Phone contacts the DLS, which thereupon looks up the virtual device that belongs to the subscriber’s E.164 number. The registration data of this virtual device are now sent to the IP Phone, thus enabling it to register.

For all virtual devices, which are to be used for HFA Mobility, **Delete after Plug & Play** on mask **IP Devices** > **IP Device Management** > **IP Device Configuration** must be switched off.

For further settings, see Section 7.1.18, "HFA Mobility".

16.14.1 HiPath 3000 Configuration Prerequisites

IP mobility is configured and working on each HiPath 3000 node as described in the HiPath 3000/5000 feature description.

16.14.2 DLS Configuration for Network-wide HFA Mobility

Only the extra DLS configuration required for HFA Mobility with HiPath 3000 will be considered here:

- Import the configuration from each node into the DLS using "Element Manager" (including the IP Clients). The IP Clients are virtual devices on the DLS.
- In **IP Devices** > **IP Device Management** > **IP Device Configuration** > **"General" Tab** activate the **Use for HFA Mobility with HiPath 3000** switch for each IP Client in each node.

16.14.3 Operating procedure

1. Activate (Mobile user logon) with this entry:
   *9419 + E.164 subscriber number + password (password optional if not configured)

2. The IP Phone will try to logon at the current HiPath 3000 node using the E.164 subscriber number that has been entered. The message "Logging On To Home" will be displayed briefly. The logon will fail because the IP Client is not configured at this HiPath 3000 node. The message "Mobile Log On Failed" will appear on the top line of the display, with "Contacting DLS" on the bottom line of the display.

   The IP Phone will then send a "mobility-configuration-request" message to the DLS. The DLS will then send the correct registration information that will allow this IP Client to logon at the correct home node.

3. Deactivate (Mobile user logoff) by entering #9419.

16.15 Data Structures for DLS-hosted XML applications

In the following, the storage locations for data to be used by DLS-hosted XML applications are described. This enables customizing the applications by the user resp. administrator.

16.15.1 Directory Structure

- Texts and default pictures are searched under `<DLS installation path>/DeploymentService/Tomcat5/webapps/XMLApplications/data/default`
- For customization by means of customer texts and pictures, it is possible to create a directory `<DLS installation path>/DeploymentService/Tomcat5/webapps/XMLApplications/data/custom` which will then serve as search path for the texts and pictures.

> It is recommended to copy the directory `.../XMLApplications/data/default` to `.../XMLApplications/data/custom` and then make the intended changes there.

- Under
  `.../XMLApplications/data/DeploymentService`,
  `.../XMLApplications/data/LocationService`,
  `.../XMLApplications/data/MakeCall`,
  `.../XMLApplications/data/NewsService`
  the texts for the respective XML applications are stored. These directories may not be changed by the user.

16.15.2 Directories at Upgrade Installations

With regard to upgrade installations, please consider the following:

- The `.../XMLApplications/data/default` directory is updated.
- The `.../XMLApplications/data/custom` is renamed to `.../XMLApplications/custom_old`

> If customizations have been made, these must be redone. For this, copy `.../XMLApplications/data/default` to `.../XMLApplications/data/custom` again or rename `.../XMLApplications/data/custom_old` to `.../XMLApplications/data/custom`

- The directories
  `.../XMLApplications/data/DeploymentService`,
  `.../XMLApplications/data/LocationService`,

.../XMLApplications/data/MakeCall,
.../XMLApplications/data/NewsService
remain unchanged.

16.15.3 Directories at Backup/Restore

With regard to a restore, please consider the following:

- The directory `.../XMLApplications/data/default` is not saved.
- The directory `.../XMLApplications/data/custom` is saved and will either be restored or copied to `.../XMLApplications/data/custom_<old Version>`, dependent on the settting of **Administration** > **Backup/Restore** > **Restore XML application data too**.

> If customizations have been made, these must be redone. For this, copy `.../XMLApplications/data/default` to `.../XMLApplications/data/custom` again or rename `.../XMLApplications/data/custom_old` to `.../XMLApplications/data/custom`

- The directories `.../XMLApplications/data/DeploymentService`, `.../XMLApplications/data/LocationService`, `.../XMLApplications/data/MakeCall`, `.../XMLApplications/data/NewsService` are saved and restored. These directories may not be changed by the user.

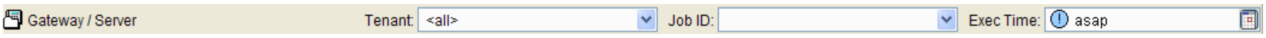
16.16 Use Multi-Tenancy

In the following, the administration of data from multiple clients (=tenants) with one single DLS installation is described.

> This function is available only when DLS multi-tenancy has been installed. This will be asked by the installation assistant.

With multi-tenancy masks, the selection menu **Tenants** is available. Otherwise, it is greyed out.

> When a a new object is created without selecting a tenant, an error message appears.



Gateway / Server Tenant: <all> Job ID: Exec Time: asap

With multi-tenancy masks, it will make a difference whether the object is assigned to a tenant or not, that is, in the tool bar under **Tenant**, either the tenant's name or <not assigned> will be displayed.

