ADMINISTRATOR GUIDE

Software 1.3.0 | September 2017 | 3725-84593-001D

Polycom® CX5100 Unified Conference Station for Skype™ for Business

6001 America Center Drive
San Jose, CA 95002
USA

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

End User License Agreement BY USING THIS PRODUCT, YOU ARE AGREEING TO THE TERMS OF THE END USER LICENSE AGREEMENT (EULA) AT: http://documents.polycom.com/indexes/licenses. IF YOU DO NOT AGREE TO THE TERMS OF THE EULA, DO NOT USE THE PRODUCT, AND YOU MAY RETURN IT IN THE ORIGINAL PACKAGING TO THE SELLER FROM WHOM YOU PURCHASED THE PRODUCT.

Patent Information The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Polycom Support Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

Before You Begin

This *Polycom CX5100 Unified Conference Station for Microsoft Skype for Business - Administrator Guide* uses a number of conventions that help you to understand information and perform tasks.

Who Should Read this Guide?

This user guide contains overview information for the Polycom® CX5100 Unified Conference Station for Microsoft® Skype™ for Business. This guide is intended for beginning users, as well as intermediate and advanced users who want to learn more about their system features.

Typographic Conventions

The following table lists the typographic conventions are used in this guide to distinguish different types of information.

Typographic Conventions Used in this Guide

Convention	Description
Blue	Used for cross-references to other information in this document and links to external web pages or documents.
Italics	Used to emphasize text, to show example values, and to show titles of reference documents.
Bold	Indicates interface items such as menus, soft keys, file names, directories, and text you need to enter.
Menu > Submenu	Indicates a series of menu choices. For example, **Administration > System** Information indicates that you should select the Administration menu and then select System Information.

Related Documentation

For additional information about the Polycom CX5100 Unified Conference Station, view the following documentation on the Polycom CX5100 support page:

- *Quick Tips*—A quick reference on how to use the system's most basic features.
- *Setup Sheet* —This guide describes the contents of your package, how to assemble the system or accessory, and how to connect the system to the network. The quick start guide is included in the unified conference station package.
- *Regulatory Notice*—This guide provides information for all regulatory and safety guidance.

Getting Started with the Polycom CX5100 Unified Conference Station

The CX5100 unified conference station provides integrated cameras, a speaker, and microphones on one device. You can use the unified conference station to place audio and video calls made using Microsoft Skype for Business, Lync 2013, Lync 2010, or Lync for Mac.

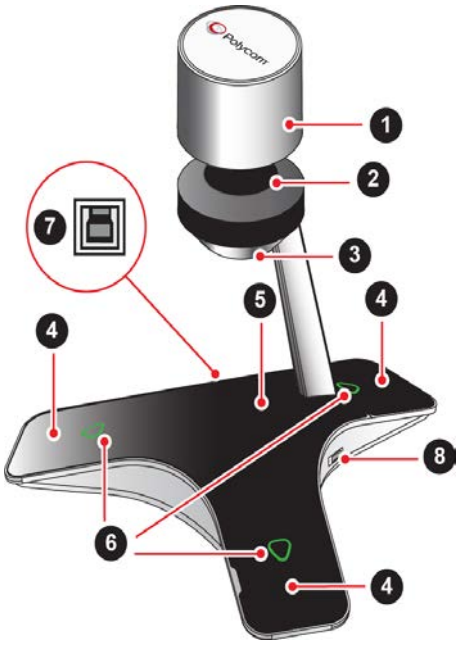
When your CX5100 unified conference station is connected to a computer running Skype for Business or Lync client, the unified conference station provides a 360-degree view of the conference room and automatically identifies the active speaker.

Note: For Mac OS computers connected to the CX5100 unified conference station, the panoramic view is now supported as an overlay in the active speaker video stream.The panoramic view of meeting participants is supported only when the UVC output resolution is 720p or 1080p.

CX5100 Hardware and Keys

Use the following figures and tables to understand your CX5100 Unified Conference Station hardware features. For more information about attaching hardware, see the *Setup Sheet for the CX5100 Unified Conference Station* available on Polycom Voice Support.

CX5100 unified conference station



CX5100 Hardware Feature Descriptions

Feature	Description
1	Camera cover
2	Cameras
3	Active video indicator
4	Microphones
5	Speaker
6	Microphone mute buttons
7	USB 3.0 Type B connection to computer
8	USB 2.0 connector for memory stick

Status Indicators

The CX5100 unified conference station has status indicators to let you know the status of the unified conference station, including when the unified conference station is sending audio or video in video calls.

Microphone Indicators and System Status

Microphone Indicator	System State
Off	Not in a call
Green	In call
Green flashing	Ringing
Green slow flashing	System is starting up
Red	In call with microphones muted
Red flashing	Ringing with microphones muted On hold
Green/red flashing	Software update in progress
Amber flashing	POST check failed.

Active Video Indicator and System Status

Active Video Indicator	System State
Off	Not in a call No video in a call

Active Video Indicator and System Status

Active Video Indicator	System State
Green	In call with active video
Flashing	Privacy cap is closed

Tips for Setting Up the Room

Follow these best practices listed below when setting up the CX5100 unified conference station in a conference room.

- Place the unified conference station in a large conference room, rather than a small room.
- If the room has hard walls or large windows, consider installing sound-absorbing panels and window blinds or drapes.
- Place the unified conference station in the center of the table, and place the table in the center of the room.
- If wall displays are part of the room’s setup, move the unified conference station closer to the displays.
- Place the unified conference station so that participants are speaking toward the microphones. Avoid placing the unified conference station so that participants speak away from the microphones.

Minimum Requirements for a Laptop Connected to the CX5100 Unified Conference Station

The CX5100 unified conference station's performance can vary based on the connected laptop, network connection, and the Skype for Business client version. Check that the connected laptop meets the minimum hardware and software requirements listed in the following table before connecting to the CX5100 unified conference station.

Minimum Computer Hardware and Software Requirements

Category	Requirements
Windows	Windows 8.1 (32-bit or 64-bit) Windows 8 (32-bit or 64-bit) Windows 7 (32-bit or 64-bit)
Mac	OS X Mavericks (version 10.9) OS X Yosemite (version 10.10) OS X El Capitan (version 10.11) OS X Sierra (version 10.12)

Minimum Computer Hardware and Software Requirements (Continued)

Category	Requirements
Desktop Client	Microsoft Skype for Business 2016 Microsoft Skye for Business for Mac, version 16.x.x Microsoft Skype for Business 2015 Microsoft Lync 2013 or Skype for Business 2013 (recommended) Microsoft Lync 2010 Microsoft Lync for Mac 14.3.3 (160216), with native Safari web access
Processor	Basic Video Transmit – 2.0 GHz or higher HD Transmit – Quad cores, 2.0 GHz or higher For the Skype for Business 2015 client, you can find detailed system requirements on the Skype for Business Server 2015 page. For the Skype for Business 2013 client, you can find detailed system requirements on the Skype for Business Server page.
RAM	2 GB
Hard drive space	1.5 GB
Video card	Minimum 128 MB RAM with support for full hardware acceleration
Monitor	Minimum 1024 x 768
USB Connector	A USB 3.0 port is required for 1080p calling. Connecting the unified conference station to a USB 2.0 or USB 1.0 port can result in reduced performance.

Note: If you use a third-party USB extension cable to increase the distance between the CX5100 unified conference station and the PC, be aware that most extension cables limit the data rate or provide only USB 2.0 performance, even when plugged into a USB 3.0 port.

When you connect the CX5100 to your computer using a USB 2.0 port, a warning message stating that your system can run faster displays.

Provision the CX5100 Unified Conference Station

This section explains methods you can use to provision and configure features on the CX5100 unified conference station. You can use one or multiple methods at the same time but note that features and settings vary by configuration method and by device.

It is important to be aware that there is a configuration priority among the methods when you use multiple methods at the same time—settings you make using a higher priority configuration method override settings made using a lower priority configuration method. When using multiple configuration methods, a setting you make using a lower-priority method does not apply to or override a duplicate setting made using a higher-priority method.

- **Web Configuration Utility** This method provisions and configures features for one system at a time and is recommended for device deployments of fewer than 20 devices. This method enables you to provision and configure systems using a web browser and enables you to manage systems remotely. However, note that the Web Configuration Utility contains a limited number of settings. Settings you make using the Web Configuration Utility override settings you make on the central provisioning server.
- **Centralized provisioning** Use this method for large-scale device deployments. This method requires you to set up your own provisioning server if your SIP call server does not provide one. Settings you make from a central provisioning server override default device and software settings.
- **RealPresence Resource Manager** This method allows you to provision the CX5100 unified conference station and perform the following operations:
  - Software Upgrade
  - Monitoring the online/offline device
  - Provisioning

Provisioning Points to Consider

- If you are provisioning multiple systems, Polycom recommends that you set up a provisioning server to install and maintain your Polycom systems, as shown in the section Using Centralized Provisioning.
- A provisioning server maximizes the flexibility you have when installing, configuring, upgrading, and maintaining the systems, and enables you to store configuration, log, directory, and override files on the server. If you allow the system write access to your provisioning server, the system can use the server to upload all of the file types and store administrator and user settings.
- Polycom systems boot up without the use of configuration files. You can specify a SIP server address and a registration address (the equivalent of a system number) in a configuration file before or after the system boots up, or from the Web Configuration Utility.

- If a system cannot locate a provisioning server upon boot up, and has not been configured with settings from any other source, it operates with internally stored default values. If the system that cannot locate a provisioning server has previously been configured with settings it operates with those previous settings.
- Each system may open multiple connections to the server.
- Settings available only to administrators require a password and are not available to users. Non-administrative users cannot duplicate or override administrator-level settings.

Note: Polycom recommends that you use RFC-compliant servers.

Using the Web Configuration Utility

The Web Configuration Utility is a web-based interface that is useful for remote provisioning and configuration. This utility allows you to update the software and configure the phone's current settings. You can either import the settings in a configuration file to the phone or export a configuration file containing phone's current settings to your computer to make changes.

Note: The Web Configuration Utility does not contain all of the settings available with centralized provisioning. Polycom recommends using centralized provisioning as your primary provisioning method when provisioning more than 10 to 20 phones.

There is a priority order when using multiple methods concurrently to provision and configure features. Settings you make from the Web Configuration Utility override settings you make on the central provisioning server and can be overridden by settings you configure from the phone menu. If you want to remove settings applied from the Web Configuration Utility, click the Reset to Default button on any page in the Web Configuration Utility.

For more detailed help using the Web Configuration Utility, see the *Polycom Web Configuration Utility User Guide* on Polycom UC Software Support Center.

Import Configuration Files to the Phone

You can import the changes made to the current phone's settings and configuration files by you from your computer to another phone using the Web Configuration Utility.

To import configuration files to the phone:

1. Find your phone's IP address on your phone's keypad or touchpad interface.
2. Enter the phone's IP address into the address bar of a web browser from your computer.
3. Choose your login option as **Admin** on the Web Configuration Utility login screen and enter the corresponding password (default 456).
4. Go to **Utilities > Import & Export Configuration > Choose File**.
5. Choose the configuration files from your computer to upload.

6 Click **Import**.

The Web Configuration Utility imports the selected file to your phone.

Export Configuration Files from the Phone

You can export the phone's configuration file to your computer and make changes to the phone's current settings. You can apply these settings to another phone by importing the configuration files using the Web Configuration Utility.

To export the configuration files to your computer:

1 Find your phone's IP address on your phone's keypad or touchpad interface.

2 Enter the phone's IP address into the address bar of a web browser from your computer.

3 Choose your login option as **Admin** on the Web Configuration Utility login screen and enter the corresponding password (default 456).

4 Navigate to **Utilities > Import & Export Configuration**.

5 Choose the files to export from the drop-down list of **Export Configuration file** under **Export Configuration** pane.

6 Click **Export**.

The Web Configuration Utility exports the selected file to your computer.

Using Centralized Provisioning

The software that you download contains template configuration files and valid XML files that you can modify using an XML editor. The configuration files enable you to maintain a set of configuration files for all your devices on a central provisioning server and configure all of your systems to read the same set of files.

The software package contains template configuration files that are flexible and enable you to rearrange the parameters within the template, move parameters to new files, or create your own configuration files from parameters you want. This flexibility is especially useful when you want to apply a set of features or settings to separate groups of systems. You can create and name as many configuration files as you want and your configuration files can contain any combination of parameters.

Note: Remember that settings made from the Web Configuration Utility override settings you make in configuration files using centralized provisioning.

Centralized provisioning requires that the system be able to read files and directories you list in the master configuration file. In addition, the system attempts to upload log files (log files provide a history of system events), a configuration override file, and a provisioning directory file to the provisioning server. Though not required, Polycom recommends configuring a separate directory for each of these files to help organize: a log file directory, an override directory, and a license directory.

Each directory can have different access permissions, however, where the security environments permits, Polycom recommends that you allow these file uploads to the provisioning server which requires you to give delete, write, and read permissions for the system's server account. All other files that the system needs to read, such as the application executable and the standard configuration files, should be made read-only

using file server file permissions. Ensure that the file permissions you create provide the minimum required access and that the account has no other rights on the server. Without permissions, the system cannot upload files.

Note: Allowing file uploads can help Polycom provide customer support when diagnosing issues with the system.

Setting Up the Provisioning Server

This section provides instructions for setting up a centralized provisioning server for your Polycom systems. Polycom systems support the FTP, TFTP, HTTP, and HTTPS protocols, and use FTP by default. The example shown in this section uses FTP and a personal computer (PC) as the provisioning server.

Prerequisites

To begin, install and set up tools on your PC and gather some information:

- Install an XML editor, such as XML Notepad 2007, on your computer.
- Install an FTP server application on your computer. FileZilla and *wftpd* are free FTP applications for windows and *vsftpd* is typically available with all standard Linux distributions.
- Take note of the following:
  - **MAC address** Each system has a unique 12-digit serial number just above the system's bar code on a label on the back of the system. Collect the MAC address for each system in your deployment.
  - **Your computer's IP address** To use your computer as the provisioning boot server, you need your computer's IP address. Jot this number down as you need it at the end of the provisioning process.

Configure Multiple Servers

You can configure multiple (redundant) provisioning servers—one logical server with multiple addresses—by mapping the provisioning server DNS name to multiple IP addresses. The default number of provisioning servers is one and the maximum number is eight.

If you set up multiple provisioning servers, you must be able to reach all of the provisioning servers with the same protocol and the contents on each provisioning server must be identical. You can configure the number of times each server is tried for a file transfer and also how long to wait between each attempt. You can configure the maximum number of servers to be tried. For more information, contact your certified Polycom reseller.

Deploy Devices from the Provisioning Server

After setting up your provisioning server, deploy your devices.

To deploy systems with a provisioning server:

1 Using the list of MAC addresses of each system you are deploying, create a per-system **system<MACaddress>.cfg** file.

Do not use the following file names as your per-system file name: <*MACaddress*>-system.cfg, <*MACaddress*>-web.cfg, <*MACaddress*>-app.log, <*MACaddress*>-boot.log, or <*MACaddress*>-license.cfg. These file names are used by the system to store overrides and logging information.

Note: If SNTP settings are not available through DHCP, you need to edit the SNTP GMT offset, and possibly the SNTP server address for the correct local conditions. Changing the default daylight savings parameters might be necessary outside of North America. If the local security policy dictates you might need to disable the local Web (HTTP) server or change its signaling port.

2 Create a master configuration file by performing the following steps:

a Enter the name of each per-system and per-site configuration file created in steps 2 and 3 in the `CONFIG_FILES` attribute of the master configuration file (**000000000000.cfg**). For help using the master configuration file, see the section Use the Master Configuration File.

For example, add a reference to **system<*MACaddress*>.cfg**.

b (Optional) Edit the `LOG_FILE_DIRECTORY` attribute of master configuration file to point to the log file directory.

3 Perform the following steps using the Web Configuration Utility (see Using the Web Configuration Utility) to configure the system to point to the IP address of the provisioning server:

a In the Web Configuration Utility, navigate to **Settings > Provisioning Server**.

b Select a **Server Type**. The default value is **FTP**.

c For **Server Address**, enter the address of your provisioning server.

d Enter the **Server User** and **Server Password** of the account you created on your provisioning server. For example, `bill1234` and `1234`, respectively.

e Under the **DHCP Menu**, select **Static** for the **Boot Server**

f Set any additional settings for your provisioning server.

g Click **Save**.

The system reboots and the software modifies the master configuration file so that it references the appropriate software and configuration files.

After this step, the system reads the unmodified attribute. Then, the system sends a DHCP Discover packet to the DHCP server. You can locate this in the Bootstrap Protocol/option 'Vendor Class Identifier' section of the packet which includes the system's part number and the BootROM version.

4 Monitor the provisioning server event log and the uploaded event log files to ensure that the configuration process completed correctly. All configuration files used by the provisioning server are logged.

The system uploads two logs files to the LOG_DIRECTORY directory: **<*MACaddress*>-app.log** and **<*MACaddress*>-boot.log**.

Override Files

When using a central provisioning server as part of your environment, you have the option to store the override file to the system, or you can permit the system to upload the override file to the provisioning server by giving the system write access to the provisioning server.

The advantage of allowing the system write access to the provisioning server for override files is that user settings for a system survive restarts, reboots, and software upgrades you apply to all systems using a provisioning server. You can also use the override files to save user custom preferences and to apply specific configurations to a device or device group. If you permit the system to upload to the provisioning server, the override file is by default named either **<*MAC Address*>-system.cfg** or **<*MAC Address*>-Web.cfg** depending on the whether the change was made from the system or Web Configuration Utility respectively.

