



**ADMINISTRATOR GUIDE**

Software 1.3.0 | September 2017 | 3725-84594-001D

# **Polycom® CX5500 Unified Conference Station for Skype™ for Business**



Copyright© 2017, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive  
San Jose, CA 95002  
USA

### **Trademarks**

Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.



All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

### **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](mailto: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](mailto: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

---

<b>About This Guide .....</b>	<b>11</b>
Who Should Read This Guide? .....	11
Conventions Used in This Guide .....	11
Recommended Software Tools .....	13
Read the Feature Parameter Tables .....	13
Example One: Feature Parameter Tables .....	14
Example Two: Configuring Grouped Parameters .....	14
Get Help and Support .....	16
<i>The Polycom Community</i> .....	16
<b>About the CX5500 Unified Conference Station for Microsoft Skype for Business.....</b>	<b>17</b>
<b>Polycom UC Software Overview.....</b>	<b>18</b>
What Is Polycom UC Software? .....	18
<i>Overview of Configuration Files</i> .....	18
<i>Overview of Resource Files</i> .....	19
<b>Set Up Your Device Network.....</b>	<b>20</b>
Establish Link Connectivity .....	21
Security and Quality of Service Settings.....	21
<i>VLANs and Wired Devices</i> .....	21
<i>802.1X Authentication</i> .....	21
IP Communication Settings.....	22
Provisioning Server Discovery .....	23
<i>Supported Provisioning Protocols</i> .....	24
System Network Menus .....	25
<i>Main Menu</i> .....	25
<i>Provisioning Server Menu</i> .....	27
<i>DHCP Menu</i> .....	29
<i>Ethernet Menu</i> .....	30
<i>VLAN Menu</i> .....	31
<i>802.1X Menu</i> .....	32
<i>PAC File Information</i> .....	33
<i>Login Credentials Menu</i> .....	33
<i>TLS Security Menu</i> .....	33
<i>TLS Profile Menu</i> .....	34
<i>Applications Menu</i> .....	35
<i>Syslog Menu</i> .....	35
<b>Configuration Methods.....</b>	<b>37</b>
Centralized Provisioning .....	37

<i>Master Configuration File</i> .....	38
<i>Variable Substitutions</i> .....	40
<i>Template Configuration Files</i> .....	41
<i>Changing Configuration Parameter Values</i> .....	43
Web Configuration Utility.....	44
<i>Import Configuration Files to the Phone</i> .....	44
<i>Export Configuration Files from the Phone</i> .....	45
<i>Choose Language Files for the Web Configuration Utility Interface</i> .....	45
System User Interface.....	47
<b>Set Up the Provisioning Server.....</b>	<b>48</b>
Why Use a Provisioning Server?.....	48
Provisioning Server Security Notes.....	48
Set up an FTP Server as Your Provisioning Server.....	49
Download Polycom CX5500 Software Files to the Update Server.....	50
Deploy and Update the CX5500 System with a Update Server.....	50
<i>Deploy CX5500 Systems with a Provisioning Server</i> .....	51
Using the RealPresence Resource Manager to provision CX5500 System.....	52
<i>Configure the RealPresence Resource Manager to Provision the CX5500 System</i> .....	53
Update CX5500 Software using a USB Flash Drive.....	55
<b>Set Up Basic System Features.....</b>	<b>56</b>
Configure Call Logs.....	57
<i>Example Call Log Configuration</i> .....	58
Understand the Call Timer.....	60
Configure Call Waiting Alerts.....	60
<i>Example Call Waiting Configuration</i> .....	61
Called Party Identification.....	61
Configure Calling Party Identification.....	61
<i>Example Calling Party Configuration</i> .....	62
Enable Missed Call Notification.....	62
<i>Example Missed Call Notification Configuration</i> .....	63
Connected Party Identification.....	63
Distinctive Incoming Call Treatment.....	64
<i>Example Call Treatment Configuration</i> .....	65
Apply Distinctive Ringing.....	66
<i>Example Distinctive Ringing Configuration</i> .....	67
Apply Distinctive Call Waiting.....	67
<i>Example Distinctive Call Waiting Configuration</i> .....	67
Configure Do Not Disturb.....	68
<i>Example Do Not Disturb Configuration</i> .....	70
Use the Local Contact Directory.....	70
<i>Example Configuration</i> .....	71
Configure the Local Digit Map.....	73
<i>Understand Digit Map Rules</i> .....	74
Microphone Mute.....	75