When objects are added which require a license, the tenant specific limits are checked. If a tenant is created or changed, the license dependent data are checked. The respective alarm thresholds are set tenant specific (see Section 6.2.1, "Tenants"). Basically, there is a difference between tenant dependent and tenant independent alarms.

16.16.1 Install/Deinstall Multi-Tenancy

16.16.1.1 First Installation

Follow the instructions of the installation assistant and, at **Components**, click **Multi-Tenancy**.

16.16.1.2 Update Installation

Follow the instructions of the installation assistant and, at **Components**, click **Multi-Tenancy**.

For all data that can be tenant specific, <not assigned> is entered as a tenant. Later, the data can be assigned to defined tenants.

16.16.1.3 Uninstalling

Execute an update installation and, at **Components**, deactivate **Multi-Tenancy**.

16.16.1.4 Import Tenants From OpenScape Voice Assistant

1. When you use a version > V3.0 of OpenScape Voice Assistant, open:
   Element Manager > **Element Manager Configuration** > **"OpenScape Voice Assistant" Tab**
   or, otherwise:
   Element Manager > **Element Manager Configuration** > **"OpenScape Voice Assistant V3.0" Tab**.
2. Enable **Tenants synchronization** and click **Update Business Groups**.

For each business group, a tenant and a location is created. The names used hereby are constructed from <BusinessGroups Switchname (OpenScape Voice Assistant Version > V3.0) ><BusinessGroups Name>. Tenants and locations already existing are updated.

16.16.2 Set Up Tenants

1. Navigate to **Administration** > **Server Configuration** > **Tenants**.
2. Enter the required number of licenses. You can check the total number via **Administration** > **Server Licenses**.
3. If an appropriate location exists already, assign it to the tenant now via **Administration** > **Server Configuration** > **Tenants** > **"Locations" Tab**. The possible values are displayed in a selection list. It is possible to assign multiple locations. After this, continue with step 6.
4. If no appropriate location should be set up yet, click **Save** firstly to create the tenant, as this will be required for setting up the location. After this, navigate to **Administration** > **Server Configuration** > **Location** and create a location.

> All IP Devices must be assigned to a defined location which is different from the default location. When IP Clients are used, please ensure that all IP addresses available for IP Clients are included when entering IP ranges.

> If IP Clients are used, please regard that all IP addresses possible for the IP Clients are incorporated when entering IP ranges.

5. Change to **Administration** > **Server Configuration** > **Location** > **"Tenants" Tab** and assign the location to a tenant. A location can be assigned to only one tenant.
6. Change to **Administration** > **Account Management** > **Account Configuration** and assign the tenant to that account which shall access the data belonging to this tenant.

> The newly created tenant will be assigned to the "admin" account. This assignment cannot be effected via the GUI.

16.16.3 Delete Tenants

To delete a tenant, all references to this tenant must be removed first.

1. Navigate to **Administration** > **Server Configuration** > **Tenants**.
2. Mark the desired tenant and delete the locations listed in the **"Locations" Tab**.
3. Click **Delete** and, in the dialog window, confirm that the tenant is to be deleted.

> A tenant that has been deleted will be removed automatically from the "admin" account. This cannot be effected via the GUI.

16.16.4 Set Up a Multi-Tenancy Account

1. Navigate to **Administration** > **Account Management** > **Account Configuration**.
2. Create an account, as described in Section 6.1, "Account Management". As **Access Type**, choose **DLS-GUI**.
3. Assign the desired roles. The role EDIT_GENERAL_ONE ensures that the account may only edit multi-tenancy masks. With the role EDIT_SYSTEM, also system relevant masks which affect all tenants can be edited.
4. Change to the **"Tenants" Tab**. In **Tenant**, enter the tenants that can be edited by this account.

Multi-tenancy accounts can edit data belonging to the assigned tenants as well as data marked with <not assigned>. To the "admin" account, the selection <all> is available in addition. With <all>, all data present in the database can be displayed and edited.

16.16.5 Multi-Tenancy Alarm Configuration

When a tenant is set up, a tenant specific alarm configuration is created automatically. At this, the data of the generic (<not assigned>) alarm configuration are copied. If a tenant is chosen in the tool bar, the corresponding tenant dependent alarm configuration will be selected. Thus, Email addresses, batch files, and SNMP traps can be entered for license, mobility, and certificate expiration in a tenant-specific manner.

16.16.6 Server Assignments

For FTP server, HTTPS server, and network drives, the tenants must be assigned in the "Tenants" tab of the respective masks. The assignment of a location (see Set Up Tenants) is not sufficient, though servers are assigned to the location on its part.

16.16.7 Mobile Users

With regard to the mobile user functionality, please regard the following:

- For the location of a tenant, an E.164 pattern should be specified in order to ensure that the call number configured for the mobile user is valid.
- If call number bands are shifted from one tenant to another, the mobile users must be assigned to the new tenant manually. For this, navigate to **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User** and enter the tenant in the **Tenant** field.

16.16.8 Multi-Tenancy Profile Management

When a location is added to a tenant, also the default profiles are assigned to this tenant, including the contained templates. All remaining profiles, user data profiles, and templates can be assigned to individual tenants via the respective "Tenants" tab.