Note: Changes to settings using a configuration method having a higher priority than another create an override file that is uploaded to your provisioning server directory. The order of priority is as follows: `<MAC Address>-system.cfg` overrides `<MAC Address>-Web.cfg`

Both override files override settings you make from the provisioning server. The system uploads an override file each time a configuration change is made from the system. If you reformat the system's file system, the override file is deleted.

Use the Master Configuration File

The centralized provisioning method requires you to use a master configuration file, named **00000000000.cfg** in the software package.

You can apply the master configuration file to systems in the following ways:

- **To all systems** If you are applying the same features and settings to all systems, you can use the default master configuration file to configure all the systems in a deployment. Note that the systems are programmed to look first for their own **<*MACaddress*>.cfg** file and if a system does not find a matching file, it looks next for the default file named **000000000000.cfg**. If you do create and use a per-system master configuration file, make a copy of the default file and rename it.
- **To a system group or to a single system** If you want to apply features or settings to a group of systems or to a single system, make a copy of the default master configuration file and rename it. You can specify a device group by model or part number.

  For single systems, rename the file with a naming scheme that uses the system's MAC address **<*MACaddress*>.cfg**. Note that you can use only lower-case letters, for example, **0004f200106c.cfg**. You can find the MAC address of a system on a label on the back of the system or in the CX5100-CX5500 Control Panel.
- **Specify a location** You can specify the location of a master configuration file you want the systems to use, for example, `http://usr:pwd@server/dir/example1.cfg`. The file name must be at least five characters long and end with **.cfg**. If the system cannot find and download a location you specify, the system searches for and uses a per-system master configuration file and then the default master configuration file.

Note: Do not use the following names as extensions for per-system files: <*MACaddress*>-system.cfg, <*MACaddress*>-Web.cfg, <*MACaddress*>-app.log, <*MACaddress*>-boot.log, or <*MACaddress*>-license.cfg. These filenames are used by the system to store override files and logging information.

The following describes the XML field attributes in the master configuration file.

- **CONFIG_FILES** Enter the names of your configuration files here as a comma-separated list. If you want to use a configuration file in a different location or use a different file name, or both, you can specify a URL with its own protocol, user name and password, for example: `ftp://usr:pwd@server/dir/system2034.cfg`.

Note: The order of the configuration files listed in CONFIG_FILES is significant:

- The files are processed in the order listed (left to right).
- If the same parameter is included in more than one file or more than once in the same file, the system uses the first (left) parameter.

- **MISC_FILES** A comma-separated list of files. Use this to list volatile files that you want systems to download. The system downloads files you list here when booted, which can decrease access time.
- **LOG_FILE_DIRECTORY** An alternative directory for log files. You can also specify a URL. This field is blank by default.
- **OVERRIDES_DIRECTORY** An alternative directory for configuration overrides files. You can also specify a URL. This field is blank by default.
- **LICENSE_DIRECTORY** An alternative directory for license files. You can also specify a URL. This field is blank by default.
- **COREFILE_DIRECTORY** An alternative directory for Polycom device core files to use to debug

Using RealPresence Resource Manager to Provision CX5100 System

The CX5100 and CX5500 unified conference stations can be dynamically managed in the RealPresence Resource Manager system, which provides the secure way to remotely provision and upgrade CX5100 and CX5500 systems as other dynamically managed Polycom video endpoints. The dynamic management from the RealPresence Resource Manager system is client-to-server over HTTPS which makes it more secure and firewall-friendly.

This function allows you to perform the following operations from the RealPresence Resource Management server:

- **Software upgrade** - Allows you to update the CX5100 and CX5500 system’s software from the RealPresence Resource Manager portal as can be done with other dynamically managed video endpoints.
- **Monitoring the online/offline device** - Allows you to monitor the CX5100 and CX5500 system's online or offline status together with the endpoint details including, but not limited to name, IP address, MAC address, and software version.
- **Provisioning** - Allows you to change the basic CX5100 and CX5500 system’s settings from the RealPresence Resource Manager including, but not limited to time zone, time format, and time server.

The RealPresence Resource Manager provisioning does not support the base profile set to **Skype** for the CX5100 system. Make sure to set the base profile to **Generic**.

The following parameters support the RealPresence Resource Manager to provision the CX5100 system:

- `tcpIpApp.sntp.daylightSavings.enable`

- `lcl.datetime.time.24HourClock`
- `tcpIpApp.sntp.address`
- `tcpIpApp.sntp.address.overrideDHCP`
- `tcpIpApp.sntp.gmtOffset`
- `tcpIpApp.sntp.gmtOffset.overrideDHCP`
- `device.prov.serverName.set`
- `device.prov.serverName`
- `device.masterConfigFile.LogFileDirectory`

For more information on these parameters, see *Configuration Parameter* section in the *Polycom® CX5500 Unified Conference Station for Skype™ for Business Administrator Guide*

Configure the RealPresence Resource Manager to Provision the CX5100 System

Before you begin to configure the RealPresence Resource Manager (RPRM) to provision the CX5100 unified conference station, make sure you do the following:

- The `device.prov.lyncDeviceUpdateEnabled` parameter value must be set to 0.

  You can also export the CX5100 system device settings configuration file through Web Configuration Utility to set the value of the parameter.
- The **Base Profile** for the CX5100 unified conference station is set to **Generic**.
- The RealPresence Resource Manager, 10.1 and above, supports provisioning the CX5100 unified conference station.

Note: You won't find the `device.prov.lyncDeviceUpdateEnabled` parameter in the CX5100 system's device settings configuration file if the value of this parameter is already set to 0.

You can configure the RPRM server to provision the CX5100 system, allowing you to perform a software upgrade and monitor the online/offline devices using the following methods:

- Provision the CX5100 system using FTP
- Provision the CX5100 system using the Web Configuration Utility

Provision the CX5100 System using FTP

You can configure the RPRM server to provision the CX5100 system through FTP by storing the configuration files in the FTP root directory.

To provision the CX5100 system using FTP:

1. Configure the FTP server address, username and password to store configuration files.
2. Prepare the following files to configure RPRM as the management server:
   - *<MACaddress>.cfg*

- CustomizedProfile.cfg

If the configuration files are already available on the FTP server, download the files to your system.

3. Edit the *<MACaddress>.cfg* file name with the systems MAC address.
4. Save the *<MACaddress>.cfg* file.
5. Edit the following parameters in the CustomizedProfile.cfg file with the RPRM server details:

   `device.cma.serverName`

   `device.logincred.user`

   `device.logincred.password`
6. Save the CustomizedProfile.cfg file.
7. Copy the following configuration files to the FTP root directory:
   - *<MACaddress>.cfg*
   - CustomizedProfile.cfg
8. Login to the RPRM server to view the CX5100 systems status.

   For more information on configuring the FTP server, see Setting Up the Provisioning Server.

Provision the CX5100 System using the Web Configuration Utility

You can configure the RPRM server to provision the CX5100 system using Web Configuration Utility by importing the edited configuration file to the CX5100 system.

To provision the CX5100 system using the Web Configuration Utility:

1. Prepare the following file to configure RPRM as the management server:
   - CustomizedProfile.cfg
2. Edit the following parameters in the CustomizedProfile.cfg file with the RPRM server details:

   `device.cma.serverName`

   `device.logincred.user`

   `device.logincred.password`
3. Save the CustomizedProfile.cfg file.
4. Login to the Web Configuration Utility of CX5100 system and navigate to **Settings > Utilities > Import & Export Configuration > Import Configuration.**
5. Click **Choose File** and select the edited CustomizedProfile.cfg file.
6. Click **Import**.
7. Login to the RPRM server to view the CX5100 systems status.

   For more information on Web Configuration Utility, see Using the Web Configuration Utility.

Use the CX5100-CX5500 Control Panel

You can customize settings for each CX5100 unified conference station using the CX5100 - CX5500 Control Panel application running on a Microsoft Windows computer connected to the unified conference station. You can also use the Web Configuration Utility to customize a subset of features available for the CX5100 (see Using the Web Configuration Utility).

Install the CX5100 - CX5500 Control Panel

The Polycom CX5100/CX5500 Control Panel enables you to change a limited group of settings for the unified conference station when connected to a Windows computer.

You can download the Polycom CX5100-CX500 Control Panel application from the Polycom CX5100 support page.

To install the CX5100 - CX5500 Control Panel:

1. Download the Control Panel installation file from Polycom CX5100 onto a computer.
2. Double-click the installation file and follow the prompts to install the application.

After you install the Control Panel, you can connect the unified conference station to your computer and create a profile for CX5100 unified conference station, view system information, change settings, view diagnostics, and retrieve logs.

The Default System Password

In order to make changes to the CX5100 unified conference station using the Control Panel, you need to enter the system password. By default, the password is the 14-digit serial number of the unified conference station. You can find the serial number on the label on the back panel of the power data box, as shown in the following figure.

Location of the Serial Number Label on the Power Data Box

After you enter the default password, you can change the unified conference station's password on the System tab in the Control Panel.

Change the Default Password

By default, the default password to change any setting for the CX5100 unified conference station is the 14-digit serial number of the unified conference station. After you enter the default password the first time, you can choose a new system password.

To change the default system password:

1. In the Control Panel, click **System > Password**.
2. Enter the default password in the **Old Password** field.
3. Enter a new password for the unified conference station in the **New Password** field and retype the new password in the **Confirm New Password** field.
4. Click **Change Password**.

   Your new password is saved for the unified conference station and you can enter your new password when you need to make changes to your CX5100 unified conference station.

Create a System Profile

The Profile Editor in the Control Panel enables you to change device settings and update software. The following table shows the network settings you can configure in the Profile Editor and save onto the CX5100 unified conference station.

Contact your system administrator before changing the power frequency settings for your CX5100 unified conference station.

Network Configuration Settings

Setting	Description
Device Name	Displays the Device Name on the Diagnostics page. Naming your CX5100 helps you manage multiple devices.
Enable Ethernet	Enables the unified conference station to connect to the network by Ethernet. You must enable Ethernet before you can configure the unified conference station for automatic software updates.
Enable DHCP	Enables the unified conference station to use Dynamic Host Configuration Protocol (DHCP) to obtain the IP Address, Default Gateway, Subnet Mask, and Preferred and Alternate DNS Server settings automatically.
Enable EAP/802.1x	Enables the unified conference station to use 802.1X authentication. You must Enter the Host Name, Domain Name, EAP Identity, and the EAP passwords manually.

To create a system profile:

1. Connect the USB cable from the CX5100 to your computer.
2. On your computer, start the **CX5100 - CX5500 Control Panel** application.

   The Control Panel opens and your device's system information displays in the System tab.

3 In the Control Panel, click **Profile Editor**.

The Enter Device Password dialog box displays.

4 Enter the **Device Password** and click **OK**.

5 On the **Network** tab, enter a **Device Name**.

6 Select **Enable Ethernet**, and choose to **Enable DHCP** or **Enable EAP 802.1x**.

7 On the **Time** tab, select your **Time Zone**, enable a **Time Server,** and enter the **NTP Server Address**.

8 On the **Software Update** tab, enter the name of the **Update Server** and select values for the **Update Frequency** and **Update Time**.

9 On the **Advanced** tab, choose the **Mute Button Function**. Select **Microphone only** to mute the audio only or select **Microphone and Camera** to mute the audio and video when you touch the Mute button.

10 On the **Advanced** tab, select the **Power Frequency** for the unified conference station.

11 Click **Apply to Device** to save the profile to the CX5100 unified conference station.

Save a System Profile

After you create a system profile, you can save the profile onto your computer to load the profile onto another CX5100.

To save a profile:

1 Connect the USB cable from the CX5100 to your computer.

2 On your computer, start the **CX5100 - CX5500 Control Panel** application.

The Control Panel opens and your device’s system information displays in the System tab.

3 In the Control Panel, click **Profile Editor**.

The Enter Device Password dialog box displays.

4 Enter the **Device Password** and click **OK**.

5 In the **Profile Editor** tab, click **Save to File (PC)** to save the profile to your computer.

6 Enter a name for the file and select the location of where to save the profile.

7 Click **Save**.

Load a System Profile

You can load a profile from a CX5100, a saved profile from your computer, or a default system profile onto the CX5100.

To load a system profile:

1 Connect the USB cable from the CX5100 to your computer.

2 On your computer, start the **CX5100 - CX5500 Control Panel** application.

The Control Panel opens and your device’s system information displays in the System tab.

3 In the Control Panel, click **Profile Editor**.
The Enter Device Password dialog box displays.
4 Enter the **Device Password** and click **OK**.
5 In the **Profile Editor** tab, click **Load Profile**.
6 Select one of the following options:
- **Load from Device**—uploads the profile saved on the CX5100.
- **Load from File (PC)**—uploads a profile saved on your computer onto the CX5100.
- **Load Default Profile**—uploads the factory default profile for the CX5100.

7 After you make your selection, click **Apply to Device**.
The profile is saved onto the CX5100.

Configure Mac OS Support

The CX5100 unified conference station is supported on Microsoft Windows and Mac OS computers. By default, the CX5100 automatically detects the operating system of a connected computer and integrates with the Lync or Skype for Business client. For Mac OS computers, Active Speaker and panoramic view is supported.

Users can connect the CX5100 to a Mac computer with the following operating system:

- OS X 10.9 (Mavericks)
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- OS X 10.12 (Sierra)

If for some reason the CX5500 system is unable to detect the operating system, you can use the CX5100-CX5500 Control Panel to disable Mac OS support.

Note: The CX5100-CX5500 Control Panel is only supported on Windows computers. You cannot use the Control Panel on Mac computers.

To configure Mac OS support using the Control Panel:

1 In the Control Panel, navigate to **Profile Editor > Advanced**.
2 Click the check box for **Enable Mac OS support**.

Updating the CX5100 Software

You can configure the CX5100 unified conference station to check for available software updates automatically, or you can update the software manually in the Control Panel or upload new software to the unified conference station using a USB flash drive.

Keep the following in mind while the software is updating on the CX5100:

- The update can take up to 40 minutes to complete. During this time, the unified conference station reboots several times during the update, and the indicator lights flash in several different patterns.

- Do not power the unified conference station off during an update. Wait at least 40 minutes to make sure the update has completed.
- The update is complete when the indicator lights stop flashing for at least 30 seconds.

Update the CX5100 Software Automatically

In the Control Panel, you can set the frequency of when the unified conference station will check for software updates and update automatically when a new software version is detected. Contact your system administrator for the software server address.

To update the CX5100 software automatically:

1. In the Profile Editor tab, select **Software Update**.
2. For **Update Server**, enter the name of the server where the unified conference station should check for software.
3. For **Update Frequency**, select how often the unified conference station should check for updates.
4. For **Update Time**, select what time the unified conference station should update when a new software version is detected.

   The CX5100 unified conference station retrieves software updates from the server on the chosen date and time, if available.

Update the CX5100 Software Manually

Using the Control Panel, you can manually update the software for the CX5100 unified conference station when you know that a new software version is available.

To update the software manually:

1. Click **System > Software Update**.
2. Click **Update Now** to start the update.

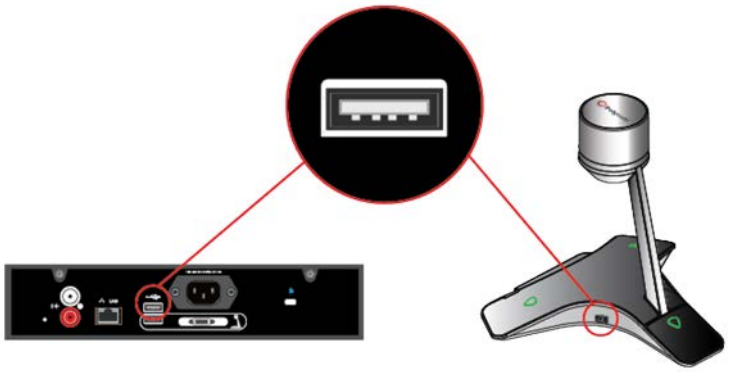
   The unified conference station uploads the software update from the server, if available.

Update the CX5100 Software using an USB

You can download the latest version of software for the CX5100 unified conference station onto a USB flash drive, and update the software on the unfired conference station. In order to use a flash drive to update the software, make sure the USB flash drive formatted as FAT32. Make sure that there is only one software update package on the flash drive.

To update the software using a USB flash drive:

1. Obtain the software update package from your network administrator, and copy the software to a USB flash drive.
2. Connect the flash drive to the USB 2.0 port on the unfired conference station or to the USB 3.0 port on the power data box, as shown in the following figure. The unified conference station detects the software on the flash drive automatically and starts the update within 30 seconds.



Troubleshooting

This section lists potential issues, problems, and common difficulties and possible solutions to guide you towards resolving those issues.

General System Issues

If you encounter any general system issues, see the following table for possible solutions to common problems.

Issue	Solution
The system won't power on.	Ensure that your power cable is connected securely to a working power outlet.
The CX5100 Control Panel does not connect to the CX5100 unified conference station.	Try the following solutions: • Disconnect the USB cable from the computer and reconnect it. • Restart the Control Panel application.
Updating the software fails because the CX5100 is unable to locate the updated software.	Try the following solutions: • Ensure that your Ethernet cable is connected securely. • Ensure that your Ethernet connection is enabled and configured correctly. • Ensure that the URL of the update server is correct. Click **Apply to Device** to transfer the settings to the device. • If you continue to have problems, copy the software package to a USB flash drive, and attach it to the CX5100 or the power data box. Ensure that there is only one software update package on the USB drive.
My computer is connected to a USB 3.0 port, but I see a warning that my computer is connected to a USB 2.0 port.	Try the following solutions: • Ensure the system is connected to a USB 3.0 port. A USB 3.0 port is usually blue and has a SS icon next to the port. • Disconnect the USB cable from the computer and reconnect it. • Update the USB 3.0 driver on the computer to ensure that the date of the driver is 2013 or later. Visit your computer's manufacturer's website for the latest driver available for your computer. • Connect the computer directly to the blue USB 3.0 port on the power data box.