---

Configure the Speed Dial Feature .....	75
<i>Example Speed Dial Configuration</i> .....	75
Set the Time and Date Display .....	77
<i>Example Configuration</i> .....	78
Set a Graphic Display Background.....	79
<i>Example Graphic Display Background Configuration</i> .....	80
Set the Idle Screen Display .....	81
Enable Automatic Off-Hook Call Placement .....	81
<i>Example Automatic Off-Hook Placement Configuration</i> .....	82
Configure Call Hold.....	82
<i>Example Call Hold Configuration</i> .....	83
Use Call Transfer .....	84
<i>Example Call Transfer Configuration</i> .....	85
Create Local and Centralized Conferences.....	85
Enable Conference Management .....	86
<i>Example Conference Management Configuration</i> .....	86
Configure Call Forwarding .....	87
<i>Example Call Forwarding Configuration</i> .....	88
Configure Lync Call Forwarding .....	89
Configure Directed Call Pick-Up .....	90
<i>Example Directed Call Pickup Configuration</i> .....	90
Enable Group Call Pickup.....	90
Configure Call Park and Retrieve .....	91
<i>Example Call Park and Retrieve Configuration</i> .....	91
Enable Last Call Return .....	92
<i>Example Configuration for Last Call Return</i> .....	93
<b>Set Up Advanced System Features.....</b>	<b>95</b>
Assign Multiple Line Keys per Registration .....	96
<i>Example Configuration</i> .....	97
Enable Multiple Call Appearances.....	97
<i>Example Multiple Call Appearances Configuration</i> .....	98
Set the System Language.....	99
<i>Example System Language Configuration</i> .....	100
Synthesized Call Progress Tones.....	101
Configure Real-Time Transport Protocol Ports.....	101
<i>Example Real-Time Transport Protocol Configuration</i> .....	103
Configure Network Address Translation .....	103
<i>Example Network Address Translation Configuration</i> .....	104
Use the Corporate Directory .....	104
<i>Example Corporate Directory Configuration</i> .....	106
Configure Enhanced Feature Keys.....	107
<i>Some Guidelines for Configuring Enhanced Feature Keys</i> .....	108
<i>Enhanced Feature Key Examples</i> .....	109
<i>Understanding Macro Definitions</i> .....	111
<i>Macro Actions</i> .....	111

<i>Prompt Macro Substitution</i> .....	112
<i>Expanded Macros</i> .....	113
<i>Special Characters</i> .....	113
<i>Example Macro</i> .....	113
<i>Speed Dial Example</i> .....	114
Configure Soft Keys .....	115
<i>Example Soft Key Configurations</i> .....	116
Capture Wireshark Trace using Flash File to USB Flash Drive.....	118
Capture Wireshark Trace to USB Flash Drive through Telnet Command.....	118
Enable the Power Saving Feature .....	119
<i>Example Power-Saving Configuration</i> .....	120
Configure Group Paging .....	120
Configure Shared Call Appearances .....	122
<i>Example Configuration</i> .....	124
Enable Bridged Line Appearance .....	125
<i>Example Bridged Line Appearance Configuration</i> .....	126
Enable Voicemail Integration .....	127
<i>Example Voicemail Configuration</i> .....	128
Enable Multiple Registrations .....	129
<i>Example Multiple Registration Configuration</i> .....	130
Set Up Server Redundancy .....	131
DNS SIP Server Name Resolution .....	132
<i>Behavior When the Primary Server Connection Fails</i> .....	133
<i>Recommended Practices for Fallback Deployments</i> .....	134
Use the Presence Feature .....	135
<i>Example Presence Configuration</i> .....	136
Configuring the Static DNS Cache .....	137
<i>Example Static DNS Cache Configuration</i> .....	138
Displaying SIP Header Warnings .....	141
<i>Example Display of Warnings from SIP Headers Configuration</i> .....	142
Quick Setup of the CX5500 System .....	142
<i>Example Quick Setup Configuration</i> .....	143
Provisional Polling of the CX5500 System .....	144
<i>Example Provisional Polling Configuration</i> .....	145
Set Up Microsoft Lync Server 2010 and 2013.....	145
<i>Register with Microsoft Lync Server 2010</i> .....	146
<i>Example Configuration: Setting the Base Profile to Lync</i> .....	148
Enable Microsoft Exchange Calendar Integration .....	151
<i>Example Exchange Calendar Configuration</i> .....	152
Configure Mac OS Support.....	153
<b>Set Up System Audio Features.....</b>	<b>155</b>
Customize Audio Sound Effects .....	156
<i>Example Configuration</i> .....	157
Voice Activity Detection .....	157
Generate Dual Tone Multi-Frequency (DTMF) Tones.....	158