16.16.9 Automatic Number Pool with Multi-Tenancy

Using automatic number assignment in a multi-tenancy system is not recommended. If this function is to be used anyhow, it must be ensured that all call numbers of the number pool are assigned to a separate tenant. This tenant must be visible to all DLS accounts. When all E.164 numbers of the number pool reside in a separate business group of the OpenScape Voice, this can be achieved by synchronizing the tenant via the Element Manager. If this should not be the case, configure a tenant with a location that contains exclusively the E.164 numbers of the number pool.

17 Appendix

The appendix contains abbreviations and additional information.

17.1 Abbreviations and Technical Terms

For more information on network technology and Voice over IP (VoIP), refer to the relevant reference material.

> For definitions of the terminology related to the mobility feature, see Section 3.7.1, „Mobility Definitions“.

EA

Abbreviation for "**E**xternal **A**ccess".
If appropriately configured, the external access must precede a phone number if this number is an external phone number. See also Canonical format.

AMO

Abbreviation for "**A**dministration and **M**aintenance **O**rder".
An order which directly provides the CBX (**C**omputerized **B**ranch **E**xchange) with administration or maintenance information. An AMO is transmitted via EMML (Extended Machine Maintenance Language).

ASCII code

Standardized character set for representing and processing text in computers and communication systems (see ASCII tables on the following pages).

ASCII Table (Standard)

Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)
	0	0	SP	20	32	@	40	64		’60	96
^A	1	1	!	21	33	A	41	65	a	61	97
^B	2	2		"22	34	B	42	66	b	62	98
^C	3	3	#	23	35	C	43	67	c	63	99
^D	4	4	$	24	36	D	44	68	d	64	100
^E	5	5	%	25	37	E	45	69	e	65	101
^F	6	6	&	26	38	F	46	70	f	66	102
^G	7	7		'27	39	G	47	71	g	67	103
^H	8	8	(	28	40	H	48	72	h	68	104
^I	9	9	)	29	41	I	49	73	i	69	105
^J	0A	10	*	2A	42	J	4A	74	j	6A	106
^K	0B	11	+	2B	43	K	4B	75	k	6B	107
^L	0C	12	,	2C	44	L	4C	76	l	6C	108
^M	0D	13	-	2D	45	M	4D	77	m	6D	109
^N	0E	14	.	2E	46	N	4E	78	n	6E	110
^O	0F	15	/	2F	47	O	4F	79	o	6F	111
^P	10	16	0	30	48	P	50	80	p	70	112
^Q	11	17	1	31	49	Q	51	81	q	71	113
^R	12	18	2	32	50	R	52	82	r	72	114
^S	13	19	3	33	51	S	53	83	s	73	115
^T	14	20	4	34	52	T	54	84	t	74	116
^U	15	21	5	35	53	U	55	85	u	75	117
^V	16	22	6	36	54	V	56	86	v	76	118
^W	17	23	7	37	55	W	57	87	w	77	119
^X	18	24	8	38	56	X	58	88	x	78	120
^Y	19	25	9	39	57	Y	59	89	y	79	121
^Z	1A	26	:	3A	58	Z	5A	90	z	7A	122
	1B	27	;	3B	59	[	5B	91	{	7B	123
	1C	28	<	3C	60	\	5C	92	|	7C	124
	1D	29	=	3D	61	]	5D	93	}	7D	125
	1E	30	>	3E	62	^	5E	94	~	7E	126
	1F	31	?	3F	63	_	5F	95	DEL	7F	127

ASCII Table (Enhanced)

Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)
_	80	128		A0	160	À	C0	192	à	E0	224
_	81	129	¡	A1	161	Á	C1	193	á	E1	225
‚	82	130	¢	A2	162	Â	C2	194	â	E2	226
ƒ	83	131	£	A3	163	Ã	C3	195	ã	E3	227
"	84	132	¤	A4	164	Ä	C4	196	ä	E4	228
...	85	133	¥	A5	165	Å	C5	197	å	E5	229
†	86	134	¦	A6	166	Æ	C6	198	æ	E6	230
‡	87	135	§	A7	167	Ç	C7	199	ç	E7	231
ˆ	88	136	¨	A8	168	È	C8	200	è	E8	232
‰	89	137	©	A9	169	É	C8	201	é	E9	233
Š	8A	138	ª	AA	170	Ê	CA	202	ê	EA	234
‹	8B	139	«	AB	171	Ë	CB	203	ë	EB	235
Œ	8C	140	¬	AC	172	Ì	CC	204	ì	EC	236
_	8D	141	-	AD	173	Í	CD	205	í	ED	237
_	8E	142	®	AE	174	Î	CE	206	î	EE	238
_	8F	143	¯	AF	175	Ï	CF	207	ï	EF	239
_	90	144	°	B0	176	Ð	D0	208	ð	F0	240
‘	91	145	±	B1	177	Ñ	D1	209	ñ	F1	241
’	92	146	²	B2	178	Ò	D2	210	ò	F2	242
"	93	147	³	B3	179	Ó	D3	211	ó	F3	243
”	94	148	´	B4	180	Ô	D4	212	ô	F4	244
•	95	149	µ	B5	181	Õ	D5	213	õ	F5	245
–	96	150	¶	B6	182	Ö	D6	214	ö	F6	246
—	97	151	·	B7	183	×	D7	215	÷	F7	247
˜	98	152	¸	B8	184	Ø	D8	216	ø	F8	248
™	99	153	¹	B9	185	Ù	D9	217	ù	F9	249
š	9A	154	º	BA	186	Ú	DA	218	ú	FA	250
›	9B	155	»	BB	187	Û	DB	219	û	FB	251
œ	9C	156	¼	BC	188	Ü	DC	220	ü	FC	252
_	9D	157	½	BD	189	Ý	DD	221	ý	FD	253
_	9E	158	¾	BE	190	Þ	DE	222	þ	FE	254
Ÿ	9F	159	¿	BF	191	ß	DF	223	ÿ	FF	255