Audio and Video

If you encounter any issues with audio or video, see the following table for possible solutions to common problems.

Common Audio and Video Issues and Solutions

Issue	Solution
My camera is not listed in the device selection list.	Try the following solutions: • Ensure that your camera cable is connected securely. • Verify your video device settings. In the Skype for Business client, click ⚙ and choose **Video Device**. Ensure that CX5100 is selected as the video device. • Restart the Polycom CX5100 system.
Others don't see my video.	Try the following solutions: • Ensure that your privacy cap is raised. • Ensure that all cables are connected securely. • Verify your video device settings. In the Skype for Business client, click ⚙ and choose **Video Device**. Ensure that CX5100 is selected as the video device. • Restart the Polycom CX5100 system.
My video is flickering.	Ensure that the Power Frequency is set correctly for your location. In the CX5100 - CX5500 Control Panel, click **System** then click **Advanced**. Choose the Power Frequency you need.
My video is displayed at a very low frame rate.	Try the following solutions: • Ensure the system is connected to a USB 3.0 port. A USB 3.0 port is usually blue and has a SS icon next to the port. • Ensure that the unified conference station is plugged into the blue USB 3.0 port on the power data box.
Others don't hear my audio.	Try the following solutions: • Ensure that your audio is not muted by pressing the mute buttons on the unified conference station or by click the mute icon in the Skype for Business client. • Ensure that your microphone cable is connected securely. • Verify your audio settings. In the Skype for Business client, click ⚙ and choose **Audio Device**. Ensure that the CX5100 is selected as the audio device.

Common Audio and Video Issues and Solutions

Issue	Solution
I don't hear audio from others.	Try the following solutions: • Ensure that the far-site audio is not muted. • Ensure that your volume is set to an audible level.
I muted my audio in Skype for Business, but the microphone indicators on the tabletop unit do not show red.	Muting your audio in the Skype for Business client does not control the microphone indicators on the CX5100 unified conference station. Your audio is still muted, and the far end does not hear your audio. Update your Skype for Business client to the latest version in order to have the capability of syncing call activity with your system.

Access System Information

You can view a listing of system settings and status that may be helpful while troubleshooting. The information is refreshed each time you access the page. To refresh the page, go to another page and return to the System Information page.

To access information about the system:

» In the CX5100 - CX5500 Control Panel, click **System** then click **System Information**.

Test the Speakers and Microphones

You can test the Microphones and speakers to ensure that the CX5100 is operating correctly.

To test the speaker and Microphones:

1. In the Skype for Business client, click .
2. Click **Audio Device** then choose the CX5100 device as the Audio Device.
3. In the Speaker section, click to play a tone.
4. Adjust the Speaker slider to increase or decrease the volume of the tone.
5. Gently brush your finger over the microphone on the CX5100 to check the Microphone indicator response.

   If there is no response, check to be sure the microphone is not muted.
6. Adjust the Microphone slider to increase or decrease the microphone’s sensitivity.

Test the Camera

You can test the camera on the CX5100 to ensure the camera is operating correctly.

To test the camera:

1. In the Skype for Business client, click .

2 Click **Video Device** and check the video preview.

View Diagnostic Information

You can view diagnostic information for the CX5100 to determine the any issues on the CX5100.

To view diagnostics information:

» In the CX5100 - CX5500 Control Panel, click **Diagnostics**.

Retrieving Logs

The CX5100 system logs various events to files stored in the flash file system and periodically uploads these log files to the provisioning server. The files are stored in the system's home directory or a user-configurable directory. You can also configure a system to send log messages to a syslog server.

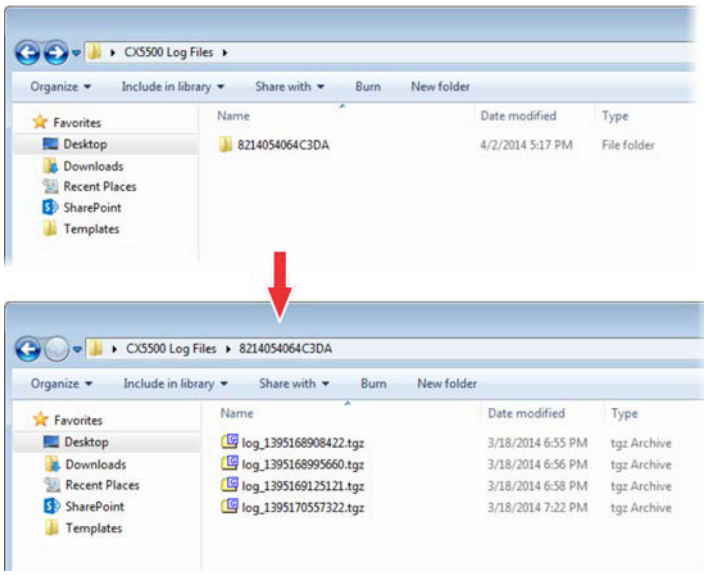
You can capture logging events of different severity for the CX5100 system, which enables you to capture lower severity events in one part of the application, and high severity events for other components.

The following are options for retrieving system log files for the CX5100 system:

- USB drive
- Control Panel
- Web Configuration Utility
- Provisioning server
- Log level parameters

Retrieve Logs with a USB

When you connect a USB flash drive to the CX5500 system, the system creates a new folder on the flash drive. The folder is named with the device's serial number and the system's log files are saved as .tar files in the device folder, as shown.



Make sure to remove any software packages from the USB flash drive.

To retrieve system logs using a USB:

» Connect a USB flash drive to the USB port on the tabletop unit or on the power data box.

The logs are transferred automatically. It takes approximately one minute to complete the transfer.

Retrieve Logs using the Control Panel

You can use the CX5100 - CX5500 Control Panel to retrieve logs to a USB flash drive connected to the CX5100. Make sure to remove any software packages from the USB flash drive.

To retrieve logs using the control panel.

1. From the CX5100 - CX5500 Control Panel, click **System** and then click **Debugging**.
2. Connect a USB flash drive to the USB port on the unified conference station.
3. Click **Retrieve Logs** to copy the logs to the USB flash drive.

   It takes approximately one minute to complete the transfer.

Retrieve Logs using the Web Configuration Utility

You can use the Web Configuration Utility to retrieve either application or system log files. You can also choose which level of logs you want to view or export.

To retrieve logs using the Web Configuration Utility:

1. Log into the Web Configuration Utility, and navigate to **Diagnostics > View & Download Logs**.
2. Select the **Log File Type** and the **Log Level Filter**, then click **Export**.

Upload Logs to a Provisioning Server

You can upload application and system log files from the CX5500 system to the provisioning server. In order to set the system to upload log files to the provisioning server, you need to enter the provisioning server information and set the logging types and frequency using the Web Configuration Utility.

1. Log into the Web Configuration Utility, and navigate to **Settings > Provisioning Server**.
2. Select the **Server Type**, enter in the **Server Address**, **Server User**, and **Server Password**, then click **Save**.
3. Navigate to **Settings > Logging**.
4. For **Global Settings**, set the **Global Log Level Limit**.
5. For **Log File Upload**, set the **Upload Period**.
6. Set any additional log settings, then click **Save**.

After you set the logging options, log files are uploaded to the provisioning server automatically after set intervals.

Log Level Parameters

The parameters for log level settings are found in the techsupport.cfg configuration file, available by special request from Polycom Customer Support. They are log.level.change.module_name. Log levels range from 0 to 6 - 0 for the most detailed logging, 6 for critical errors only. Many different log types can be adjusted to assist with the investigation of different problems. The exact number of log types is dependent on the system model.

When testing is complete, remember to remove the configuration parameter from the configuration files.

You can modify the logging parameters described next. Changing these parameters will not have the same impact as changing the logging levels, but you should still understand how your changes will affect the system and the network.

- `log.render.level`—Sets the lowest level that can be logged (default=1)
- `log.render.file.size`—Maximum size before log file is uploaded (default=32 kb)
- `log.render.file.upload.period`—Frequency of log uploads (default is 172800 seconds = 48 hours)
- `log.render.file.upload.append`—Controls whether log files on the provisioning server are overwritten or appended, not supported by all servers (default=1 so files are appended)

Scheduled Logging

Scheduled logging is a powerful tool that can help you troubleshoot issues that occur after the system has been operating for some time.

The output of these instructions is written to the application log, and can be examined later (for trend data).

The parameters for scheduled logging are found in the techsupport.cfg configuration file. They are `log.sched.module_name`. Note that passwords display in a level 1 .cfg log file.

Restore to Factory Settings

If you experience severe problems with the CX5100, you can restore the unified conference station to its factory settings. To restore the CX5100, you need to press the restore button, which is located on the back of the power data box, as shown in the following figure:

Location of the system restore button

To restore the CX5100 to factory settings:

1. Power off the unified conference station.
2. Use a paper clip to press and hold the restore button.
3. While holding the restore button, power on the unified conference station.
4. Continue holding the restore button for 20 more seconds, then release it.

Maintenance Tasks

This section provides information on updating and maintaining your CX5100 unified conference station.

Trusted Certificate Authority List

The system trusts the following certificate authorities by default:

- AAA Certificate Services by COMODO
- ABAecom (sub., Am. Bankers Assn.) Root CA
- Add Trust Class1 CA Root by COMODO
- Add Trust External CA Root by COMODO
- Add Trust Public CA Root by COMODO
- Add Trust Qualified CA Root by COMODO
- ANX Network CA by DST
- American Express CA
- American Express Global CA
- BelSign Object Publishing CA
- BelSign Secure Server CA
- COMODO CA Limited
- COMODO Certificate Authority
- Deutsche Telekom AG Root CA
- Digital Signature Trust Co. Global CA 1
- Digital Signature Trust Co. Global CA 2
- Digital Signature Trust Co. Global CA 3
- Digital Signature Trust Co. Global CA 4
- Entrust Worldwide by DST
- Entrust.net Premium 2048 Secure Server CA
- Entrust.net Secure Personal CA
- Entrust.net Secure Server CA
- Equifax Premium CA
- Equifax Secure CA
- Equifax Secure eBusiness CA 1
- Equifax Secure eBusiness CA 2

- Equifax Secure Global eBusiness CA 1
- GeoTrust Primary Certification Authority
- GeoTrust Global CA
- GeoTrust Global CA 2
- GeoTrust Universal CA
- GeoTrust Universal CA 2
- GTE CyberTrust Global Root
- GTE CyberTrust Japan Root CA
- GTE CyberTrust Japan Secure Server CA
- GTE CyberTrust Root 2
- GTE CyberTrust Root 3
- GTE CyberTrust Root 4
- GTE CyberTrust Root 5
- GTE CyberTrust Root CA
- GlobalSign Partners CA
- GlobalSign Primary Class 1 CA
- GlobalSign Primary Class 2 CA
- GlobalSign Primary Class 3 CA
- GlobalSign Root CA
- Go Daddy Class 2 Certification Authority Root Certificate
- Go Daddy Class 2 Certification Authority Root Certificate – G2
- National Retail Federation by DST
- RSA 2048 v3 Root CA
- Secure Certificate Services by COMODO
- TC TrustCenter, Germany, Class 1 CA
- TC TrustCenter, Germany, Class 2 CA
- TC TrustCenter, Germany, Class 3 CA
- TC TrustCenter, Germany, Class 4 CA
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA
- Thawte Universal CA Root
- Trusted Certificate Services by COMODO
- UTN-DATA Corp SGC by COMODO
- UTN-USER First-Client Authentication and Email by COMODO
- UTN-USER First-Hardware by COMODO

- UTN-USER First-Object by COMODO
- UPS Document Exchange by DST
- ValiCert Class 1 VA
- ValiCert Class 2 VA
- ValiCert Class 3 VA
- Verisign 2048 Root CA
- VeriSign Class 4 Primary CA
- Verisign Class 1 Public Primary Certification Authority
- Verisign Class 1 Public Primary Certification Authority - G2
- Verisign Class 1 Public Primary Certification Authority - G3
- Verisign Class 2 Public Primary Certification Authority
- Verisign Class 2 Public Primary Certification Authority - G2
- Verisign Class 2 Public Primary Certification Authority - G3
- Verisign Class 3 Public Primary Certification Authority
- Verisign Class 3 Public Primary Certification Authority - G2
- Verisign Class 3 Public Primary Certification Authority - G3
- Versign Class 3 Public Primary Certification Authority – G5
- Verisign Class 4 Public Primary Certification Authority - G2
- Verisign Class 4 Public Primary Certification Authority - G3
- Verisign/RSA Commercial CA
- Verisign/RSA Secure Server CA
- Windows Root Update by COMODO

Troubleshoot: Polycom endeavors to maintain a built-in list of the most commonly used Certificate Authority (CA) certificates. Due to memory constraints, we cannot ensure a complete set of certificates.

If you are using a certificate from a commercial CA not in the list above, you can submit a feature request for Polycom to add your CA to the trusted list. At this point, you can use the custom certificate method to load your particular CA certificate into the system. See *Using Custom Certificates on Polycom systems (Technical Bulletin 17877)*.

Encrypt Configuration Files

The system can recognize encrypted files. Systems can download encrypted files from the provisioning server and can encrypt files before uploading them to the provisioning server. There must be an encryption key on the system to perform these operations. You can encrypt configuration files (excluding the master configuration file), contact directories, and configuration override files.

You can generate your own 32 hex-digit, 128 bit key to encrypt and decrypt configuration files on a UNIX or Linux server.

The SDK generates a random key and applies Advanced Encryption Standard (AES) 128 in Cipher Block Chaining (CBC) mode. For example, a key can look like this:

```
Crypt=1;KeyDesc=companyNameKey1;Key=06a9214036b8a15b512e03d53412006;
```

The `device.set`, `device.sec.configEncryption.key`, and `device.sec.configEncryption.key.set` configuration file parameters are used to set the key on the system.

If the system doesn't have a key, it must be downloaded to the system in plain text (a potential security concern if not using HTTPS). If the system already has a key, a new key can be downloaded to the system encrypted using the old key.

Polycom recommends that you give each key a unique descriptive string in order to identify which key was used to encrypt a file. This makes provisioning server management easier.

After encrypting a configuration file, it is useful to rename the file to avoid confusing it with the original version, for example rename site.cfg to site.enc. However, the directory and override filenames cannot be changed in this manner.

Change the System Key

For security purposes, you can change the key on the systems and the server from time to time.

To change a key on the system:

1. Put all encrypted configuration files on the provisioning server to use the new key.

   The system may reboot multiple times.

   The files on the server must be updated to the new key or they must be made available in unencrypted format. Updating to the new key requires decrypting the file with the old key, then encrypting it with the new key.
2. Put the new key into a configuration file that is in the list of files downloaded by the system, specified in **000000000000.cfg** or **<*MACaddress*>.cfg**.
3. Use the `device.sec.configEncryption.key` parameter to specify the new key.
4. Provision the system again so that it downloads the new key. The system automatically reboots a second time to use the new key.

   Note that configuration files, contact directory files and configuration override files may all need to be updated if they were already encrypted. In the case of configuration override files, they can be deleted from the provisioning server so that the system replaces them when it successfully boots.

To check whether an encrypted file is the same as an unencrypted file:

1. Run the *configFileEncrypt* utility, available from Polycom Support, on the unencrypted file with the "-d" option. This shows the “digest” field.
2. Look at the encrypted file using a text editor, and check the first line that shows a "Digest=…." field. If the two fields are the same, then the encrypted and unencrypted file are the same.

Capture Wireshark Trace using Flash File to USB Flash Drive

The CX5100 unified conference station allows you to the capture the Wireshark trace to a USB flash drive. You must connect the USB flash drive to the CX5100 system. Ensure that the USB flash drive is FAT32 formatted.

To capture the Wireshark trace to USB flash drive:

1. Format a USB flash drive to FAT32.
2. Set the capture length in the only parameter of the `plcm_tcpdump_in_seconds.cfg` file between 1 to 300 seconds.
3. Copy the `plcm_tcpdump_in_seconds.cfg` file to a FAT32 formatted USB flash drive.
4. Connect the USB flash drive to the CX5100 system.
5. Turn on the CX5100 system.

   The CX5100 system starts capturing the Wireshark trace to USB flash drive automatically. When the time interval exceeds the capture length defined in the plcm_tcpdump_in_seconds.cfg file, the CX5100 system stops capturing the trace.

   The captured trace is stored in the USB flash drive as **.pcap** file.

Capture Wireshark Trace to USB Flash Drive through Telnet Command

You can capture the Wireshark trace to USB flash drive using Telnet. The CX5100 unified conference station allows you to capture the trace through Telnet when you enable the following parameters:

- `diags.pcap.enabled`
- `diags.telnetd.enabled`

To capture the Wireshark trace to USB flash drive through Telnet:

1. In the configuration file, edit the following parameters to:
   - `diags.pcap.enabled=”1”`
   - `diags.telnetd.enabled=”1”`
2. Copy the configuration file to a FAT32 formatted USB flash drive.
3. Connect the USB flash drive to the CX5100 system.
4. Turn on the CX5100 system.
5. From a computer connected to the same network, perform a telnet to the CX5100 unified conference station.
6. Use the following commands to start capturing:
   1. `pcapFilterSet` – Sets the capture filter to be used with the USB flash drive
   2. `pcapStart` – Starts the capture to the USB flash drive
7. To stop capturing, use the `pcapStop` command.