DTMF Event RTP Payload.....	158
Acoustic Echo Cancellation .....	158
Audio Codecs.....	159
IP Type-of-Service .....	161
IEEE 802.1p/Q .....	161
Voice Quality Monitoring (VQMon) .....	162
Built-In Audio Processing Features .....	163
<i>Automatic Gain Control</i> .....	163
<i>Background Noise Suppression</i> .....	163
<i>Comfort Noise Fill</i> .....	163
<i>Dynamic Noise Reduction</i> .....	163
<i>Jitter Buffer and Packet Error Concealment</i> .....	163
<i>Low-Delay Audio Packet Transmission</i> .....	163
<b>Set Up User and System Security Features .....</b>	<b>164</b>
Local User and Administrator Passwords.....	164
Incoming Signaling Validation.....	165
Configuration File Encryption.....	166
Digital Certificates.....	166
Generate a Certificate Signing Request .....	168
Configure TLS Profiles.....	169
<i>Download Certificates to a CX5500 System</i> .....	171
<i>Set TLS Profiles</i> .....	171
Support Mutual TLS Authentication .....	172
Configurable TLS Cipher Suites .....	173
Secure Real-Time Transport Protocol .....	174
Lock the System .....	176
Support 802.1X Authentication .....	177
Set User Profiles .....	179
<b>Use the CX5100/5500 Control Panel.....</b>	<b>183</b>
<i>Find Your Default System Password</i> .....	184
<i>Create or Load a System Profile</i> .....	184
<i>Update the CX5500 System's Software Automatically</i> .....	185
<b>Troubleshoot Your CX5500 System .....</b>	<b>187</b>
Understand Error Message Types.....	187
<i>Error Messages</i> .....	187
<i>Polycom UC Software Error Messages</i> .....	188
Status Menu.....	190
Log Files.....	190
<i>Logging Options</i> .....	191
<i>Reading a Boot Log File</i> .....	195
<i>Reading an Application Log File</i> .....	196
<i>Reading a Syslog File</i> .....	197
Manage the CX5500 System's Memory Resources.....	197

---

<i>Identify Symptoms</i> .....	198
<i>Check the System's Available Memory</i> .....	198
Test System Hardware .....	199
Upload a System's Configuration .....	199
Network Diagnostics .....	199
Restore the Default Settings.....	200
<i>Restore Default Settings using a USB Flash Drive</i> .....	200
<i>Restore to Default using the Local Interface</i> .....	201
Ports Used on the CX5500 System .....	201
Power and Startup Issues.....	202
Touch Screen Issues .....	203
Screen and System Access Issues .....	203
Calling Issues.....	204
Display Issues.....	205
Audio Issues .....	205
Licensed Feature Issues.....	205
Upgrading Issues .....	206
<b>Maintenance Tasks .....</b>	<b>207</b>
Trusted Certificate Authority List.....	207
Encrypt Configuration Files.....	210
Internal Key Functions .....	211
Assign a VLAN ID Using DHCP.....	214
Parse Vendor ID Information .....	215
Product, Model, and Part Number Mapping .....	216
Capture the System's Current Screen .....	216
LLDP and Supported TLVs.....	217
<i>Supported TLVs</i> .....	218
<b>Configuration Parameters.....</b>	<b>222</b>
<apps/> .....	222
<bg/> .....	224
<button/> .....	224
<call/>.....	225
<callLists/> .....	229
<device/> .....	229
<i>Type of Device Parameters</i> .....	230
<diags/> .....	241
<dialplan/> .....	242
<dir> .....	245
<broadsoft/> .....	246
<local/> .....	246
<corp/> .....	247
<divert/> .....	249
<dns/> .....	250