PU

Abbreviation for "Call **P**ick**u**p".
If you have one workpoint in an office and another in a lab and want your contacts to be able to reach you at a single subscriber number, you can create a pickup group containing both workpoints. The workpoint called rings. The call can be accepted. The "call pickup" LED also flashes on the other workpoint. You can answer the call by simply pressing the appropriate button.

C-SWS

Abbreviation for "**C**entral **S**oft**w**are **S**upply Server".
Name of the central software supply server in Brussels.

CAP

Abbreviation for "**C**ommon **A**pplication **P**latform".

CAT NetInstall

In Germany, you can use CAT NetInstall for installation on → TAP.

CD

Abbreviation for "**C**all **D**eflection".
ISDN feature for call deflection in ringing state.

CF

Abbreviation for "**C**all **F**orwarding".
ISDN feature for automatic call forwarding.

The following types of call forwarding exist:

- **CFU**
  Call **F**orwarding **U**nconditional (immediate call forwarding)
- **CFNR**
  Call **F**orwarding **N**o **R**eply (forward call if no reply)
- **CFB**
  Call **F**orwarding **B**usy (forward call if busy)

CLA

Abbreviation for "**C**ustomer **L**icense **A**gent".
The HLM component that encrypts the licenses for the product and assigns them to the relevant products.

CLI

Abbreviation for "**C**ommand **L**ine **I**nterface".
Operating network devices by entering data in a command line. This interface is usually password-protected and is reached via Telnet.

CLM

Abbreviation for "**C**ustomer **L**icense **M**anager".
The HLM component that administers HiPath product licenses for the customer.

CSV

Abbreviation for "**C**omma-**S**eparated **V**alues".
File with tabular data. In some cases, the column labels are entered in the first line. In general, a column is set off by a semicolon or comma, and a line change is indicated by the start of a new line. Can be imported with Microsoft Excel, for example.

CTI

Abbreviation for "**C**omputer **T**elephony **I**ntegration".
CTI uses computer technology to support telephone services. It not only supports the varied attendant functions associated with service features but also system management and accounting.

CTS

Abbreviation for "**C**lear **T**o **S**end".
Clear to send is an interface function signal. It is part of modem control in handshake mode and is also used for access authorization in the CSMA/CA procedure. In this procedure (which is also used in WLANs with 802.11), a station that wants to send data transmits an RTS (Ready To Send) packet. If the transmission route to the receiver is clear, the station receives a CTS packet.

CW

Abbreviation for "**C**all **W**aiting".
ISDN feature for signaling the arrival of more calls during a call.

DBFS

Abbreviation for "**D**ata**b**ase **F**eature **S**erver".
Manager for the HiPath 3000/5000 communication platform.

Default Route

A default route is a route that is suitable for each target address. This means that the route can be used for all target addresses. The default route has the lowest priority and is only used if no other routes match. A route essentially determines which path the packets should or can take for transport in the network – if no path is prescribed or known, the default route is used.

DCMP

Abbreviation for "**D**LS-**C**ontact-**M**e-**P**roxy". The DCMP acts as a proxy for routing between the DLS and devices when a firewall or NAT prevents the DLS from sending Contact-Me messages to the devices. The DCMP can communicate with the DLS over the firewall or NAT and is polled regularly by the devices for messages from the DLS. If messages are present, the DCMP creates a connection between the device and the DLS. The DLS can then send control and configuration data to the device.

DHCP

Abbreviation for "**D**ynamic **H**ost **C**onfiguration **P**rotocol".
Dynamic assignment of IP addresses for stations in an IP network using a central DHCP server.

DLS

Abbreviation for "OpenScape **D**ep**l**oyment **S**ervice".
The DLS is an OpenScape Management application for administering IP devices (IP phones, IP client installations, and IP gateways) in HiPath and non-HiPath networks.

DMC

Abbreviation for "**D**irect **M**edia **C**onnection".
Workpoints that use signaling to establish connections via a switching element (for example, a gateway) also usually transmit reference data via this switching element. If both workpoints use the same signaling protocol and the same type of reference data transmission, switching via the gateway can be used to directly exchange reference data between the two workpoints. This direct exchange of reference data is referred to as "**D**irect **M**edia **C**onnection".