   The Wireshark trace capture is written out to a file with the naming convention **<MAC>-<date>-<time>.pcap** and is placed in the root directory of the USB flash drive.

Assigning a VLAN ID Using DHCP

In deployments where is not possible or desirable to assign a virtual local area network (VLAN) statically in the system’s network configuration menu or use Cisco Discovery Protocol (CDP) or Link-Layer Discovery

Protocol (LLDP) to assign a VLAN ID, it is possible to assign a VLAN ID to the system by distributing the VLAN ID via DHCP.

When using this method to assign the system's VLAN ID, the system first boots on the default VLAN (or statically configured VLAN, if first configured in the system's network configuration menu), obtains its intended VLAN ID from the DHCP offer, then continues booting (including a subsequent DHCP sequence) on the newly obtained VLAN.

DVD string in the DHCP option must meet the following conditions to be valid:

- Must start with "VLAN-A=" (case-sensitive)
- Must contain at least one valid ID
- VLAN IDs range from 0 to 4095
- Each VLAN ID must be separated by a "+" character
- The string must be terminated by a semi colon ";"
- All characters after the semi colon ";" are ignored
- There must be no white space before the semi colon ";"
- VLAN IDs may be decimal, hex, or octal

  The following DVD strings result in the system using VLAN 10:

  ```
  VLAN-A=10;
  VLAN-A=0x0a;
  VLAN-A=012;
  ```

Note: If a VLAN tag is assigned by CDP or LLDP, DHCP VLAN tags are ignored.

Parse Vendor ID Information

After the system boots, it sends a DHCP discover packet to the DHCP server. This is found in the bootstrap protocol/option 'Vendor Class Identifier' section of the packet and includes the system's part number and the BootROM version. RFC 2132 does not specify the format of this option's data, and can be defined by each vendor.

To be useful, every vendor's format must be distinguishable from every other vendor's format. To make our format uniquely identifiable, the format follows RFC 3925, which uses the IANA private enterprise number to determine which vendor's format should be used to decode the remaining data. The private enterprise number assigned to Polycom is 13885 (0x0000363D).

This vendor ID information is not a character string, but an array of binary data.

The steps for parsing are as follows:

1. Check for the Polycom signature at the start of the option:

   4 octet: 00 00 36 3d
2. Get the length of the entire list of sub-options:

   1 octet
3. Read the field code and length of the first sub-option, 1+1 octets

4. If this is a field you want to parse, save the data.
5. Skip to the start of the next sub-option.
6. Repeat steps 3 to 5 until you have all the data or you encounter the End-of-Suboptions code (0xFF).

The following example is a sample decode of a packet (DHCP Option 60):

```
3c 7a
```

- Option 60, length of Option data (part of the DHCP specification)

```
00 00 36 3d
```

- Polycom signature (always 4 octets)

```
75
```

- Length of Polycom data

```
01 07 50 6f 6c 79 63 6f 6d
```

- sub-option 1 (company), length, “Polycom”

```
02 0b 56 56 58 2d 56 56 58 5f 34 31 30
```

- sub-option 2 (part), length, “CX5100”

```
03 10 33 31 31 31 2d 34 36 31 36 32 2d 30 30 31 2c 37
```

- sub-option 3 (part number), length, "2345-11605-001,2"

```
04 1e 53 49 50 2f 35 2e 32 2e 30 2e 58 58 58 58 2f 30 36 2d 41 75 67 2d 31 34
20 32 30 3a 35 35
```

- sub-option 4 (Application version), length, "SIP/Tip.XXXX/08-Jun-07 10:44"

```
05 1d 55 50 2f 35 2e 34 2e 30 2e 58 58 58 58 2f 30 36 2d 41 75 67 2d 31 34 20
32 31 3a 30 34
```

- sub-option 5 (Updater version), length, "BR/3.1.0.XXXX/28-Apr-05”

```
06 0c 64 73 6c 66 6f 72 75 6d 2e 6f 72 67
```

Product, Model, and Part Number Mapping

You can use the master configuration file to direct system upgrades to a software image and configuration files based on a system model number, a firmware part number, or a system’s MAC address.

The part number has precedence over the model number, which has precedence over the original version.

For example, `CONFIG_FILES_2345-11560-001=”system1_2345-11560-001.cfg, sip_2345-11560-001.cfg” will override CONFIG_FILES_CX5100=”system1_CX5500.cfg, sip_CX5100.cfg”`, which will override `CONFIG_FILES=”system1.cfg, sip.cfg`” for the CX5100.

You can also add variables to the master configuration file that are replaced when the system reboots. The variables include `SYSTEM_MODEL, SYSTEM_PART_NUMBER, and SYSTEM_MAC_ADDRESS`.

LLDP and Supported TLVs

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network.

Web Info: The protocol was formally ratified as IEEE standard 802.1AB in May 2005. Refer to section 10.2.4.4 of the LLDP-MED standard.

The LLDP feature supports VLAN discovery and LLDP power management, but not power negotiation. LLDP has a higher priority than CDP and DHCP VLAN discovery.

Note: The following are ways to obtain VLAN on the system and they can all be enabled, but the VLAN used is chosen by the priority of each method: 1. LLDP; 2. CDP; 3. DVD (VLAN Via DHCP).

The following mandatory and optional Type Length Values (TLVs) are supported:

Mandatory:

- Chassis ID—Must be first TLV
- Port ID—Must be second TLV
- Time-to-live—Must be third TLV, set to 120 seconds
- End-of-LLDPDU—Must be last TLV
- LLDP-MED Capabilities
- LLDP-MED Network Policy—VLAN, L2 QoS, L3 QoS
- LLDP-MED Extended Power-Via-MDI TLV—Power Type, Power Source, Power Priority, Power Value

Optional:

- Port Description
- System Name—Administrator assigned name
- System Description—Includes device type, system number, hardware version, and software version
- System Capabilities—Set as ‘Telesystem’ capability
- MAC / PHY config status—Detects duplex mismatch
- Management Address—Used for network discovery
- LLDP-MED Location Identification—Location data formats: Co-ordinate, Civic Address, ECS ELIN
- LLDP-MED Inventory Management —Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer’s Name, Model Name, Asset ID

An LLDP frame shall contain all mandatory TLVs. The frame is recognized as LLDP only if it contains mandatory TLVs. Polycom systems running the UC Software support LLDP frames with both mandatory and optional TLVs. The basic structure of an LLDP frame and a table containing all TLVs along with each field is explained in Supported TLVs.

LLDP-MED Location Identification

As per section 10.2.4.4 of the LLDP-MED standard, LLDP-MED endpoint devices need to transmit location identification TLVs if they are capable of either automatically determining their physical location by use of GPS or radio beacon or capable of being statically configured with this information.

At present, the systems do not have the capability to determine their physical location automatically or provision to a statically configured location. because of these limitations, the systems do not transmit location identification TLV in the LLDP frame. However, the location information from the switch is decoded and displayed on the system's menu.

Supported TLVs

The basic TLV format is as follows:

- TLV Type (7 bits) [0-6]
- TLV Length (9 bits) [7-15]
- TLV Information (0-511 bytes)

The following table lists the supported TLVs.

Supported TLVs

No	Name	Type (7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Sub Type
1	**Chassis-Id**[1]	**1**	**6**	**0x0206**	**-**	**5**
IP address of system (4 bytes). Note that 0.0.0.0 is not sent until the system has a valid IP address.						
2	**Port-Id**[1]	**2**	**7**	**0x0407**	**-**	**3**
MAC address of system (6 bytes)						
3	**TTL**	**3**	**2**	**0x0602**	**-**	**-**
TTL value is 120/0 sec						
4	**Port description**	**4**	**1**	**0x0801**	**-**	**-**
Port description 1						
5	**System name**	**5**	**min len > 0, max len <= 255**	**-**	**-**	**-**
6	**System description**	**6**	**min len > 0, max len <= 255**	**-**	**-**	**-**
Manufacturer's name - "Polycom"; Hardware version; Application version; BootROM version						
7	**Capabilities**	**7**	**4**	**0x0e04**	**-**	**-**
System Capabilities: Telesystem and Bridge if the system has PC port support and it is not disabled. Enabled Capabilities: Telesystem and Bridge if system has PC port support, it is not disabled and PC port is connected to PC.						
8	**Management Address**	**8**	**12**	**0x100c**	**-**	**-**
Address String Len - 5, IPV4 subtype, IP address, Interface subtype - "Unknown", Interface number - "0", ODI string Len - "0"						

Supported TLVs

No	Name	Type (7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Sub Type
9	**IEEE 802.3 MAC/PHY config/status[1]**	**127**	**9**	**0xfe09**	**0x00120f**	**1**
Auto Negotiation Supported - “1”, enabled/disabled, Refer to PMD Advertise and Operational MAU.						
10	**LLDP-MED capabilities**	**127**	**7**	**0xfe07**	**0x0012bb**	**1**
Capabilities - 0x33 (LLDP-Med capabilities, Network policy, Extended Power Via MDI-PD, Inventory) Class Type III Note: After support for configuring location Identification information is locally available: Capabilities - 0x37 (LLDP-Med capabilities, Network policy, Location Identification, Extended Power Via MDI-PD, Inventory) Class Type III						
11	**LLDP-MED network policy[2]**	**127**	**8**	**0xfe08**	**0x0012bb**	**2**
ApplicationType: Voice (1), Policy: (Unknown(=1)/Defined(=0) Unknown, if system is in booting stage or if switch doesn't support network policy TLV. Defined, if system is operational stage and Networkpolicy TLV is received from the switch.), Tagged/Untagged, VlanId, L2 priority and DSCP						
12	**LLDP-MED network policy[2]**	**127**	**8**	**0xfe08**	**0x0012bb**	**2**
ApplicationType: Voice Signaling (2), Policy: (Unknown(=1)/Defined(=0) Unknown, if system is in booting stage or if switch doesn't support network policy TLV. Defined, if system is operational stage and Networkpolicy TLV is received from the switch.),Tagged/Untagged, VlanId, L2 priority and DSCP. **Note**: Voice signaling TLV is sent only if it contains configuration parameters that are different from voice parameters.						
13	**LLDP-MED network policy[2]**	**127**	**8**	**0xfe08**	**0x0012bb**	**2**
ApplicationType: Video Conferencing (6),Policy: (Unknown(=1)/Defined(=0). Unknown, if system is in booting stage or if switch doesn't support network policy TLV. Defined, if system is operational stage and Networkpolicy TLV is received from the switch.),Tagged/Untagged, VlanId, L2 priority and DSCP.						
14	**LLDP-MED location identification[3]**	**127**	**min len > 0, max len <= 511**	**-**	**0x0012bb**	**3**
ELIN data format: 10 digit emergency number configured on the switch. Civic Address: physical address data such as city, street number, and building information.						
15	**Extended power via MDI**	**127**	**7**	**0xfe07**	**0x0012bb**	**4**
16	**LLDP-MED inventory hardware revision**	**127**	**min len > 0, max len <= 32**	**-**	**0x0012bb**	**5**
Hardware part number and revision						
17	**LLDP-MED inventory firmware revision**	**127**	**min len > 0, max len <= 32**	**-**	**0x0012bb**	**6**

Supported TLVs

No	Name	Type (7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Sub Type
BootROM revision						
18	**LLDP-MED inventory software revision**	**127**	**min len > 0, max len <= 32**	**-**	**0x0012bb**	**7**
Application (SIP) revision						
19	**LLDP-MED inventory serial number**	**127**	**min len > 0, max len <= 32**	**-**	**0x0012bb**	**8**
MAC Address (ASCII string)						
20	**LLDP-MED inventory manufacturer name**	**127**	**11**	**0xfe0b**	**0x0012bb**	**9**
Polycom						
21	**LLDP-MED inventory model name**	**127**	**min len > 0, max len <= 32**	**-**	**0x0012bb**	**10**
22	**LLDP-MED inventory asset ID**	**127**	**4**	**0xfe08**	**0x0012bb**	**11**
Empty (Zero length string)						
23	**End of LLDP DU**	**0**	**0**	**0x0000**	**-**	**-**

[1] For other subtypes, refer to IEEE 802.1AB, March 2005.
[2] For other application types, refer to TIA Standards 1057, April 2006.
[3] At this time, this TLV is not sent by the system.

PMD Advertise and Operational MAU

The following table lists values for the PMD advertise and operational MAU.

PMD Advertise and Operational MAU Type

Mode/Speed	PMD Advertise Capability Bit	Operational MAU Type
10BASE-T half duplex mode	1	10
10BASE-T full duplex mode	2	11
100BASE-T half duplex mode	4	15
100BASE-T full duplex mode	5	16
1000BASE-T half duplex mode	14	29
1000BASE-T full duplex mode	15	30
Unknown	0	0

Note: By default, all systems have the PMD advertise capability set for 10HD, 10FD, 100HD, and 100FD bits.

Configuration Parameters

This section is a reference guide to the configuration parameters you can use to configure system features and functions. This section provides a description of each configuration parameter, and permitted and default values.

<device/>

The <device/> parameters—also known as device settings—contain default values that you can use to configure basic settings for multiple systems.

Note: The default values for the <device/> parameters are set at the factory when the systems are shipped. For a list of the default values, see the latest Product Shipping Configuration Change Notice at Polycom Engineering Advisories and Technical Notifications.

Polycom provides a global device.set parameter that you must enable to install software and change device parameters. In addition, each <device/> parameter has a corresponding .set parameter that enables or disables the value for that device parameter. You need to enable the corresponding .set parameter for each parameter you want to apply.

After you complete the software installation or configuration changes to device parameters, remove device.set to prevent the systems from rebooting and triggering a reset of device parameters that system users might have changed after the initial installation.

If you configure any parameter values using the <device/> parameters, any subsequent configuration changes you make from the Web Configuration Utility do not take effect after a system reboot or restart.

The <device/> parameters are designed to be stored in flash memory, and are therefore not added to the <MAC>-web.cfg or <MAC>-system.cfg override files whether the changes are made through the Web Configuration Utility. This design protects the ability to manage and access the systems using the standard set of parameters on a provisioning server after the initial installation.

.set Parameter Exception

Each <device/> parameter has a corresponding .set parameter that enables or disables the parameter. There is one exception to this rule: the device.sec.TLS.customDeviceCertX.set parameter applies to device.sec.TLS.customDeviceCertX.publicCert and to device.sec.TLS.customDeviceCertX.privateKey.

Note: Each <device/> parameter has a corresponding .set parameter that enables or disables the parameter. There is one exception to this rule: the device.sec.TLS.customDeviceCertX.set parameter applies to device.sec.TLS.customDeviceCertX.publicCert and to device.sec.TLS.customDeviceCertX.privateKey.

Use Caution When Changing Device Parameters

Use caution when changing <device/> parameters as incorrect settings may apply the same IP address to multiple systems.

Note that some parameters may be ignored. For example, if DHCP is enabled it will still override the value set with device.net.ipAddress.

Though individual parameters are checked to see whether they are in range, the interaction between parameters is not checked. If a parameter is out of range, an error message displays in the log file and parameter will not be used.

Incorrect configuration can put the systems into a reboot loop. For example, server A has a configuration file that specifies that server B should be used, and server B has a configuration file that specifies that server A should be used.

To detect errors, including IP address conflicts, Polycom recommends that you test the new configuration files on two systems before initializing all systems.

Types of Device Parameters

The following table outlines the three types of <device/> parameters, their permitted values, and the default value.

Device Parameter Types

Parameter	*Permitted Values*	*Default*
device.set[1]	**0 or 1**	**0**
If set to 0, do not use any device.xxx fields to set any parameters. Set this to 0 after the initial software installation. If set to 1, use the device.xxx fields that have device.xxx.set=1. Set this to 1 only for the initial software installation.		
device.xxx[1]	**string**	
Configuration parameter.		
device.xxx.set[1]	**0 or 1**	**0**
If set to 0, do not use the device.xxx value. If set to 1, use the device.xxx value. For example, if device.net.ipAddress.set=1, then use the value set for device.net.ipAddress.		

[1] Change causes system to restart or reboot

device.cma.serverName	**string**	
The server address that the system uses to connect to the provisioning server.		

The following table lists each of the <device/> parameters that you can configure.