<i>DNS-A</i> .....	250
<i>DNS-NAPTR</i> .....	251
<i>DNS-SRV</i> .....	252
<efk/> .....	252
<exchange/> .....	254
<feature/>.....	255
<httpd/>.....	257
<keyboard/> .....	258
<lcl/>.....	258
<ml/> .....	259
<datetime/>.....	260
<loc/> .....	261
<lldp/> .....	262
<license/>.....	263
<log/> .....	263
<level/> <change/>and<render/>.....	265
<sched/>.....	266
<msg/> .....	267
<mwi/>.....	268
<nat/> .....	268
<systemLock/>.....	269
<powerSaving/> .....	269
<pres/> .....	271
<prov/> .....	271
<ptt/> .....	273
<qos/> .....	274
<reg/>.....	276
<request/>.....	284
<roaming_buddies/> .....	284
<roaming_privacy/> .....	285
<saf/> .....	285
<se/> .....	286
<pat/> .....	287
<rt/> .....	290
<sec/> .....	292
<encryption/>.....	292
<pwd/><length/>.....	293
<srtp/> .....	293
<dot1x><eapollogoff/> .....	296
<hostmovedetect/> .....	296
<TLS/>.....	296
<softkey/> .....	299
<tcpIpApp/>.....	301
<dhcp/>.....	302
<dns/>.....	302
<ice/>.....	303

---

<sntp/>.....	303
<port/><rtp/>.....	305
<keepalive/>.....	306
<fileTransfer/>.....	306
<tones/>.....	307
<DTMF/>.....	307
<chord/>.....	308
<up/>.....	309
<upgrade/>.....	312
<video/>.....	312
<camera/>.....	314
<codecs/>.....	314
<voice/>.....	318
<codecPref/>.....	318
<volume/>.....	320
<vad/>.....	320
<quality monitoring/>.....	321
<rxQoS/>.....	322
<volpProt/>.....	323
<server/>.....	324
<SDP/>.....	327
<SIP/>.....	327
<webutility/>.....	335
<xmpp/>.....	335
<b>Session Initiation Protocol (SIP) .....</b>	<b>337</b>
RFC and Internet Draft Support.....	337
Request Support.....	338
Header Support.....	339
Response Support.....	342
Hold Implementation.....	346
Reliability of Provisional Responses.....	346
Transfer.....	346
Third Party Call Control.....	346
SIP for Instant Messaging and Presence Leveraging Extensions.....	347
Shared Call Appearance Signaling.....	347
Bridged Line Appearance Signaling.....	347

# About This Guide

---

The *Polycom® CX5500 Unified Conference Station Administrator Guide* provides instructions for installing, provisioning, and administering the CX5500 Unified Conference Station. This guide will help you understand the Polycom VoIP network and telephony components of the CX5500 system, provides descriptions of all available system features, and helps you perform the following tasks:

- Install and configure your system on a network server or Web server
- Configure your system's features and functions
- Configure your system's user settings
- Troubleshoot common system issues



## Web Info: Using the Polycom CX5500 Unified Conference Station

For more information on how to use the features available on the CX5500 system, see the [Polycom CX5500 Unified Conference Station for Microsoft Lync User Guide](#).

## Who Should Read This Guide?

System administrators and network engineers should read this guide to learn how to properly set up the CX5500 system. This guide describes administration-level tasks and is not intended for end users.

Before reading this guide, you should be familiar with the following:






- Computer networking and driver administration for your operating system
- An XML editor
- The XML-based configuration file format used for the Polycom UC Software

## Conventions Used in This Guide

Polycom guides contain graphical elements and a few typographic conventions. Familiarizing yourself with these elements and conventions will help you successfully perform tasks.

### Icons Used in this Guide

<i>Name</i>	<i>Icon</i>	<i>Description</i>
<b>Note</b>		The Note icon highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.
<b>Important</b>		Important highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.

<i>Name</i>	<i>Icon</i>	<i>Description</i>
<b>Caution</b>		The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.
<b>Warning</b>		The Warning icon highlights an action you must perform (or avoid) to prevent issues that may cause you to lose information or your configuration setup, and/or affect system or network performance.
<b>Web Info</b>		The Web Info icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.
<b>Troubleshooting</b>		The Troubleshooting icon highlights information that may help you solve a relevant problem or to refer you to other relevant troubleshooting resources.
<b>Settings</b>		The Settings icon highlights settings you may need to choose for a specific behavior, to enable a specific feature, or to access customization options.

A few typographic conventions, listed next, are used in this guide to distinguish types of in-text information.