DNS

Abbreviation for "**D**omain **N**ame **S**ervice".
The DNS service converts an alphanumeric name query (such as www.siemens.en) into an IP address.

The large primary name servers at InterNIC and the national registration agencies (such as, en-NIC for Germany) have database servers for this to assign the IP addresses to the host names.

Domain

A domain is a logical network of computers and can also be split up into subdomains. DNS servers are used for resolving domain names. An example of a domain name is www.microsoft.com, for example. In this case, the "." (period) stands for the ROOT of the DNS server, ".com" stands for the commercial top-level domain, ".microsoft" stands for the company and "www" stands for the computer. Domain names are resolved from right to left.

Downgrade

Installation of software with a version number that is lower than the one currently in use.

DSM

Abbreviation for "optiPoint **DIs**play **M**odule".
A key module for optiPoint workpoints which features a touchscreen and enhanced functions, such as phone book, browser, and Java programs.

DTMF

Abbreviation for "**D**ual-**T**one **M**ulti**f**requency".
This dual-tone procedure is used in phone systems for dialing. DTMF replaced the pulse-tone procedure used in older rotary-dial telephones and establishes connections quickly in communications networks. The DTMF signal consists of two tones which are generated by pressing the keys on a phone and transmitted to the switching center. These two tones are taken from a set of eight different tones. They are assigned to the lines (1, 4, 7, star) and rows (1, 2, 3) on a telephone keypad. The DTMF procedure can also be used to access menu-driven services (for example, answering machines, mailboxes) directly via a telephone keypad.

E.164

Standardized phone number according to the ITU’s international numbering plan with a maximum of 15 digits. Normally composed of three parts: CC, **(C**ountry **C**ode), NDC (**N**ational **D**estination **C**ode) and SN (**S**ubscriber **N**umber).

EAP

Abbreviation for "**E**xtensible **A**uthentication **P**rotocol".

ECT

Abbreviation for "**E**xplicit **C**all **T**ransfer".
ISDN feature for call transfer during the call.

ENB

Abbreviation for "**E**lectronic **N**ote **B**ook".
A personal phone book in a display or application module.

EOR

Abbreviation for "**E**nd **O**f **R**ecord".
Describes the end of a data record or reporting interval.

EOS

Abbreviation for "**E**nd **O**f **S**ession".
Describes the end of a connection.

FTP

Abbreviation for "**F**ile **T**ransfer **P**rotocol".
Used for transferring files in networks, for example, for updating telephone software.

G.711

Audio protocol for uncompressed voice transmission based on the Pulse Code Modulation (PCM) procedure. Requires a bandwidth of 64 Kbps ("ISDN quality").

G.722

Audio protocol for compressed voice transmission with max. 7 kHz. Requires a bandwidth of 64 Kbps.

G.723

Audio protocol for compressed voice transmission. The quality is inferior to G.711 and G.729. Requires a bandwidth of approximately 6 Kbps.

G.729

Audio protocol for compressed voice transmission. The quality is inferior to G.711 and superior to G.723. Requires a bandwidth of approximately 8 Kbps.

Gatekeeper

A gatekeeper is a logical component of the H.323 standard that can be implemented as Windows or UNIX software, as a router option, or as a part of an MCU or a Gateway.

Gateway

A system (computer or module) that transmits data between different networks. Where necessary, gateways coordinate different protocols with each other, for example, IP network and ISDN network protocols. A gateway can also simultaneously comprise a Router.

H.323 standard

The standard consists of at least three of the following components:

- Terminals
- Gateways
- Gatekeeper
- Multipoint Control Units (MCUs)

HFA

Abbreviation for "**H**icom **F**eature **A**ccess" or "**H**iPath **F**eature **A**ccess".
Produces the connection using a gateway (for example, HG 1500 or HG 3530) between IP telephony and a PBX.

HLM

Abbreviation for "**H**iPath **L**icense **M**anagement".

HTTP

Abbreviation for "**H**yper**t**ext **T**ransfer **P**rotocol".
Protocol for transmitting data in IP networks.

INCA

Abbreviation for "**I**nterleaved **N**ative **C**ompiled **A**rchitecture".
Part of the software and hardware architecture of a workpoint.

IP

Abbreviation for "**I**nternet **P**rotocol".

IP address

Also called "IP" for short. Unambiguous address of a telephone in the network; both IPv4 and IPv6 can be used.

An IPv4 address consists of 4 number blocks, each between 0 and 255, separated by ".". Example:
1.222.44.123

An IPv6 address consists of 8 hexadecimal number blocks, separated by ":". Example:
2001:0db8:85a3:08d3:1319:8a2e:0370:7347
or, if not all blocks are used:
2000:1::3

IPSec

Abbreviation for "**I**nternet **P**rotocol **S**ecurity".

Jitter

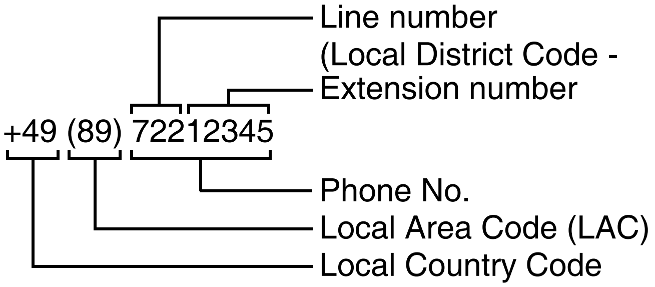
Runtime fluctuations during data transmission in IP networks.