Device Parameters

Parameter	*Permitted Values*	*Default*
device.dhcp.bootSrvOpt[1]	**Null, 128 to 254**	
When the boot server is set to Custom or Custom+Option66, specify the numeric DHCP option that the system looks for.		
device.dhcp.bootSrvOptType[1]	**IP address or string**	
The type of DHCP option the system looks for its provisioning server (if `device.dhcp.bootSrvUseOpt` is set to `Custom`). If IP, the IP address provided must specify the format of the provisioning server. If String, the string provided must match one of the formats specified by `device.prov.serverName`.		
device.dhcp.bootSrvUseOpt[1]	**Default, Custom, Static, CustomAndDefault**	
Default The system looks for option number 66 (string type) in the response received from the DHCP server. The DHCP server should send address information in option 66 that matches one of the formats described for `device.prov.serverName`. **Custom** The system looks for the option number specified by `device.dhcp.bootSrvOpt`, and the type specified by `device.dhcp.bootSrvOptType` in the response received from the DHCP server. **Static** The system uses the boot server configured through the provisioning server `device.prov.*` parameters. **Custom** and **Default** The system uses the custom option first or use Option 66 if the custom option is not present.		
device.dhcp.enabled[1]	**0 or 1**	
If 0, DHCP is disabled. If 1, DHCP is enabled.		
device.dhcp.option60Type[1]	**Binary, ASCII**	
The DHCP option 60 type. `Binary:` vendor-identifying information is in the format defined in RFC 3925. `ASCII`: vendor-identifying information is in ASCII format.		
device.dhcp.dhcpVlanDiscUseOpt[1]	**Disabled, Fixed, Custom**	
VLAN Discovery. `Disabled`, no VLAN discovery through DHCP. `Fixed`, use predefined DHCP vendor-specific option values of 128, 144, 157 and 191 (`device.dhcp.dhcpVlanDiscOpt` is ignored). `Custom`, use the number specified by `device.dhcp.dhcpVlanDiscOpt`.		
device.dhcp.dhcpVlanDiscOpt[1]	**128 to 254**	
The DHCP private option to use when `device.dhcp.dhcpVlanDiscUseOpt` is set to `Custom`.		
device.dns.altSrvAddress[1]	**server address**	
The secondary server to which the system directs domain name system (DNS) queries.		

Device Parameters (continued)

Parameter	*Permitted Values*	*Default*
device.dns.domain[1]	**string**	
The system's DNS domain.		
device.dns.serverAddress[1]	**string**	
The primary server to which the system directs DNS queries.		
device.host.hostname[1]	**string**	
This parameter enables you to specify a hostname for the system when using DHCP by adding a hostname string to the system's configuration. If `device.host.hostname.set=1`, and `device.host.hostname=Null`, the DHCP client uses Option 12 to send a predefined hostname to the DHCP registration server using `Polycom_<MACaddress>`. Note that the maximum length of the hostname string is <=255 bytes. The valid character set is defined in RFC1035.		
device.local.usbConnectionResetInterval	**-1 or 86400 to 172800**	**-1**
The intervals (in seconds) when the system will reboot to resolve any USB connection issues.		
device.local.usbConnectionResetTime	**0 to 2400hrs**	**0**
The set time when the system will reboot to resolve any USB connection issues.		
device.local.panoviewEnable	**0 or 1**	**1**
Enables or disables panoramic video. If set to 1, panoramic video is enabled. If set to 0, panoramic view is disabled and active speaker video displays only. **Note**: Panoramic video is not supported for connected Mac computers.		
device.local.usb3Optimize	**0 or 1**	**0**
Optimizes the USB port on the system for a USB 3 connection when a computer is connected to the USB port on the power data box. If set to 1, the USB port is optimized for a USB 3 connection. If set to 0, the USB port is not optimized for a USB 3 connection.		
device.local.enableMacSupport	**0 or 1**	**1**
Enables Mac OS support for the system. If set to 1, the system supports Skype for Business calls on a connected Mac computer. If set to 0, the system does not support Skype for Business calls on a connected Mac computer.		
device.local.fishEyeEnable	**0 or 1**	**0**
Enables the Fisheye Correction feature to correct video distortion for Active Speaker video. If set to 1, Fisheye Correction is enabled, and Active Speaker video does not appear distorted. If set to 1, If set to 1, Fisheye Correction is disabled, and Active Speaker video appears distorted.		
device.local.ntpEnable	**0 or 1**	**0**
Enables Network Time Protocol (NTP). If set to 1, NTP is enabled. If set to 0, NTP is disabled.		
device.local.ntpServer	**string**	
Sets the NTP server that is used when the parameter `device.local.ntpEnable` is enabled.		

Device Parameters (continued)

Parameter	*Permitted Values*	*Default*
device.local.deviceName	**string**	
Sets the device name for each system.		
device.local.updateServer	**string**	**http://downloads.polycom.com/voice/millennium_cx_series**
Sets the server URL the system uses to retrieve software updates.		
device.local.autoUpdateEnabled	**0 or 1**	**0**
Enables the system to automatically check for software updates. If set to 1, the system checks for updates at a specified time. If set to 0, the system does not check for updates.		
device.local.updateInterval	**-1 (never) or a number greater than or equal to 0.**	**-1**
Sets the frequency for how often the system checks for software updates on the server.		
device.local.updateTime	**A number greater than or equal to 0**	**0**
Sets the time when the system checks for software updates.		
device.local.muteType	**0 = Audio only** **1 = Audio and Video**	**0**
Sets the function of the Mute button on the system.		
device.local.lightingFrequency	**0, 1, or 2**	**0**
Sets the power frequency of the system. 0 = 50Hz 1 = 60HZ 2 = 50HZ at 30fps		
device.logincred.password[1]	**string**	
The user password that the system uses to connect to the provisioning server.		
device.logincred.user[1]	**string**	
The user name that the system uses to connect to the provisioning server.		
device.net.cdpEnabled[1]	**0 or 1**	
If set to 1, the system attempts to determine its VLAN ID and negotiate power through CDP.		

Device Parameters (continued)

Parameter	*Permitted Values*	*Default*
device.net.dot1x.anonid[1]	**string**	
EAP-TTLS and EAP-FAST only. The anonymous identity (user name) for 802.1X authentication.		
device.net.dot1x.enabled[1]	**0 or 1**	
If 0, 802.1X authentication is disabled. If 1, 802.1X authentication is enabled.		
device.net.dot1x.identity[1]	**string**	
The identity (user name) for 802.1X authentication.		
device.net.dot1x.method	**EAP-None, EAP-TLS, EAP-PEAPv0-MSCHAPv2, EAP-PEAPv0-GTC, EAP-TTLS-MSCHAPv2, EAP-TTLS-GTC, EAP-FAST, EAP-MD5**	
Specify the 802.1X authentication method, where `EAP-NONE` means no authentication.		
device.net.dot1x.password[1]	**string**	
The password for 802.1X authentication. This parameter is required for all methods except EAP-TLS.		
device.net.etherModeLAN[1]	**Auto, 10HD, 10FD, 100HD, 100FD, 1000FD**	
The LAN port mode that sets the network speed over Ethernet. HD means half-duplex and FD means full duplex. Note: Polycom recommends that you do not change this setting.		
device.net.etherModePC[1]	**Disabled, Auto, 10HD, 10FD, 100HD, 100FD, 1000FD**	**Auto**
The PC port mode that sets the network speed over Ethernet. If set to `Disabled`, the PC port is disabled. HD means half duplex and FD means full duplex.		
device.net.etherStormFilter[1]	**0 or 1**	
If 1, DoS storm prevention is enabled and received Ethernet packets are filtered to prevent TCP/IP stack overflow caused by bad data or too much data. If 0, DoS storm prevention is disabled.		
device.net.etherVlanFilter[1]	**0 or 1**	

Device Parameters (continued)

Parameter	*Permitted Values*	*Default*
VLAN filtering is done by the Linux operating system and it cannot be disabled.		
device.net.ipAddress[1]	**string**	
The system's IP address. Note: This parameter is disabled when DHCP is enabled (`device.dhcp.enabled` is set to 1.		
device.net.IPgateway[1]	**IP address**	
The system's default router.		
device.net.lldpEnabled[1]	**0 or 1**	
If set to 1, the system attempts to determine its VLAN ID and negotiate power through LLDP.		
device.net.subnetMask[1]	**subnet mask**	
The system's subnet mask. Note: This parameter is disabled when DHCP is enabled (`device.dhcp.enabled` is set to 1).		
device.net.vlanId[1]	**Null, 0-4094**	
The system's 802.1Q VLAN identifier. If Null, no VLAN tagging.		
device.prov.maxRedunServers[1]	**1 to 8**	
The maximum number of IP addresses to use from the DNS.		
	0 or 1	**1**
If set to 1, the system will attempt to check for the latest version available on update server.		
device.prov.password[1]	**string**	
The password for the system to log in to the provisioning server. Note that a password may not be required. Note: If you modify this parameter, the system re-provisions. The system may also reboot if the configuration on the provisioning server has changed.		
device.prov.redunAttemptLimit[1]	**1 to 10**	
The maximum number of attempts to attempt a file transfer before the transfer fails. When multiple IP addresses are provided by DNS, 1 attempt is considered to be a request sent to each server.		
device.prov.redunInterAttemptDelay[1]	**0 to 300**	
The number of seconds to wait after a file transfer fails before retrying the transfer. When multiple IP addresses are returned by DNS, this delay only occurs after each IP has been tried.		
device.prov.serverName	**IP address, domain name string, or URL**	

Device Parameters (continued)

Parameter	*Permitted Values*	*Default*
The IP address, domain name, or URL of the provisioning server, followed by an optional directory and optional configuration filename. This parameter is used if DHCP is disabled (`device.dhcp.enabled` is `0`), if the DHCP server does not send a boot server option, or if the boot server option is static (`device.dhcp.bootSrvUseOpt` is `static`). Note: If you modify this parameter, the system re-provisions. The system may also reboot if the configuration on the provisioning server has changed.		
device.prov.serverType[1]	**FTP, TFTP, HTTP, HTTPS, FTPS**	
The protocol the system uses to connect to the provisioning server. Note: Active FTP is not supported for BootROM version 3.0 or later. Note: Only implicit FTPS is supported.		
device.prov.upgradeServer	**string**	
A browser-based Software Upgrade button that enables the user to upgrade the system with a compatible software version available on the Polycom provisioning server.		
device.prov.tagSerialNo	**0 or 1**	
If 0, the system's serial number (MAC address) is not included in the User-Agent header of HTTPS/HTTPS transfers and communications to the microbrowser and web browser. If 1, the system's serial number is included.		
device.prov.user	**string**	
The user name required for the system to log in to the provisioning server (if required). Note: If you modify this parameter, the system re-provisions. The system may also reboot if the configuration on the provisioning server has changed.		
device.prov.ztpEnabled	**0 or 1**	
If 0, Disable the ZTP feature. If 1, enable the ZTP feature. For information, see Polycom Zero Touch Provisioning Solution.		
device.sec.configEncryption.key[1]	**string**	
The configuration encryption key used to encrypt configuration files. For more information, see the section Encrypt Configuration Files.		
device.sec.coreDumpEncryption.enabled	**0 or 1**	**1**
This parameter enables you to bypass the encryption of the core dump. When set to 1, the core dump is encrypted. When set to 0, encryption of the core dump is bypassed.		
device.sec.TLS.customCaCert1 (TLS Platform Profile 1) **device.sec.TLS.customCaCert2 (TLS Platform Profile 2)**	**string, PEM format**	
The custom certificate to use for TLS Platform Profile 1 and TLS Platform Profile 2 and TLS Application Profile 1 and TLS Application Profile 2 `device.sec.TLS.profile.caCertList` must be configured to use a custom certificate. Custom CA certificate cannot exceed 4096 bytes total size.		

Device Parameters (continued)

Parameter	*Permitted Values*	*Default*
device.sec.TLS.customDeviceCert1.publicCert **device.sec.TLS.customDeviceCert2.publicCert**	**Enter the signed custom device certificate in PEM format (X.509)**	
device.sec.TLS.customDeviceCert1.privateKey **device.sec.TLS.customDeviceCert2.privateKey**	**Enter the corresponding signed private key in PEM format (X.509)**	
device.sec.TLS.customDeviceCert1.set **device.sec.TLS.customDeviceCert2.set** Note that you use a single `.set` parameter to enable or disable only these two related <`device/`> parameters - `device.sec.TLS.customDeviceCertX.publicCert` and `device.sec.TLS.customDeviceCertX.privateKey.` All other <`device/`> parameters have their own corresponding `.set` parameter that enables or disables that parameter. Size constraints are: 4096 bytes for the private key, 8192 bytes for the device certificate.	**0 or 1**	**0**
device.sec.TLS.profile.caCertList1 (TLS Platform Profile 1) **device.sec.TLS.profile.caCertList2 (TLS Platform Profile 2)** Choose the CA certificate(s) to use for TLS Platform Profile 1 and TLS Platform Profile 2 authentication: The built-in default certificate The built-in and Custom #1 certificates The built-in and Custom #2 certificates Any certificate (built in, Custom #1 or Custom #2) Only the Custom #1 certificate Only the Custom #2 certificate Either the Custom #1 or Custom #2 certificate	**Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1And Platform2**	
device.sec.TLS.profile.cipherSuite1 (TLS Platform Profile 1) **device.sec.TLS.profile.cipherSuite2 (TLS Platform Profile 2)** The cipher suites to use for TLS Platform Profile 1 and TLS Platform Profile 2)	**string**	

Device Parameters (continued)

Parameter	*Permitted Values*	*Default*
device.sec.TLS.profile.cipherSuiteDefault1 (TLS Platform Profile 1) **device.sec.TLS.profile.cipherSuiteDefault2 (TLS Platform Profile 2)**	**0 or 1**	
The cipher suite to use for TLS Platform Profile 1 and TLS Platform profile 2. If set to 0, the custom cipher suite is used. If set to 1, the default cipher suite is used.		
device.sec.TLS.profile.deviceCert1 (TLS Platform Profile 1) **device.sec.TLS.profile.deviceCert2 (TLS Platform Profile 2)**	**Builtin, Platform1, Platform2**	
Choose the device certificate(s) for TLS Platform Profile 1 and TLS Platform Profile 2 to use for authentication.		
device.sec.TLS.profile.profileSelection.dot1x	**PlatformProfile1, PlatformProfile2**	
Choose the TLS Platform Profile to use for 802.1X, either TLS Platform Profile 1 or TLS Platform Profile 2.		
device.sec.TLS.profileSelection.provisioning[1]	**PlatformProfile1, PlatformProfile2**	
The TLS Platform Profile to use for provisioning, either TLS Platform Profile 1 or TLS Platform Profile 2.		
device.sec.TLS.profileSelection.syslog[1]	**PlatformProfile1, PlatformProfile2**	
The TLS Platform Profile to use for syslog, either TLS Platform Profile 1 or TLS Platform Profile 2.		
device.sec.TLS.prov.strictCertCommonNameValidation	**0 or 1**	**1**
If set to 1, provisioning always verifies the server certificate for commonName/SubjectAltName match with the server hostname that the system is trying to connect.		
device.sec.TLS.syslog.strictCertCommonNameValidation	**0 or 1**	**1**
If set to 1, syslog always verifies the server certificate for commonName/SubjectAltName match with the server hostname that the system is trying to connect.		
device.sntp.gmtOffset	**-43200 to 46800**	
The GMT offset—in seconds—to use for daylight savings time, corresponding to -12 to +13 hours.		
device.sntp.serverName	**IP address or domain name string**	

Device Parameters (continued)

Parameter	*Permitted Values*	*Default*
The SNTP server from which the system obtains the current time.		
device.syslog.facility	**0 to 23**	
A description of what generated the log message. For more information, see RFC 3164.		
device.syslog.prependMac[1]	**0 or 1**	
If 1, the system's MAC address is prepended to the log message sent to the syslog server.		
device.syslog.renderLevel[1]	**0 to 6**	
Specify the logging level that displays in the syslog. Note that when you choose a log level, you are including all events of an equal or greater severity level and excluding events of a lower severity level. The logging level you choose determines the lowest severity of events to log. **0** or **1**: SeverityDebug(7). **2** or **3**: SeverityInformational(6). **4**: SeverityError(3). **5:** SeverityCritical(2). **6:** SeverityEmergency(0).		
device.syslog.serverName	**IP address or domain name string**	
The syslog server IP address or domain name string.		
device.syslog.transport	**None, UDP, TCP, TLS**	
The transport protocol that the system uses to write to the syslog server. If set to None, transmission is turned off but the server address is preserved.		

[1] Change causes system to restart or reboot.

<diags/>

Use these parameters to enable and set up the remote packet capture feature.

Remote Packet Capture Parameters

Parameter	*Permitted Values*	*Default*
diags.dumpcore.enabled[1]	**0 or 1**	**1**
When enabled, the system generates a core file if it crashes. When disabled, the system does not generate a core file when it crashes. The default value is 1, enabled.		
diags.pcap.enabled	**0 or 1**	**0**
Enable or disable all on-board packet capture features.		
diags.telnetd.enabled	**0 or 1**	**0**
Enable or disable all on-board packet capture features using telnet.		

Remote Packet Capture Parameters (continued)

Parameter	*Permitted Values*	*Default*
diags.pcap.remote.enabled	**0 or 1**	**0**
Enable or disable the remote packet capture server.		
diags.pcap.remote.password	**alphanumeric**	**<MAC Address>**
Enter the remote packet capture password.		
diags.pcap.remote.port	**Valid TCP Port**	**2002**
Specify the TLS profile to use for each application.		

[1] Change causes system to restart or reboot.

<dns/>

The <dns/> parameters include:

- DNS-A
- DNS-NAPTR
- DNS-SRV

You can enter a maximum of 12 record entries for DNS-A, DNS-NAPTR, and DNS-SRV. records.

DNS-A

Add up to 12 DNS-A record entries using the parameters in the following table. Specify the address, name, and cache time interval for DNS-A record *x*, where x is from 1 to 12.

DNA-A Parameters

Parameter	*Permitted values*	*Default*
dns.cache.A.x.address	**IP version 4 address**	**Null**
IP address.		
dns.cache.A.x.name	**valid hostname**	**Null**
Hostname		
dns.cache.A.x.ttl	**300 to 536870912 (2^29), seconds**	**300**
The TTL describes the time period the system uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and its reset TTL timer again.		

DNS-NAPTR

Add up to 12 DNS-NAPTR record entries using parameters in the following table. Specify each parameter for DNS-NAPTR record *x*, where x is from 1 to 12.