### Typographic Conventions

<i>Convention</i>	<i>Description</i>
<b>Bold</b>	Highlights interface items such as menu selections, soft keys, file names, and directories. Also used to represent menu selections and text entry.
<i>Italics</i>	Used to emphasize text, to show example values or inputs, and to show titles of reference documents available from the <a href="#">Polycom Support</a> web site and other reference sites.
<a href="#">Blue Text</a>	Used for cross references to other sections within this document and for hyperlinks to external documents and web sites.
<code>Courier</code>	Used for code fragments and parameter names.

This guide also uses a few writing conventions to distinguish conditional information.

### Writing Conventions

<i>Convention</i>	<i>Description</i>
<MACaddress>	Indicates that you must enter information specific to your installation, system, or network. For example, when you see <MACaddress>, enter your device's 12-digit MAC address. If you see <installed-directory>, enter the path to your installation directory.

<i>Convention</i>	<i>Description</i>
>	Indicates that you need to select an item from a menu. For example, <b>Settings &gt; Basic</b> indicates that you need to select <b>Basic</b> from the <b>Settings</b> menu.
parameter.*	Used for configuration parameters. If you see a parameter name in the form <code>parameter.*</code> , the text is referring to all parameters beginning with <code>parameter.</code> . See <a href="#">Read the Feature Parameter Tables</a> for an example.

## Recommended Software Tools

Polycom recommends that you use an XML editor—such as XML Notepad—to create and edit configuration files to ensure that any configuration files you create are valid XML files. If the configuration files are not valid XML, they will not load onto the system, and an error message is logged to the provisioning server.

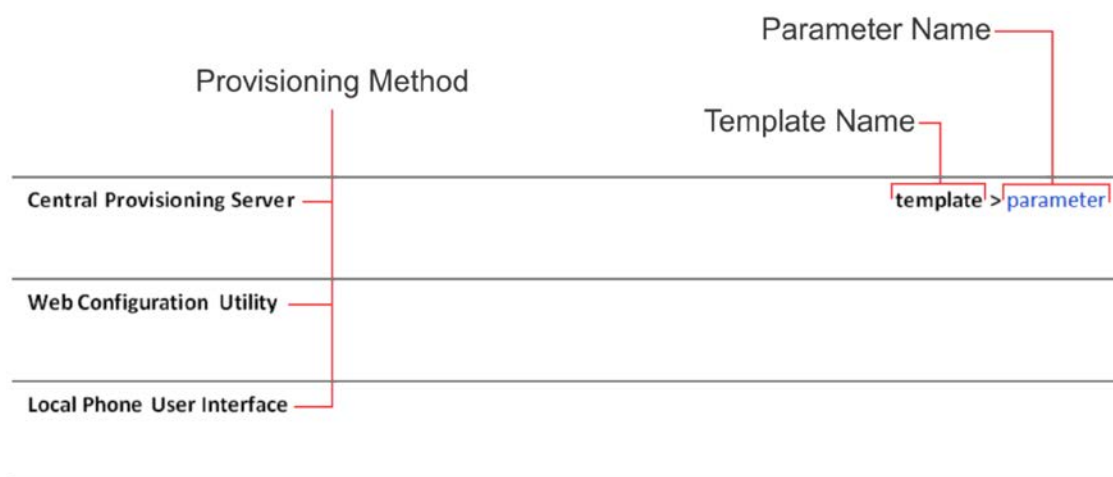
## Read the Feature Parameter Tables

Each of the feature descriptions discussed in this administrator guide includes a table of parameters that you can configure to enable or customize features. The feature parameter tables indicate one or more of the three provisioning methods you can use to configure a feature: a centralized provisioning server, the Web Configuration Utility, or the local system user interface. The types of provisioning methods available for each feature vary, and not every feature uses all three methods.

Some feature parameters are located in more than one template file, and in these cases, the parameter tables list all related template files.

The central provisioning server method requires you to configure parameters located in template configuration files that Polycom provides in XML format. The following illustration shows the template name and the name of the parameter you configure in the configuration file.