JDBC

Abbreviation for "**J**ava **D**ata**b**ase **C**onnectivity".
JDBC is an interface that establishes a connection between a Java program and a database.

Canonical format

Example of a phone number in canonical format:



To dial phone numbers saved in canonical format, these must be made "dialable" using output rules or dialing properties. The various codes are recognized here as part of the phone number and, where applicable, replaced with the corresponding dial prefixes (see DP) or the external access code (see EA).

Examples of number resolution:

Phone number saved in canonical format:	LCC/IDP	LAC/NDP	LDC/EA	Phone number dialed
+49 (89) 722 12345	49/00	89/0	722/0	12345
+49 (89) 5593 22581	49/00	89/0	722/0	0559322581
+49 (9721) 884 6543	49/00	89/0	722/0	0097218846543
+43 (562) 2186 22415	49/00	89/0	722/0	00043562218622415
+43 (562) 2186 22415	43/00	562/0	2186/9	22415
+49 (89) 722 12345	49/00	89/0	5593/9	972212345
+49 (89) 722 12345	49/00	9721/0	5593/74	7408972212345
+49 (89) 722 12345	43/00	562/0	2186/74	7400498972212345

Table 17-1 Examples of number resolution:

KDC

Abbreviation for "**K**ey **D**istribution **C**enter".

LAN

Abbreviation for "**L**ocal **A**rea **N**etwork".

Layer 2

Second layer (data link layer) in the seven-layer OSI model for describing data transmission interfaces.

The "network access protocol" in the LAN is found in layer 2. The layer contains the access mechanism (for example, CSMA/CD in the case of Ethernet) and MAC addresses.

Layer 3

Third layer (network layer) in the seven-layer OSI model for description of data transmission interfaces.

The network protocol, for example, IP (Internet Protocol) is found on layer 3. This can unambiguously transmit data packets based on the address. Devices that perform this task are called routers.

LDAP

Abbreviation for "**L**ightweight **D**irectory **A**ccess **P**rotocol".
Simplified protocol for access to standardized directory systems, such as, a company telephone book.

LCD

Abbreviation for "**L**iquid **C**rystal **D**isplay".
Display of numbers, text, or graphics, using liquid crystal technology.

LEAP

Abbreviation for "**L**ightweight **E**xtensible **A**uthentication **P**rotocol".

LED

Abbreviation for "**L**ight **E**mitting **D**iode".
Cold-light lamp with low energy consumption and various colors.

LOGO

A graphically designed image.

Mask

The subnet mask classifies networks into A, B, and C networks. Each class has a subnet mask that masks out the relevant bits. 255.0.0.0 for class A, 255.255.0.0 for class B, and 255.255.255.0 for class C. For example, 254 → IP addresses are available in a class C network.

MAC

Abbreviation for "**M**edium **A**ccess **C**ontrol **A**ddress".
A 48-bit address with which each terminal (for example, → IP telephone or network card) unambiguously identifies itself globally in a network.

MCU

An MCU (**M**ultipoint **C**ontrol **U**nit) makes conferences possible between three or more geographically discrete stations. The MCU acts as a kind of "star distributor", which connects the telephones (known as "commercial systems") to one another.

MD5

Abbreviation for "**M**essage **D**igest". The **5** stands for a new variant of the MD algorithm. MD5 is a pure hash algorithm and generates a unique checksum comprising 128 bits (16 characters) from any data length.

MDIX

Abbreviation for "**M**ultiple **D**ocument **I**nterface".
Allows users to display one or more documents in different views within a window.

MDI-X

Abbreviation for **M**edia **D**ependent **I**nterface crossover. Allows two network devices to be connected without using a crossover cable. If auto MDI-X is available, the MDI can automatically switch between normal connection assignment and crossover assignment, depending on the connected device.

MEB

Abbreviation for "**M**edia **E**xtension **B**ridge".

MIB

Abbreviation for "**M**anagement **I**Information **B**ase".
Database that contains descriptions and error messages for devices and functions in a network.

MoH

The file contains **M**usic **o**n **H**old (waiting melody).

MWI

Abbreviation for "**M**essage **W**aiting **I**ndicator".
Signals a new message, meaning one that has not yet been read or heard.

NAT

Abbreviation for "**N**etwork **A**ddress **T**ranslation".
The source NAT (source address) and/or the destination NAT are replaced by other addresses via a router, firewall or another network component. This translation usually occurs between two networks, for example between the local network and the Internet.

OCK

A fast roaming technology made possible by 802.11i is also referred to as "**O**pportunistic **K**ey **C**aching" or "Proactive Key Caching".
If multiple Access Points share PMKs (Pairwise Master Keys), it is possible that an IP Phone changes over to an access point it has not visited before without having performed pre-authentication. The PMK that has been used with the last access point is reused thereby.