DNS-NAPTR Parameters

Parameter	*Permitted values*	*Default*
dns.cache.NAPTR.x.flags	**A single character from [A-Z, 0-9]**	**Null**
The flags to control aspects of the rewriting and interpretation of the fields in the record. Characters are case-sensitive. At this time, only ‘S’, ‘A’, ‘U’, and ‘P’ are defined as flags. See RFC 2915 for details of the permitted flags.		
dns.cache.NAPTR.x.name	**domain name string**	**Null**
The domain name to which this resource record refers.		
dns.cache.NAPTR.x.order	**0 to 65535**	**0**
An integer specifying the order in which the NAPTR records must be processed to ensure the correct ordering of rules.		
dns.cache.NAPTR.x.preference	**0 to 65535**	**0**
A 16-bit unsigned integer that specifies the order in which NAPTR records with equal "order" values should be processed. Low numbers are processed before high numbers.		
dns.cache.NAPTR.x.regexp	**string containing a substitution expression**	**Null**
This parameter is currently unused. Applied to the original string held by the client. The substitution expression is applied in order to construct the next domain name to look up. The grammar of the substitution expression is given in RFC 2915.		
dns.cache.NAPTR.x.replacement	**domain name string with SRV prefix**	**Null**
The next name to query for NAPTR records depending on the value of the flags field. It must be a fully qualified domain-name.		
dns.cache.NAPTR.x.service	**string**	**Null**
Specifies the service(s) available down this rewrite path. For more information, see RFC 2915.		
dns.cache.NAPTR.x.ttl	**300 to 536870912 (2^29), seconds**	**300**
The TTL describes the time period the system uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and its reset TTL timer again.		

DNS-SRV

Add up to 12 DNS-SRV record entries using parameters in the following table. Specify each parameter for DNS-SRV record *x*, where x is from 1 to 12.

DNS-SRV Parameters

Parameter	*Permitted values*	*Default*
dns.cache.SRV.x.name	**domain name string with SRV prefix**	**Null**
The domain name string with SRV prefix.		
dns.cache.SRV.x.port	**0 to 65535**	**0**
The port on this target host of this service. For more information, see RFC 2782.		
dns.cache.SRV.x.priority	**0 to 65535**	**0**
The priority of this target host. For more information, see RFC 2782.		
dns.cache.SRV.x.target	**domain name string**	**Null**
The domain name of the target host. For more information, see RFC 2782.		
dns.cache.SRV.x.ttl	**300 to 536870912 (2^29), seconds**	**300**
The TTL describes the time period the system uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and its reset TTL timer again.		
dns.cache.SRV.x.weight	**0 to 65535**	**0**
A server selection mechanism. For more information, see RFC 2782.		

<httpd/>

The system contains a local Web Configuration Utility server for user and administrator features. Note that several of these parameters can be used with Microsoft Skype for Business Server and have two default states: a generic default value and a different value when the system is registered with Skype for Business Server. The following table lists the default values for both states where applicable.

The web server supports both basic and digest authentication. The authentication user name and password are not configurable for this release.

HTTPD (Web Server) Parameters

Parameter	*Permitted Values*	*Default*
httpd.enabled[1]	**0 or 1**	**Generic=1** **Lync=0**
If 0, the HTTP server is disabled (the Web Configuration Utility is also be disabled). If 1, the server is enabled.		
httpd.cfg.enabled[1]	**0 or 1**	**Generic=1** **Lync=0**
If 0, the Web Configuration Utility is disabled. If 1, the Web Configuration Utility is enabled.		

HTTPD (Web Server) Parameters (continued)

Parameter	*Permitted Values*	*Default*
httpd.cfg.port[1]	**1 to 65535**	**80**
Port is 80 for HTTP servers. Care should be taken when choosing an alternate port.		
httpd.cfg.secureTunnelEnabled[1]	**0 or 1**	**Generic=1** **Lync=0**
If 0, the web does not use a secure tunnel. If 1, the server connects through a secure tunnel.		
httpd.cfg.secureTunnelPort[1]	**1 to 65535**	**443**
The port to use for communications when the secure tunnel is used.		
httpd.cfg.secureTunnelRequired[1]	**0 or 1**	**1**
If 0, communications to the web server do not require a secure tunnel. If 1, communications do require a secure tunnel.		

[1] Change causes system to restart or reboot.

<license/>

The parameters listed in the next table enable you to configure the feature licensing system.

Feature License Parameters

Parameter	*Permitted Values*	*Default*
license.polling.time[1]	**00:00 – 23:59**	**02:00**
The time (using the 24-hour clock) to check if the license has expired.		

[1] Change causes system to restart or reboot.

Note: Removing the installed license
Once the license is installed on a system, it cannot be removed.

<log/>

The event logging system supports the classes of events listed in the table Logging Levels. Two types of logging are supported:

- level, change, and render
- <sched/>

Caution: Changing the logging parameters
Logging parameter changes can impair system operation. Do not change any logging parameters without prior consultation with Polycom Technical Support.

Logging Levels

Logging Level	*Interpretation*
0	Debug only
1	High detail class event
2	Moderate detail event class
3	Low detail event class
4	Minor error—graceful recovery
5	Major error—will eventually incapacitate the system
6	Fatal error

Each event in the log contains the following fields separated by the | character:

- time or time/date stamp
- 1-5 character component identifier (such as “so”)
- event class
- cumulative log events missed due to excessive CPU load
- free form text - the event description

Three formats available for the event timestamp are listed in the next table.

Event Timestamp Formats

0 - seconds.milliseconds	011511.006 -- 1 hour, 15 minutes, 11.006 seconds since booting.
1 - absolute time with minute resolution	0210281716 -- 2002 October 28, 17:16
2 - absolute time with seconds resolution	1028171642 -- October 28, 17:16:42

<level/> <change/> and <render/>

This configuration parameter is defined in the following table.

Logging Level, Change, and Render Parameters

Parameter	*Permitted Values*	*Default*
log.level.change.xxx	**0 to 6**	**4**
Control the logging detail level for individual components. These are the input filters into the internal memory-based log system. Possible values for xxx are acom, ares, app1, bluet, bdiag, brow, bsdir, cap, cdp, cert, cfg, cipher, clink, clist, cmp, cmr, copy, curl, daa, dapi, dbs, dbuf, dhcpc, dis, dock, dot1x, dns, drvbt, ec, efk, ethf, flk, h323, hset, httpa, httpd, hw, ht, ib, key, ldap, lic, lldp, loc, log, mb, mobil, net, niche, ocsp, osd, pcap, pcd, pdc, peer, pgui, pmt, poll, pps, pres, pstn, ptt, push, pwrsv, rdisk, res, rtos, rtls, sec, sig, sip, slog, so, srtp, sshc, ssps, style, sync, sys, ta, task, tls, trace, ttrs, usb, usbio, util, utilm, wdog, wmgr, and xmpp.		

Logging Level, Change, and Render Parameters (continued)

Parameter	*Permitted Values*	*Default*
log.level.change.prox	**0 - 6**	**4**
Initial logging level for the Proximity log module.		
log.level.change.ptp	**0 - 6**	**4**
Initial logging level for the Precision Time Protocol log module.		
log.render.file	**0 or 1**	**1**
Set to 1. Polycom recommends that you do not change this value.		
log.render.file.size	**positive integer, 1 to 180**	**32**
Maximum size of flash memory for logs in Kbytes. When this size is about to be exceeded, the system uploads all logs that have not yet been uploaded, and erase half of the logs on the system. The administrator may use web browser to read all logs on the system.		
log.render.file.upload.append	**0 or 1**	**1**
If set to 1, use append mode when uploading log files to server. Note: HTTP and TFTP don't support append mode unless the server is set up for this.		
log.render.file.upload.append.limitMode	**delete, stop**	**delete**
Behavior when server log file has reached its limit. delete=delete file and start over stop=stop appending to file		
log.render.file.upload.append.sizeLimit	**positive integer**	**512**
Maximum log file size that can be stored on provisioning server in Kbytes.		
log.render.file.upload.period	**positive integer**	**172800**
Time in seconds between log file uploads to the provisioning server. Note: The log file is not uploaded if no new events have been logged since the last upload.		
log.render.level	**0 to 6**	**1**
Specifies the lowest class of event rendered to the log files. This is the output filter from the internal memory-based log system. The log.render.level maps to syslog severity as follows: 0 SeverityDebug (7) 1 SeverityDebug (7) 2 SeverityInformational (6) 3 SeverityInformational (6) 4 SeverityError (3) 5 SeverityCritical (2) 6 SeverityEmergency (0)		
log.render.realtime	**0 or 1**	**1**
Set to 1. Polycom recommends that you do not change this value.		
log.render.stdout	**0 or 1**	**0**

Logging Level, Change, and Render Parameters (continued)

Parameter	*Permitted Values*	*Default*
Set to 0. Polycom recommends that you do not change this value.		
log.render.type	**0 to 2**	**2**
Refer to the table Event Timestamp Formats for timestamp type.		

<sched/>

The system can be configured to schedule certain advanced logging tasks on a periodic basis. Polycom recommends that you set the parameters listed in the next table in consultation with Polycom Technical Support. Each scheduled log task is controlled by a unique parameter set starting with log.sched.x where *x* identifies the task. A maximum of 10 schedule logs is allowed.

Logging Schedule Parameters

Parameter	*Permitted Values*	*Default Value*
log.sched.x.level	**0 to 5**	**3**
Event class to assign to the log events generated by this command. This needs to be the same or higher than log.level.change.slog for these events to display in the log.		
log.sched.x.name	**alphanumeric string**	
Name of an internal system command to be periodically executed. To be supplied by Polycom.		
log.sched.x.period	**positive integer**	**15**
Seconds between each command execution. 0=run once		
log.sched.x.startDay	**0 to 7**	**7**
When startMode is abs, specifies the day of the week to start command execution. 1=Sun, 2=Mon, ..., 7=Sat		
log.sched.x.startMode	**0 - 64**	
Start at an absolute time or relative to boot.		
log.sched.x.startTime	**positive integer OR hh:mm**	
Seconds since boot when startMode is rel or the start time in 24-hour clock format when startMode is abs.		

<nat/>

The parameters listed in the next table define port and IP address changes used in NAT traversal. The port changes alter the port used by the system, while the IP entry simply changes the IP advertised in the SIP signaling. This allows the use of simple NAT devices that can redirect traffic, but does not allow for port mapping. For example, port 5432 on the NAT device can be sent to port 5432 on an internal device, but not to port 1234.

Network Access Translation Parameters

Parameter	*Permitted Values*	*Default*
nat.ip[1]	**IP address**	**Null**
IP address to advertise within SIP signaling - should match the external IP address used by the NAT device.		
nat.keepalive.interval	**0 to 3600**	**0**
The keep-alive interval in seconds. Sets the interval at which systems sends a keepalive packet to the gateway/NAT device to keep the communication port open so that NAT can continue to function. If Null or 0, the system does not send out keepalive messages.		
nat.mediaPortStart[1]	**0 to 65440**	**0**
The initially allocated RTP port. Overrides the value set for `tcpIpApp.port.rtp.mediaPortRangeStart`.		
nat.signalPort[1]	**1024 to 65535**	**0**
The port used for SIP signaling. Overrides `voIpProt.local.port`.		

[1] Change causes system to restart or reboot.

<prov/>

The parameters listed in the next table control the provisioning server for your systems.

Provisioning Parameters

Parameter	*Permitted Values*	*Default*
prov.autoConfigUpload.enabled	**0 or 1**	**1**
Enable or disable the automatic upload Web Configuration Utility override configuration files to the provisioning server. By default, `MAC-web.cfg` files are automatically uploaded to the provisioning server when a configuration change is made from the Web Configuration Utility respectively. When disabled, per-system override files are not uploaded to the provisioning server.		
prov.configUploadPath	**string**	**Null**
The directory - relative to the provisioning server - where the system uploads the current configuration file when the user selects Upload Configuration. If set to Null, use the provisioning server directory.		
prov.login.automaticLogout	**0 to 46000**	**0**
The time (in minutes) before a non-default user is automatically logged out of the handset. If 0, the user is not automatically logged out.		
prov.login.defaultPassword	**String**	**Null**
The login password for the default user.		
prov.login.defaultOnly	**0 or 1**	**0**
If 1, the default user is the only user who can log in. If 0, other users can log in.		

Provisioning Parameters (continued)

Parameter	*Permitted Values*	*Default*
prov.login.defaultUser	**String**	**Null**
The username for the default user. If present, the user is automatically logged in when the system boots up and logged in after another user logs out.		
prov.login.enabled	**0 or 1**	**0**
If 0, the user profile feature is disabled. If 1, the user profile feature is enabled.		
prov.login.lcCache.domain	**0 to 64**	**Null**
The user's sign-in domain name.		
prov.login.lcCache.user	**0 to 64**	**Null**
The user's sign-in user name.		
prov.login.localPassword	**String**	**123**
The password used to validate the user login. It is stored either as plain text or encrypted (an SHA1 hash).		
prov.login.persistent	**0 or 1**	**0**
If 0, users are logged out if the handset reboots. If 1, users remain logged in when the system reboots.		
prov.login.required	**0 or 1**	**0**
If 1, a user must log in when the login feature is enabled. If 0, the user does not have to log in.		
prov.loginCredPwdFlushed.enabled	**0 or 1**	**1**
If 1, when a user logs in or logs out, the login credential password is reset. If 0, the login credential password is not reset.		
prov.polling.enabled	**0 or 1**	**0**
If 0, the provisioning server is not automatically polled for upgrades. If 1, the provisioning server is polled.		
prov.polling.mode	**abs, rel, random**	**abs**
The polling mode. `abs` The system polls every day at the time specified by `prov.polling.time`. `rel` The system polls after the number of seconds specified by `prov.polling.period`. `random` The system polls at random between a starting time set in `prov.polling.time` and an end time set in `prov.polling.timeRandomEnd`. Note that if you set the polling period in `prov.polling.period` to a time greater than 86400 seconds (one day) polling occurs on a random day within that polling period (meaning values such as 86401 would be over 2 days) and only between the start and end times. The day within the period is decided based upon the systems MAC address and does not change with a reboot whereas the time within the start and end is calculated again with every reboot.		
prov.polling.period	**integer > 3600**	**86400**
The polling period in seconds. The polling period is rounded up to the nearest number of days in absolute and random mode. In relative mode, the polling period starts once the system boots. In random mode, if this is set to a time greater than 86400 (one day) polling occurs on a random day based on the system's MAC address.		

Provisioning Parameters (continued)

Parameter	*Permitted Values*	*Default*
prov.polling.time	**hh:mm**	**03:00**
The polling start time. Used in absolute and random modes.		
prov.polling.timeRandomEnd	**hh:mm**	**Null**
The polling stop time. Only used in random mode.		
prov.quickSetup.enabled	**0 or 1**	**0**
If 0, the quick setup feature is disabled. If 1, the quick setup feature is enabled.		

[1] Change causes system to restart or reboot.

<qos/>

These parameters listed in the next table configure the following Quality of Service (QoS) options:

- The 802.1p/Q user_priority field RTP, call control, and other packets
- The “type of service” field RTP and call control packets

Quality of Service (Type-of-Service) Parameters

Parameter	*Permitted Values*	*Default*
qos.ethernet.callControl.user_priority[1]	**0 to 7**	**5**
User-priority used for call control packets.		
qos.ethernet.other.user_priority[1]	**0 to 7**	**2**
User-priority used for packets that do not have a per-protocol setting.		
qos.ethernet.rtp.user_priority[1]	**0 to 7**	**5**
Choose the priority of voice Real-Time Protocol (RTP) packets. The default priority level is 5.		
qos.ethernet.rtp.video.user_priority[1]	**0 to 7**	**5**
User-priority used for Video RTP packets.		
qos.ip.callControl.dscp[1]	**0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43**	**Null**
Specify the DSCP of packets. If the value is not null, this parameter overrides the other `qos.ip.callControl.*` parameters. The default value is Null, so the other `qos.ip.callControl.*` parameters are used if no value is entered.		

Quality of Service (Type-of-Service) Parameters (continued)

Parameter	*Permitted Values*	*Default*
qos.ip.callControl.max_reliability[1]	**0 or 1**	**0**
qos.ip.callControl.max_throughput[1]	**0 or 1**	**0**
qos.ip.callControl.min_cost[1]	**0 or 1**	**0**
qos.ip.callControl.min_delay[1]	**0 or 1**	**1**
qos.ip.callControl.precedence[1]	**0 -7**	**5**
Set the bits in the IP ToS field of the IP header used for call control. Specify whether or not to set the max reliability bit, the max throughput bit, the min cost bit, the min delay bit, and the precedence bits. If 0, the bit in the IP ToS field of the IP header is not set. If 1, the bit is set.		
qos.ip.rtp.dscp[1]	**0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43**	**Null**
Specify the DSCP of packets. If the value is not null, this parameter overrides the other `qos.ip.rtp.*` parameters. The default value is Null, so the other `quality.ip.rtp.*` parameters are used.		
qos.ip.rtp.max_reliability[1]	**0 or 1**	**0**
qos.ip.rtp.max_throughput[1]	**0 or 1**	**1**
qos.ip.rtp.min_cost[1]	**0 or 1**	**0**
qos.ip.rtp.min_delay[1]	**0 or 1**	**1**
qos.ip.rtp.precedence[1]	**0 -7**	**5**
Set the bits in the IP ToS field of the IP header used for RTP. Specify whether or not to set the max reliability bit, the max throughput bit, the min cost bit, the min delay bit, and the precedence bit. If 0, the bit in the IP ToS field of the IP header is not set. If 1, the bit is set.		
qos.ip.rtp.video.dscp[1]	**0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43**	**Null**
Allows the DSCP of packets to be specified. If the value is non-null, this parameter overrides the other `qos.ip.rtp.video.*`parameters. The default value is Null, so the other `qos.ip.rtp.video.*` parameters are used.		
qos.ip.rtp.video.max_reliability[1]	**0 or 1**	**0**
qos.ip.rtp.video.max_throughput[1]	**0 or 1**	**1**
qos.ip.rtp.video.min_cost[1]	**0 or 1**	**0**
qos.ip.rtp.video.min_delay[1]	**0 or 1**	**1**
qos.ip.rtp.video.precedence[1]	**0 -7**	**5**
Set the bits in the IP ToS field of the IP header used for RTP video. Specify whether or not to set the max reliability bit, the max throughput bit, the min cost bit, the min delay bit, and the precedence bit. If 0, the bit in the IP ToS field of the IP header is not set. If 1, the bit is set.		