### Feature Parameter Table Format



## Example One: Feature Parameter Tables

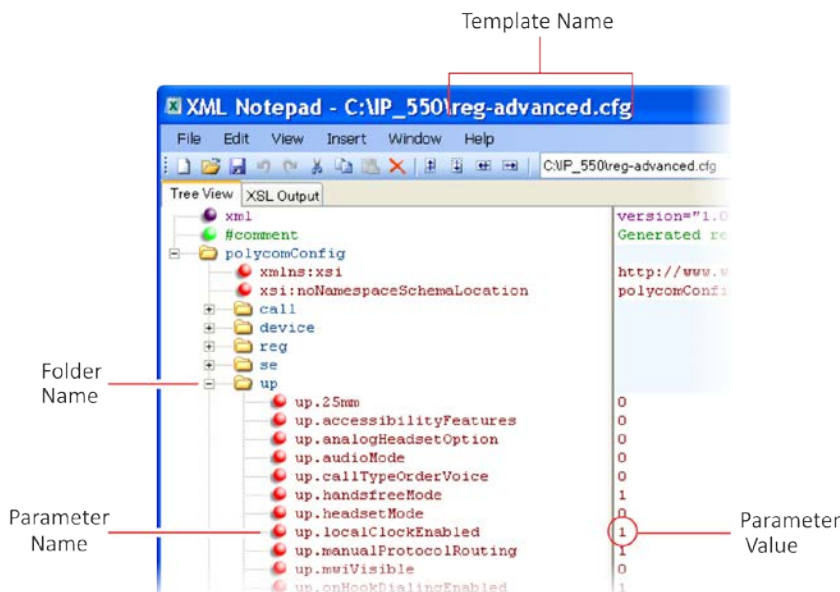
The example shown next is taken from the section [Set the Time and Date Display](#) in the [Configuration Methods](#) section.

### Feature Parameter Table for Time and Date Display

<b>Central Provisioning Server</b>	<b>template &gt; parameter</b>
Turn the time and date display on or off..... <b>reg-advanced.cfg &gt; up.localClockEnabled</b>	

This example indicates that the **reg-advanced.cfg** template file contains the `up.localClockEnabled` parameter, which turns the time and date display on or off. This parameter is enabled by default. If you want to turn the time and date display on or off, locate and open the **reg.advanced** template, expand the **up** folder, and locate the parameter name `up.localClockEnabled`. Set the parameter value to 1 to turn on or 0 to turn off the time and date display, as shown in the following illustration.

### Example Time and Date Display



## Example Two: Configuring Grouped Parameters

Some of the features have several related parameters that you must configure, and in these cases, the table will specify a group of related parameters, instead of listing every parameter, with an abbreviated XML path name ending with `(.*)`, which indicates you can configure a group of related parameters.

The next example shows that in the **site.cfg** template, the `tcpIpApp.sntp` folder contains several related parameters that configure basic SNTP settings.