Outbound Proxy

SIP proxy (=representative) that decides in the case of a dialed SIP-URI where the outgoing call is routed.

In the following example, the registrar server is in *dom1.com* and is resolved as the IP address *w.x.y.z*; *dom2.com* is resolved as *a.b.c.d*.

Dialed URI (before proxy)	**Outbound Proxy**			

Payload

That percentage of the IP data or of an IP data package that contains the user data, such as, the voice data in the VoIP .

PBX

Abbreviation for "**P**rivate **B**ranch E**X**change".
Private telephone system that connects different internal devices to the ISDN network.

PING

Abbreviation for "**P**acket **In**ternet **G**roper".
Program for testing whether a connection can be set up to a defined IP destination. During the test, data is sent to the destination and back again. The result that is output is the success or failure of the transmission and, if applicable, additional information, such as transmission time.

Port

Ports are used to allow multiple communication connections at one time in IP networks. Different services often have different port numbers.

Proxy

A proxy server is interim memory that saves information locally.

PSK

Abbreviation for "**P**re-**S**hared **K**ey".
A passphrase that is distributed and used for authenticating encrypted communication.

PSS

Abbreviation for "**P**re-**S**hared **S**ecret".
Password for authentication in VoIP Security.

PSTN

Abbreviation for "**P**ublic **S**witched **T**elephone **N**etwork", analog telephone network or analog connections to digital network nodes, also public international telephone network.

QCU

Abbreviation for "**Q**uality **C**ontrol **U**nit".

QDC

Abbreviation for "**Q**uality **D**ata **C**ollection".
Concept for centrally collecting data on the quality of voice connections via IP networks.

QoS

Abbreviation for "**Q**uality **o**f **S**ervice".
Describes the subjectively detectable quality of a voice connection over IP networks. QoS properties are packet loss rate, packet delay, delay variation, reserved bandwidth, type of bit rate (variable, constant, or unspecified bit rate), and the bit rate.

RADIUS

Abbreviation for "**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice".
Protocol or software for user authentication via dial-up lines.

RAM

Abbreviation for "**R**andom **A**ccess **M**emory".
Memory with read/write access.

RCC

Abbreviation for "**R**outing **C**ontrol **C**enter".
If central routing is used in a network, individual network nodes transmit local route information to the RCC in regular intervals. The RCC saves this information and uses its global network knowledge to calculate the best routes between nodes.

Regular expression

Character string that uses specific syntactic rules to describe a set or subset of character strings. Regular expressions are firstly a type of text-based filter criterion that compares the expression in the form of a pattern with the text. For instance, it lets your find all character strings starting with 1 or 2, without having to enter any subsequent digits. Secondly, you can use regular expressions as a type of template for generating sets of digit combinations without having to specify each individual digit combination.

ROM

Abbreviation for "**R**ead **O**nly **M**emory".
Memory with read-only access.

Router

Routers set up connections to gateways and have access to several subnets and other routers. Using the IP address, a router determines the subnet or other router to which it should send data. It decides which path is the most favorable for the data at a given time.

RSM

Abbreviation for "**R**ealtime **S**ervice **M**anager".

RTC

Abbreviation for "**R**eal-**T**ime **C**ommunications Server" from Microsoft.

RTS

Abbreviation for "**R**eady **T**o **S**end).
This transmission request is part of modem control and is also used in the collision-free access procedure CSMA/CA (as implemented in 802.11). In modem control, the RTS signal is used in handshake mode as a control signal between a modem and a digital device that initiates data transmission via the transmission line.

SDLP

Abbreviation for "**S**tandard **D**evice **L**evel **P**rotocol".

SHA1

Abbreviation for "**S**ecure **H**ash **A**lgorithm". The **1** indicates a newer version. SHA1 is a hash algorithm and generates a checksum of 160 bits (20 characters) out of data lengths under 264 bits.

SIP

Abbreviation for "**S**ession **I**nitiation **P**rotocol".
Protocol standard for initializing calls in IP networks.

SNMP

Abbreviation for "**S**imple **N**etwork **M**anagement **P**rotocol".
The protocol is used for communicating with servers that take on network management functions. For example, this includes logging errors that occur on network components (SNMP trap).

SNTP

Abbreviation for "**S**imple **N**etwork **T**ime **P**rotocol".
The protocol is used between time servers and telephones in a network in order to synchronize the time on the telephones.

SPA

Abbreviation for "**S**oftware **P**roduct **A**ssurance".

SQL

Abbreviation for Structured Query Language. This is programming language that was developed by IBM to retrieve information from relational databases (for example, Microsoft Access). Particular emphasis was placed on client/server environments (a client sends a request, the server provides the relevant information) during development.

SRSR

Abbreviation for "**S**mall **R**emote **S**ide **R**edundancy".
Indicates that a redundancy system is available.

SRTP

Abbreviation for "**S**ecure **R**ealtime **T**ransport **P**rotocol".
Protocol for the secure transmission of multimedia data via symmetrical encryption.

SSID

Abbreviation for "**S**ervice **S**et **ID**entifier".
Network name in a WLAN.