[1] Change causes system to restart or reboot.

<sec/>

The parameters listed in the next table configure security features of the system.

General Security Parameters

Parameter	*Permitted Values*	*Default*
sec.tagSerialNo[1]	**0 or 1**	**0**
If 0, the system does not advertise its serial number (MAC address) through protocol signaling. If 1, the system may advertise its serial number through protocol signaling.		

[1] Change causes system to restart or reboot.

This parameter also includes:

- <encryption/>
- <pwd/><length/>
- <srtp/>
- <dot1x><eapollogoff/>
- <hostmovedetect/>
- <TLS/>

<encryption/>

The next table lists available encryption parameters.

File Encryption Parameters

Parameter	*Permitted Values*	*Default*
sec.encryption.upload.config	**0 or 1**	**0**
The encryption on the system-specific configuration file created and uploaded to the provisioning server. If 0, the file is uploaded unencrypted, and overwrites whatever system-specific configuration file is on the server, even if the file on the server is encrypted. If 1, the file is uploaded encrypted and replaces any existing system-specific configuration file on the server. If there is no encryption key on the system, the file is not uploaded.		
sec.encryption.upload.overrides	**0 or 1**	**0**
The encryption on the system-specific **<MACaddress>-system.cfg** override file that is uploaded to the server. If 0, the file is uploaded unencrypted regardless of how it was downloaded, the file replaces whatever file was on the server, even if the file on the server is encrypted. If 1, the file is uploaded encrypted regardless of how it was downloaded. The file replaces any existing system-specific override file on the server.		

[1] Change causes system to restart or reboot.

<pwd/><length/>

The next table lists configurable password length parameters.

Password Length Parameters

Parameter	Permitted Values	Default
sec.pwd.length.admin[1]	**0-32**	**1**
The minimum length for administrator passwords changed using the system. Use 0 to allow null passwords.		
sec.pwd.length.user[1]	**0-32**	**2**
The minimum length for user passwords changed using the system. Use 0 to allow null passwords.		

[1] Change causes system to restart or reboot.

<srtp/>

As per RFC 3711, you cannot turn off authentication of RTCP. The next table lists SRTP parameters.

SRTP Parameters

Parameter	*Permitted values*	*Defaults*
sec.srtp.enable[1]	**0 or 1**	**1**
If 0, the system always declines SRTP offers. If 1, the system accepts SRTP offers.		
sec.srtp.key.lifetime[1]	**0, positive integer minimum 1024 or power of 2 notation**	**Null**
The lifetime of the master key used for the cryptographic parameter in SDP. The value specified is the number of SRTP packets. If 0, the master key lifetime is not set. If set to a valid value (at least 1024, or a power such as 2^10), the master key lifetime is set. When the lifetime is set, a re-invite with a new key is sent when the number or SRTP packets sent for an outgoing call exceeds half the value of the master key lifetime. Note: Setting this parameter to a non-zero value may affect the performance of the system.		
sec.srtp.mki.enabled[1]	**0 or 1**	**Lync = 1** **Generic = 0**
If enabled, the system sends two encrypted attributes in the SDP, one with MKI and one without MKI. If disabled, the system sends only one encrypted attributed without MKI.		
sec.srtp.mki.startSessionAtOne	**0 or 1**	**0**
If set to 1, use an MKI value of 1 at the start of an SDP session. If set to 0, the MKI value increments for each new crypto key.		
sec.srtp.offer[1]	**0 or 1**	**0**
If 1, the system includes a secure media stream description along with the usual non-secure media description in the SDP of a SIP INVITE. This parameters applies to the system initiating (offering) a call. If 0, no secure media stream is included in SDP of a SIP invite.		
sec.srtp.offer.HMAC_SHA1_32[1]	**0 or 1**	**0**
If 1, a crypto line with the `AES_CM_128_HMAC_SHA1_32` crypto-suite is included in offered SDP. If 0, the crypto line is not included.		

SRTP Parameters (continued)

Parameter	*Permitted values*	*Defaults*
sec.srtp.offer.HMAC_SHA1_80[1]	**0 or 1**	**1**
If 1, a crypto line with the `AES_CM_128_HMAC_SHA1_80` crypto-suite is included in offered SDP. If 0, the crypto line is not included.		
sec.srtp.padRtpToFourByteAlignment[1]	**0 or 1**	**0**
Packet padding may be required when sending or receiving video from other video products. If 1, RTP packet padding is needed. If 0, no packet padding is needed.		
sec.srtp.require[1]	**0 or 1**	**0**
If 0, secure media streams are not required. If 1, the system is only allowed to use secure media streams. Any offered SIP INVITEs must include a secure media description in the SDP or the call is rejected. For outgoing calls, only a secure media stream description is included in the SDP of the SIP INVITE, meaning that the non-secure media description is not included. If this parameter set to 1, `sec.srtp.offer` is also set to 1, regardless of the value in the configuration file.		
sec.srtp.requireMatchingTag[1]	**0 or 1**	**1**
If 0, the tag values in the crypto parameter in an SDP answer are ignored. If 1, the tag values must match.		
sec.srtp.sessionParams.noAuth.offer[1]	**0 or 1**	**0**
If 0, authentication of RTP is offered. If 1, no authentication of RTP is offered; a session description that includes the `UNAUTHENTICATED_SRTP` session parameter is sent when initiating a call.		
sec.srtp.sessionParams.noAuth.require[1]	**0 or 1**	**0**
If 0, authentication of RTP is required. If 1, no authentication of RTP is required; a call placed to a system configured with this parameter must offer the UNAUTHENTICATED_SRTP session parameter in its SDP. If this parameter is set to 1, `sec.srtp.sessionParams.noAuth.offer` is also set to 1, regardless of the value in the configuration file.		
sec.srtp.sessionParams.noEncrypRTCP.offer[1]	**0 or 1**	**0**
If 0, encryption of RTCP is offered. If 1, no encryption of RTCP is offered; a session description that includes the UNENCRYPTED_SRTCP session parameter is sent when initiating a call.		
sec.srtp.sessionParams.noEncrypRTCP.require[1]	**0 or 1**	**0**
If set to 0, encryption of RTCP is required. If set to 1, no encryption of RTCP is required; a call placed to a system configured with `noAuth.require` must offer the UNENCRYPTED_SRTCP session parameter in its SDP. If this parameter is set to 1, `sec.srtp.sessionParams.noEncryptRTCP.offer` is also set to 1, regardless of the value in the configuration file.		
sec.srtp.sessionParams.noEncrypRTP.offer[1]	**0 or 1**	**0**
If 0, encryption of RTP is offered. If 1, no encryption of RTP is offered; a session description that includes the UNENCRYPTED_SRTP session parameter is sent when initiating a call.		
sec.srtp.sessionParams.noEncrypRTP.require[1]	**0 or 1**	**0**
If 0, encryption of RTP is required. If 1, no encryption of RTP is required. A call placed to a system configured with noAuth.require must offer the UNENCRYPTED_SRTP session parameter in its SDP. If set to 1, sec.srtp.sessionParams.noEncryptRTP.offer is also set to 1, regardless of the value in the configuration file.		

SRTP Parameters (continued)

Parameter	*Permitted values*	*Defaults*
sec.srtp.simplifiedBestEffort	**0 or 1**	**0**
If 0, no SRTP is supported. If 1, negotiation of SRTP compliant with Microsoft Session Description Protocol Version 2.0 Extensions is supported.		

[1] Change causes system to restart or reboot.

<dot1x><eapollogoff/>

The next table lists configurable parameters.

802.1X EAP over LAN (EAPOL) Logoff Parameters

Parameter	*Permitted Values*	*Default*
sec.dot1x.eapollogoff.enabled[1]	**0 or 1**	**0**
If 0, the system does not send an EAPOL Logoff message on behalf of the disconnected supplicant. If 1, the feature is enabled and the system sends an EAPOL Logoff message on behalf of the disconnected supplicant connected to the system's secondary (PC) port.		
sec.dot1x.eapollogoff.lanlinkreset[1]	**0 or 1**	**0**
If 0, the system software does not reset (recycle) the LAN port link in the application initiation stage. If 1, the LAN port link resets in the application initiation stage.		

[1] Change causes system to restart or reboot.

<hostmovedetect/>

The next table lists configurable parameters.

Host Movement Detection Parameters

Parameter	*Permitted Values*	*Default*
sec.hostmovedetect.cdp.enabled[1]	**0 or 1**	**0**
If set to 1, the system software unconditionally sends a CDP packet (to the authenticator switch port) to indicate a host has been connected or disconnected to its secondary (PC) port.		
sec.hostmovedetect.cdp.sleepTime[1]	**0 to 60000**	**1000**
If `sec.hostmovedetect.cdp.enabled` is set to 1, there is an x microsecond time interval between two consecutive link–up state change reports, which reduces the frequency of dispatching CDP packets.		

[1] Change causes system to restart or reboot.

<TLS/>

The next table lists configurable TLS parameters. For the list of configurable ciphers, refer to the table .

This parameter also includes:

- <profile/>
- <profileSelection/>.

TLS Parameters

Parameter	*Permitted Values*	*Default*
sec.TLS.browser.cipherList	**String**	**NoCipher**
The cipher list for browser. The format for the cipher list uses OpenSSL syntax found at: http://www.openssl.org/docs/apps/ciphers.html.		
sec.TLS.cipherList	**String**	**“RSA:!EXP:!LOW:!NULL:!MD5:@STRENGTH”**
The global cipher list parameter. The format for the cipher list uses OpenSSL syntax found at: http://www.openssl.org/docs/apps/ciphers.html.		
sec.TLS.customCaCert.x	**String**	**Null**
The custom certificate for TLS Application Profile x (x= 1 to 6).		
sec.TLS.customDeviceCert.x	**String**	**Null**
The custom device certificate for TLS Application Profile x (x= 1 to 6).		
sec.TLS.customDeviceKey.x	**String**	**Null**
The custom device certificate private key for TLS Application Profile x (x= 1 to 6).		
sec.TLS.LDAP.cipherList	**String**	**NoCipher**
The cipher list for the corporate directory. The format for the cipher list uses OpenSSL syntax found here: http://www.openssl.org/docs/apps/ciphers.html.		
sec.TLS.profileSelection.SOPI	**1 - 7**	**PlatformProfile1**
Select the platform profile you want to use. You can choose platform profile 1 - 7.		
sec.TLS.profile.x.caCert.application7	**0 or 1**	**1**
Enable or disable the ability to choose a CA certificate for the application7 profile.		
sec.TLS.profile.webServer.cipherSuiteDefault	**0 or 1**	**1**
If 0, use the custom cipher suite for web server profile. If 1, use the default cipher suite.		
sec.TLS.prov.cipherList	**String**	**NoCipher**
The cipher list for provisioning. The format for the cipher list uses OpenSSL syntax found here: http://www.openssl.org/docs/apps/ciphers.html.		
sec.TLS.SIP.cipherList	**String**	**NoCipher**
The cipher list for SIP. The format for the cipher list uses OpenSSL syntax found here: http://www.openssl.org/docs/apps/ciphers.html.		
sec.TLS.SIP.strictCertCommonNameValidation	**0 or 1**	**1**

TLS Parameters (continued)

Parameter	*Permitted Values*	*Default*
If 1, enable common name validation for SIP.		
sec.TLS.SOPI.cipherList	**1 – 1024 character string**	**NoCipher**
Choose a cipher key.		
sec.TLS.SOPI.strictCertCommonNameValidation	**0 or 1**	**1**
Enable or disable strict common name validation for the URL provided by the server.		
sec.TLS.syslog.cipherList	**String**	**NoCipher**
The cipher list for syslog. The format for the cipher list uses OpenSSL syntax found here: http://www.openssl.org/docs/apps/ciphers.html.		
sec.TLS.webServer.cipherList	**String**	**RSA:!EXP:!LOW:!NULL:!MD5:!RC4:@STRENGTH**
The cipher list for a web server profile.		

<profile/>

Profiles are a collection of related security parameters. The next table lists TLS profile parameters. There are two platform profiles and six application profiles.

TLS Profile Parameters

Parameter	*Permitted Values*	*Default*
sec.TLS.profile.x.caCert.application1 **Application CA 1**	**0 or 1**	**1**
sec.TLS.profile.x.caCert.application2 **Application CA 2**	**0 or 1**	**1**
sec.TLS.profile.x.caCert.application3 **Application CA 3**	**0 or 1**	**1**
sec.TLS.profile.x.caCert.application4 **Application CA 4**	**0 or 1**	**1**
sec.TLS.profile.x.caCert.application5 **Application CA 5**	**0 or 1**	**1**
sec.TLS.profile.x.caCert.application6 **Application CA 6**	**0 or 1**	**1**
sec.TLS.profile.x.caCert.application7 **Application CA 7**	**0 or 1**	**1**
sec.TLS.profile.x.caCert.platform1 **Platform CA 1**	**0 or 1**	**1**
sec.TLS.profile.x.caCert.platform2 **Platform CA 2**	**0 or 1**	**1**
Specify which CA certificates should be used for TLS Application Profile x (where x is 1 to 7). If set to 0, the CA is not used. If set to 1, the CA is used.		
sec.TLS.profile.x.caCert.defaultList	**String**	**Null**
The list of default CA certificates for TLS Application Profile x (x= 1 to 7).		
sec.TLS.profile.x.cipherSuite	**String**	**Null**
The cipher suite for TLS Application Profile x (where x is 1 to 7).		
sec.TLS.profile.x.cipherSuiteDefault	**0 or 1**	**1**
If 0, use the custom cipher suite for TLS Application Profile x (x= 1 to 7). If 1, use the default cipher suite.		
sec.TLS.profile.x.deviceCert	**Polycom, Platform1, Platform2, Application1, Application2, Application3, Application4, Application5, Application6, Application7**	**Polycom**
The device certificate to use for TLS Application Profile x (x = 1 to 7).		

<profileSelection/>

You can configure the parameters listed in the next table to choose the platform profile or application profile to use for each TLS application.

The permitted values are:

- PlatformProfile1

- PlatformProfile2
- ApplicationProfile1
- ApplicationProfile2
- ApplicationProfile3
- ApplicationProfile4
- ApplicationProfile5
- ApplicationProfile6
- ApplicationProfile7

TLS Profile Selection Parameters

Parameter	*Permitted Values*	*Default*
sec.TLS.profileSelection.LDAP	**a TLS profile**	**PlatformProfile1**
The TLS platform profile or TLS application profile (see preceding list) to use for the Corporate Directory.		
sec.TLS.profileSelection.SIP	**a TLS profile**	**PlatformProfile1**
The TLS platform profile or TLS application profile (see preceding list) to use for SIP operations.		
sec.TLS.profileSelection.syslog	**PlatformProfile1 or PlatformProfile2**	**PlatformProfile1**
The TLS platform profile to use for syslog operations.		

<tcpIpApp/>

This parameter includes:

- <dhcp/>
- <dns/>
- <ice/>
- <sntp/>
- <port/><rtp/>
- <keepalive/>
- <fileTransfer/>

<dhcp/>

The DHCP parameters listed in the next table enable you to configure how the system reacts to DHCP changes.

DHCP Parameters

Parameter	*Permitted Values*	*Default*
tcpIpApp.dhcp.releaseOnLinkRecovery	**0 or 1**	**1**
If 0, no DHCP release occurs. If 1, a DHCP release is performed after the loss and recovery of the network.		

<dns/>

The <dns/> parameters listed in the next table enables you to set Domain Name System (DNS). However, any values set through DHCP have a higher priority and any values set through the <device/> parameter in a configuration file have a lower priority.

Domain Name System (DNS) Parameters

Parameter	Permitted Values	Default
tcpIpApp.dns.address.overrideDHCP[1]	**0 or 1**	**0**
If set to 0, a DNS address is requested from the DHCP server. When set to 1, a DNS primary and secondary address is set using the parameters `tcpIpApp.dns.server` and `tcpIpApp.dns.altServer`.		
tcpIpApp.dns.server[1]	**IP address**	**Null**
The primary server to which the system directs DNS queries.		
tcpIpApp.dns.altServer[1]	**IP address**	**Null**
The secondary server to which the system directs DNS queries.		
tcpIpApp.dns.domain[1]	**String**	**Null**
The system's DNS domain.		
tcpIpApp.dns.domain.overrideDHCP[1]	**0 or 1**	**0**
If set to 0, a domain name is retrieved from the DHCP server, if one is available. If set to 1, the DNS domain name is set using the parameter `tcpIpApp.dns.domain`.		

[1] Change causes system to restart or reboot.