SSL

Abbreviation for "**S**ecure **S**ocket **L**ayer".
Technology for encrypted data transmission between client and server using authentication.

SSSO

Abbreviation for "**S**ecure **S**ingle **S**ign **O**n".
Access to the DLS is password-protected. The SSSO and all information in the DLS are transmitted in encrypted form using SSL.

Switch

Switching center in a star-shaped network, for example, HiPath 4000 system.

TAP

Abbreviation for "**T**echniker **A**rbeits**P**latz" (EWS - Engineering Workstation).

TCP

Abbreviation for "**T**ransmission **C**ontrol **P**rotocol".
Along with IP, this is the main protocol on the Internet. It provides a reliable, connection-oriented, full duplex service in the form of a data flow.

TKIP

Abbreviation for "**T**emporal **K**ey **I**ntegrity **P**rotocol".
Algorithm for encryption in WLANs.

TLS

Abbreviation for "**T**ransport **L**ayer **S**ecurity".
Standard protocol for performing computer authentication using certificates and encryption.

TTL

Abbreviation for "**T**ime **T**o **L**ive".
This value specifies the lifespan of an IP data packet. Data packets transferred in IP networks can take different routes to reach their destination. Every time the data packet moves to a new network it passes a router which decrements the packet’s TTL value by one. The packet is discarded when the value reaches 0. This ensures that packets that are unable to find their des-

tination despite lengthy searches do not drift around the Internet ad infinitum. The higher the original TTL value of a data packet, therefore, the longer the packet can try to reach its destination.

UDP

Abbreviation for "**U**ser **D**atagram **P**rotocol".
Can be used as an alternative to TCP if there are no requirements in terms of reliability. UDP does not guarantee to deliver packets or supply them in a particular sequence.

URI/URL

Abbreviations for "**U**niform **R**esource **I**dentifier" and "**U**niform **R**esource **L**ocator".
These are the address of a file or a directory. The most common form of a URI is a URL. A typical URI indicates:

- the mechanism for accessing the contents (for example, a protocol such as http, ftp, or file).
- the computer where the contents can be found, and
- the specific name of the contents on this computer (usually a file name).

The parts are optional with the result that a file name is in itself a URL (even a relative one).

DP

Abbreviation for "**D**ial **P**refix".
A distinction is made between the national DP (NDP or National Dial Prefix) and the international DP (IDP or International Dial Prefix). For example, the national DP for Munich is the "0" in "**0**89". See also Canonical format.

VLAN

Abbreviation for "**V**irtual **L**ocal **A**rea **N**etwork".
Subdivision of an IP network into autonomous administration groups (domains). An option for identifying VLAN membership is by using a VLAN ID.

VLAN is, therefore, a network structure with all the properties of a conventional LAN but without any physical connections. In contrast to LANs where the distances between stations are subject to restriction, VLANs allows nodes that are further apart to be combined into a virtual local network.

VoIP

Abbreviation for "**V**oice **o**ver **IP**".
This refers to voice transmission using IP technology.

VoIP Security

Abbreviation for "**V**oice **o**ver **IP S**ecurity".
This describes measures for secure VoIP voice transmission.

VPN

Abbreviation for "**V**irtual **P**rivate **N**etwork".
A VPN connects two networks, a computer, and a network or two computers via public connections (for example, the Internet).
A tunneling protocol encrypts and decodes transmitted data to ensure that it cannot be accessed by unauthorized parties.
This technology was developed to cut costs as it is considerably cheaper for field workers to send data to headquarters via public lines than to create individual networks.

WAP

Abbreviation for "**W**ireless **A**pplication **P**rotocol".
This also refers to graphic applications on mobile telephones, organizers, and other suitable terminals that are transmitted using the protocol of the same name.

WBM

Abbreviation for "**W**eb-**B**ased **M**anagement".
A Web-based workpoint (IP phone) interface for administering configurations and modifying user settings via remote access.

WEP

Abbreviation for "**W**ired **E**quivalent **P**rivacy".
Standard encryption for WLANs. All stations in a WLAN and the access point or WLAN router use the same key for encrypting and decoding data. WEP distinguishes between 64- and 128-bit encryption.

See also WPA, WPA-PSK.

WLAN

Abbreviation for "**W**ireless **L**ocal **A**rea **N**etwork".

Workpoint

Workpoint is a term for both IP telephones, such as, optiPoint 410 standard, and soft clients, such as optiClient 130.

WPA

Abbreviation for "**W**I-FI **P**rotected **A**ccess".
WPA provides security in WLANs by using dynamic keys for encryption. When a connection or session is set up, dynamic keys are exchanged via the Extensible Authentication Protocol (EAP).

See also WEP, WPA-PSK.

WPA-PSK

Abbreviation for "**W**I-FI **P**rotected **A**ccess with **P**re-**S**hared **K**ey".
An encryption procedure for WLANs. This procedure uses station-specific keys made up of a pre-shared key and the MAC address of each device. These keys are automatically updated at regular intervals (rekeying intervals)

See also WEP, WPA.

WSP

Abbreviation for "**W**ireless **S**ession **P**rotocol".
Protocol for transmitting data on WAP-compatible telephones.

Index