<ice/>

Parameters in the following table enable you to set the STUN/TURN/ICE feature.

ICE Parameters

Parameter	*Permitted Values*	*Default*
tcpIpApp.ice.mode	**Disabled, Standard, MSOCS**	**Disabled**
Turn SIP ICE negotiation on or off. If using Lync Server 2010, set to MSOCS to enable ICE.		
tcpIpApp.ice.password	**String**	**Null**

ICE Parameters (continued)

Parameter	*Permitted Values*	*Default*
Enter the password to authenticate to the TURN server.		
tcpIpApp.ice.stun.server	**String**	**Null**
Enter the IP address of the STUN server.		
tcpIpApp.ice.stun.udpPort	**1-65535**	**3478**
The UDP port number of the STUN server.		
tcpIpApp.ice.tcp.enabled	**0 or 1**	**1**
If 0, TCP is disabled. If 1, TCP is enabled.		
tcpIpApp.ice.turn.callAdmissionControl.enabled		**1**
tcpIpApp.ice.turn.server	**String**	**Null**
Enter the IP address of the TURN server.		
tcpIpApp.ice.turn.tcpPort	**1-65535**	**443**
The UDP port number of the TURN server.		
tcpIpApp.ice.turn.udpPort	**1-65535**	**443**
The UDP port number of the TURN server.		
tcpIpApp.ice.username	**String**	**Null**
Enter the user name to authenticate to the TURN server.		

<sntp/>

The next table lists the Simple Network Time Protocol (SNTP) parameters used to set up time synchronization and daylight savings time. The default values enable and configure daylights savings time (DST) for North America.

Daylight savings time defaults:

- Do not use fixed day, use first or last day of week in the month.
- Start DST on the second Sunday in March at 2am.
- Stop DST on the first Sunday in November at 2am.

Simple Network Time Protocol (SNTP) Parameters

Parameter	*Permitted Values*	*Default*
tcpIpApp.sntp.address	**Valid hostname or IP address**	**Null**
The address of the SNTP server.		

Simple Network Time Protocol (SNTP) Parameters (continued)

Parameter	*Permitted Values*	*Default*
tcpIpApp.sntp.AQuery	**0 or 1**	**0**
If set to 0, queries to resolve the SNTP hostname are performed using DNS SRV. If set to 1, the host name is queried for a DNS A record instead.		
tcpIpApp.sntp.address.overrideDHCP	**0 or 1**	**0**
If 0, the DHCP values for the SNTP server address are used. If 1, the SNTP parameters override the DHCP values.		
tcpIpApp.sntp.retryDnsPeriod	**60 – 2147483647 seconds**	**86400**
Set a retry period for DNS queries. Note that the DNS retry period you configure is affected by other DNS queries made by the system. If the system makes a query for another service such as SIP registration during the retry period you configure and receives no response, the Network Time Protocol (NTP) DNS query is omitted to limit the overall number of retry attempts made to the unresponsive server. If no other DNS attempts are made by other services, then the rety period you configure is not affected. If at any time the DNS server becomes responsive to another service, then NTP also immediately retries its DNS query as well.		

<port/><rtp/>

The parameters listed in the next table enable you to configure the port filtering used for RTP traffic.

RTP Port Parameters

Parameter	*Permitted Values*	*Default*
tcpIpApp.port.rtp.filterByPort[1]	**0 or 1**	**0**
Ports can be negotiated through the SDP protocol. If set to 1, the system rejects RTP packets arriving from (sent from) a non-negotiated port.		
tcpIpApp.port.rtp.forceSend[1]	**0 to 65535**	**0**
Send all RTP packets to, and expect all RTP packets to arrive on, this port. If 0, RTP traffic is not forced to one port. Note: Both `tcpIpApp.port.rtp.filterByIp` and `tcpIpApp.port.rtp.filterByPort` must be set to 1 for this to work.		
tcpIpApp.port.rtp.mediaPortRangeEnd[1]	**Default, 1024 to 65485**	**2269**
Determines the maximum supported end range of audio ports.		
tcpIpApp.port.rtp.mediaPortRangeStart[1]	**even integer 1024 to 65440**	**2222**
The starting port for RTP packets. Ports are allocated from a pool starting with this port up to a value of (start-port + 47) for a voice-only system or (start-port + 95) for a video system. Note: Ensure that there is no contention for port numbers. For example, do not use 5060 (default port for SIP).		

[1] Change causes system to restart or reboot.

<keepalive/>

The parameters listed in the next table enable the configuration of TCP keep-alive on SIP TLS connections; the system can detect a failure quickly (in minutes) and attempt to re-register with the SIP call server (or its redundant pair).

TCP Keep-Alive Parameters

Parameter	*Permitted Values*	*Default*
tcpIpApp.keepalive.tcp.idleTransmitInterval	**10 to 7200**	**30**
The amount of time to wait (in seconds) before sending the keep-alive message to the call server. Note: If this parameter is set to a value that is out of range, the default value is used. Note: This parameter specifies the number of seconds TCP waits between transmission of the last data packet and the first keep-alive message.		
tcpIpApp.keepalive.tcp.noResponseTransmitInterval	**5 to 120**	**20**
If no response is received to a keep-alive message, subsequent keep-alive messages are sent to the call server at this interval (every x seconds). Note: This parameter specifies the amount of idle time between the transmission of the keep-alive packets the TCP stack waits. This applies whether the last keep-alive was acknowledged or not.		
tcpIpApp.keepalive.tcp.sip.tls.enable	**0 or 1**	**0**
If 0, disable TCP keep-alive for SIP signaling connections that use TLS transport. If 1, enable TCP keep-alive for SIP signaling connections that use TLS transport.		

[1] Change causes system to restart or reboot.

<fileTransfer/>

The parameters listed in the next table configure file transfers from the system to the provisioning server.

File Transfer Parameters

Parameter	*Permitted Values*	*Default*
tcpIpApp.fileTransfer.waitForLinkIfDown	**0 or 1**	**1**
If 1, file transfer from the FTP server is delayed until Ethernet comes back up. If 0, file transfer from the FTP server is not attempted.		

<upgrade/>

Use the parameters listed in the next table to specify the URL of a custom download server and the Polycom UC Software download server for the system to check when searching for software upgrades.

Upgrade Server Parameters

Parameter	Permitted Values	Default
upgrade.custom.server.url	**URL**	**Null**

Upgrade Server Parameters (continued)

The URL of a custom download server.		
upgrade.plcm.server.url	**URL**	`http://downloads.polycom.com/voice/millennium_cx_series`
The URL of the Polycom software download server.		

<video/>

The parameters in the following table include parameters you can use to configure video for the CX5100 system. This parameter also includes:

- <camera/>
- <codecs/>

Video Parameters

Parameter	*Permitted Values*	*Default*
video.autoFullScreen	**0 or 1**	**0**
If 0, video calls only use the full screen layout if it is explicitly selected by the user. If 1, video calls use the full screen layout by default, such as when a video call is first created or when an audio call transitions to a video call)		
video.autoStartVideoTx	**0 or 1**	**1**
When enabled, video transmission to the far side begins when you start a call. When disabled, video transmission does not begin until you press the **Video > Start Video** soft keys. This parameter controls video sent to the far side. Video from the far side always displays if available, and far side users can control when to send video.		
video.callMode.default	**audio or video**	**audio**
When the device uses SIP protocol, this parameter allows users to select the outbound call mode.		
video.callRate	**128 to 2048**	**512**
The default call rate (in kbps) to use when initially negotiating bandwidth for a video call.		
video.dynamicControlMethod	**0 or 1**	**0**
If 1, the first I-Frame request uses the method defined by `video.forceRtcpVideoCodecControl` and subsequent requests alternate between RTCP-FB and SIP INFO.		
video.enable	**0=Disable, 1=Enable**	**1**
If 0, video is not enabled and all calls—both sent and received—are audio-only. If 1, video is sent in outgoing calls and received in incoming calls if the other device supports video.		
video.forceRtcpVideoCodecControl[1]	**0 or 1**	**0**
If 1, the system is forced to send RTCP feedback messages to request fast update I-frames along with SIP INFO messages for all video calls irrespective of a successful SDP negotiation of a=rtcp-fb. If 0, RTCP-FB messages depend on a successful SDP negotiation of a=rtcp-fb and are not used if that negotiation is missing.		
video.iFrame.delay[1]	**0 to 10, seconds**	**0**

Video Parameters (continued)

When non-zero, an extra I-frame is transmitted after video starts. The amount of delay from the start of video until the I-frame is sent is configurable up to 10 seconds.		
video.iFrame.minPeriod	**1 - 60**	**2**
After sending an I-frame, the system always waits at least this amount of time before sending another I-frame in response to requests from the far end.		
video.iFrame.onPacketLoss	**0 or 1**	**0**
If 1, an I-frame is transmitted to the far end when a received RTCP report indicates that video RTP packet loss has occurred.		
video.maxCallRate[1]	**128 to 2048 kbps**	**768**
The maximum call rate allowed. This allows the administrator to limit the maximum call rate that the users can select. If `video.callRate` exceeds this value, this value is used as the maximum.		
video.quality[1]	**motion, sharpness**	**NULL**
The optimal quality for video that you send in a call or a conference. Use `motion` if your outgoing video has motion or movement. Use `sharpness` or Null if your outgoing video has little or no movement. Note: If `motion` is not selected, moderate to heavy motion can cause some frames to be dropped.		

[1] Change causes system to restart or reboot.

<camera/>

The settings in the next table control the performance of the camera.

Video Camera Parameters

Parameter	*Permitted Values*	*Default*
video.camera.brightness	**0 to 6**	**3**
Set brightness level. The value range is from 0 (Dimmest) to 6 (Brightest).		
video.camera.contrast	**0 to 4**	**0**
Set contrast level. The value range is from 0 (No contrast increase) to 3 (Most contrast increase), and 4 (Noise reduction contrast).		
video.camera.flickerAvoidance	**0 to 2**	**0**
Set flicker avoidance. If set to 0, flicker avoidance is automatic. If set to 1, 50hz AC power frequency flicker avoidance (Europe/Asia). If set to 2, 60hz AC power frequency flicker avoidance (North America).		
video.camera.frameRate	**5 to 30**	**25**
Set target frame rate (frames per second). Values indicate a fixed frame rate, from 5 (least smooth) to 30 (most smooth). Note: If `video.camera.frameRate` is set to a decimal number, the value 25 is used.		

Video Camera Parameters (continued)

Parameter	*Permitted Values*	*Default*
video.camera.saturation	**0 to 6**	**3**
Set saturation level. The value range is from 0 (Lowest) to 6 (Highest).		
video.camera.sharpness	**0 to 6**	**3**
Set sharpness level. The value range is from 0 (Lowest) to 6 (Highest).		

<codecs/>

The video codecs include:

- <profile/>

<profile/>

The next table lists settings for a group of low-level video codec parameters. For most use cases, the default values are appropriate. Polycom does not recommend changing the default values unless specifically advised to do so.

Video Profile Parameters

Parameter	*Permitted Values*	*Default*
video.profile.H261.annexD[1]	**0 or 1**	**1**
Enable or disable Annex D when negotiating video calls.		
video.profile.H261.CifMpi[1]	**1 to 32**	**1**
Specify the frame rate divider that the system uses when negotiating CIF resolution for a video call. You can enter a value between 0-4. To disable, enter ‘0’. The default frame rate divider is ‘1’.		
video.profile.H261.jitterBufferMax[1]	**(video.profile.H261.jitter BufferMin + 500ms) to 2500ms**	**2000ms**
The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size always causes lost packets. This parameter should be set to the smallest possible value that support the expected network jitter.		
video.profile.H261.jitterBufferMin[1]	**33ms to 1000ms**	**150ms**
The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out still continues. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter.		
video.profile.H261.jitterBufferShrink[1]	**33ms to 1000ms**	**70ms**
The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (33 ms) to minimize the delay on known good networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).		
video.profile.H261.payloadType[1]	**0 to 127**	**31**

Video Profile Parameters (continued)

Parameter	*Permitted Values*	*Default*
RTP payload format type for H261 MIME type.		
video.profile.H261.QcifMpi[1]	**1 to 32**	**1**
Specify the frame rate divider that the system uses when negotiating Quarter CIF resolution for a video call. You can enter a value between 0-4. To disable, enter ‘0’. The default frame rate divider is ‘1’.		
video.profile.H263.CifMpi[1]	**1 to 32**	**1**
Specify the frame rate divider that the system uses when negotiating CIF resolution for a video call. You can enter a value between 0-32. To disable, enter ‘0’. The default frame rate divider is ‘1’.		
video.profile.H263.jitterBufferMax[1]	**(video.profile.H263.jitter BufferMin + 500ms) to 2500ms**	**2000ms**
The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size always causes lost packets. This parameter should be set to the smallest possible value that supports the expected network jitter.		
video.profile.H263.jitterBufferMin[1]	**33ms to 1000ms**	**150ms**
The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out still continues. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter.		
video.profile.H263.jitterBufferShrink[1]	**33ms to 1000ms**	**70ms**
The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (33 ms) to minimize the delay on known good networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).		
video.profile.H263.payloadType[1]	**0 to 127**	**34**
RTP payload format type for H263 MIME type.		
video.profile.H263.QcifMpi[1]	**1 to 32**	**1**
Specify the frame rate divider that the system uses when negotiating Quarter CIF resolution for a video call. You can enter a value between 0-32. To disable, enter ‘0’. The default frame rate divider is ‘1’.		
video.profile.H263.SqcifMpi[1]	**1 to 32**	**1**
Specify the frame rate divider that the system uses when negotiating Sub Quarter CIF resolution for a video call. You can enter a value between 0-32. To disable, enter ‘0’. The default frame rate divider is ‘1’.		
video.profile.H2631998.annexF[1]	**0 or 1**	**0**
Enable or disable Annex F when negotiating video calls.		
video.profile.H2631998.annexI[1]	**0 or 1**	**0**
Enable or disable Annex I when negotiating video calls.		
video.profile.H2631998.annexJ[1]	**0 or 1**	**0**

Video Profile Parameters (continued)

Parameter	*Permitted Values*	*Default*
Enable or disable Annex J when negotiating video calls.		
video.profile.H2631998.annexK[1]	**0, 1, 2, 3, 4**	**1**
Specify the value of Annex K to use when negotiating video calls. You can enter a value between 0-4. To disable, enter ‘0’. The default value is ‘1’.		
video.profile.H2631998.annexN[1]	**0, 1, 2, 3, 4**	**1**
Specify the value of Annex N to use when negotiating video calls. You can enter a value between 0-4. To disable, enter ‘0’. The default value is ‘1’.		
video.profile.H2631998.annexT[1]	**0 or 1**	**0**
Enable or disable Annex T when negotiating video calls.		
video.profile.H2631998.CifMpi[1]	**1 to 32**	**1**
Specify the frame rate divider that the system uses when negotiating CIF resolution for a video call. You can enter a value between 0-32. To disable, enter ‘0’. The default frame rate divider is ‘1’.		
video.profile.H2631998.jitterBufferMax[1]	**(video.profile.H2631998.jitter BufferMin+ 500ms) to 2500ms**	**2000ms**
The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size always causes lost packets. This parameter should be set to the smallest possible value that supports the expected network jitter.		
video.profile.H2631998.jitterBufferMin[1]	**33ms to 1000ms**	**150ms**
The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out still continues. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter.		
video.profile.H2631998.jitterBufferShrink[1]	**33ms to 1000ms**	**70ms**
The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (33 ms) to minimize the delay on known good networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).		
video.profile.H2631998.payloadType[1]	**96 to 127**	**96**
RTP payload format type for H263-1998/90000 MIME type.		
video.profile.H2631998.QcifMpi[1]	**1 to 32**	**1**
Specify the frame rate divider that the system uses when negotiating Quarter CIF resolution for a video call. You can enter a value between 0-32. To disable, enter ‘0’. The default frame rate divider is ‘1’.		
video.profile.H2631998.SqcifMpi[1]	**1 to 32**	**1**
Specify the frame rate divider that the system uses when negotiating Sub Quarter CIF resolution for a video call. You can enter a value between 0-32. To disable, enter ‘0’. The default frame rate divider is ‘1’.		

Video Profile Parameters (continued)

Parameter	*Permitted Values*	*Default*
video.profile.H264.jitterBufferMax[1]	**(video.profile.H264.jitter BufferMin + 500ms) to 2500ms**	**2000ms**
The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size always causes lost packets. This parameter should be set to the smallest possible value that supports the expected network jitter.		
video.profile.H264.jitterBufferMin[1]	**33ms to 1000ms**	**150ms**
The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out still continues. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter.		
video.profile.H264.jitterBufferShrink[1]	**33ms to 1000ms**	**70ms**
The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (33 ms) to minimize the delay on known good networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).		
video.profile.H264.payloadType[1]	**96 to 127**	**109**
RTP payload format type for H264/90000 MIME type.		
video.profile.H264.profileLevel[1]	**1, 1b, 1.1, 1.2, 1.3, and 2**	**1.3**
Specify the highest profile level within the baseline profile supported in video calls. The system supports the following levels: 1, 1b, 1.1, 1.2, 1.3, and 2. The default level is 1.3.		

1 Change causes system to restart or reboot.

<webutility/>

The parameters listed in the next table specify the download location of the translated language files for the Web Configuration Utility.

Web Configuration Utility Parameters

Parameter	Permitted Values	Default
webutility.language.plcmServerUrl	**URL**	`http://downloads.polycom.com/voice/software/languages/`
The download location of the translated language files for the Web Configuration Utility.		