**Feature Parameter Table for Time and Date SNTP Settings**

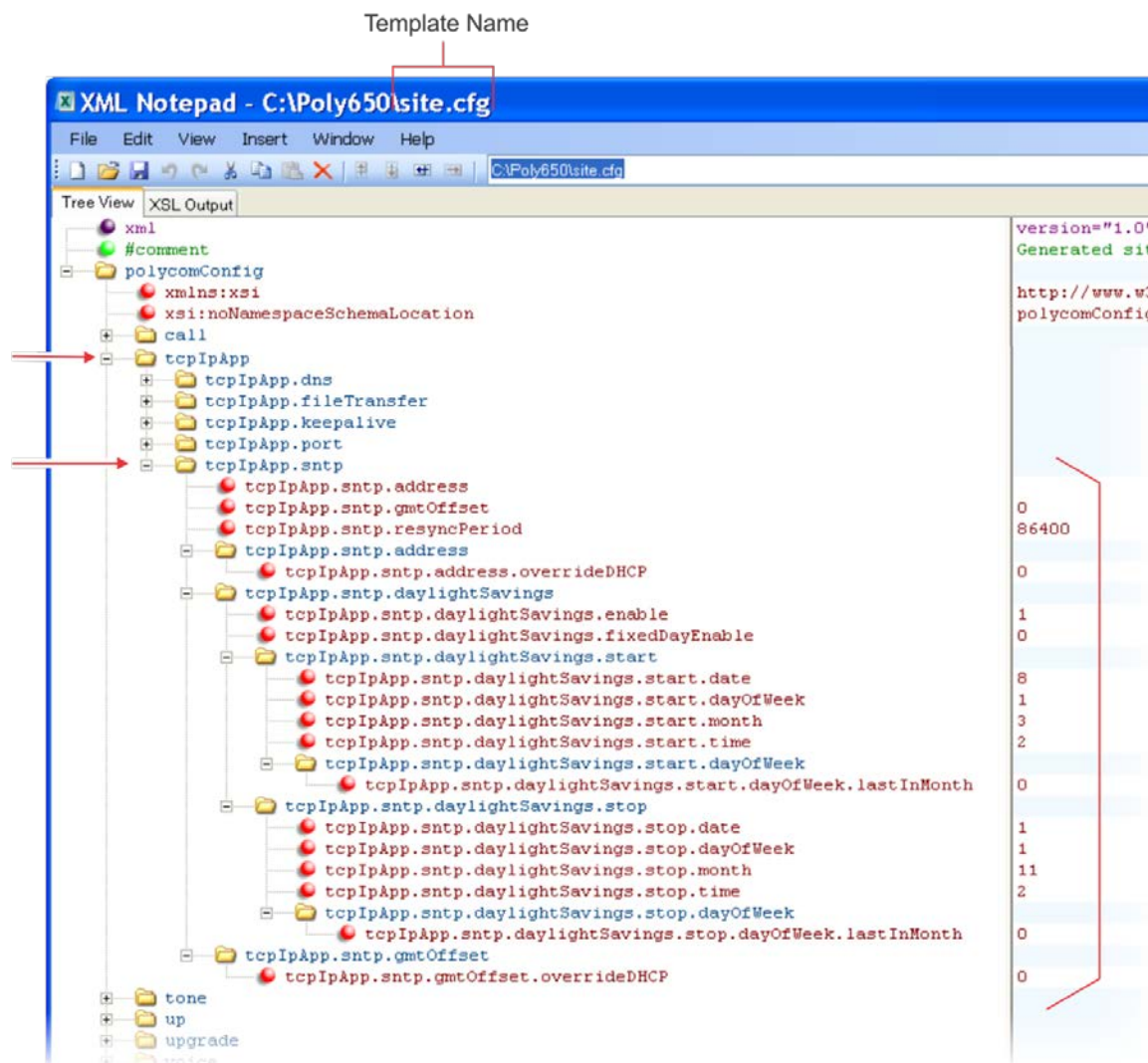
Central Provisioning Server

template > parameter

Set the basic SNTP settings and daylight savings parameters..... site.cfg > tcpIpApp.sntp.\*

This example indicates that there is a group of SNTP parameters you can configure in the **site.cfg** template file. The abbreviated parameter name `tcpIpApp.sntp.*` indicates that you can configure parameters in the `tcpIpApp.sntp` folder as well as parameters in `tcpIpApp.sntp` subfolders.

**Locating Parameters in the Templates**



In cases where the feature has several related parameters, refer to the parameter reference section in the section [Polycom UC Software Menu System](#) for a definition of each parameter. This section has shown you how to read the configuration parameter tables so that you can locate the parameters in the XML template file.

---

## Get Help and Support

If you are looking for help or technical support for your systems, the following types of documents are available at the [Polycom Support](#):

You can find Request for Comments (RFC) documents by entering the RFC number at <http://www.ietf.org/rfc.html>.

### ***The Polycom Community***

The [Polycom Community](#) gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.



# About the CX5500 Unified Conference Station for Microsoft Skype for Business

---

The CX5500 unified conference station provides integrated cameras, a speaker, and microphones on one device. Users can use the Polycom CX5500 Unified Conference Station to make the following types of calls:

- Audio-only conference calls with Open SIP voice platforms or in a Lync Server or Skype for Business Server environment.
- Audio and video calls made using Microsoft® Lync® or Skype™ for Business. When your CX5500 system is connected to a computer running Lync client, the system provides a 360-degree view of the conference room and automatically identifies the active speaker.

Note that this administrator guide focuses on configuring the telephony features available on the CX5500 system when used as an audio-only conference system. For information on configuring settings available on the CX5500 system when connected to a computer and used as an audio and video conference system, see the section [Use the CX5100/5500 Control Panel](#).

# Polycom UC Software Overview

---

The Polycom CX5500 Unified Conference Station supports most of the features of the Polycom UC Software 5.5.1 release. UC software supports the deployment of Polycom systems as a Session Initiation Protocol (SIP)-based endpoint interoperating with a SIP call server or softswitch.

For Polycom systems to successfully operate as a SIP endpoint in your network, you need the following:

- A working IP network
- Routers configured for VoIP
- VoIP gateways configured for SIP
- The latest or a compatible version of Polycom UC Software
- An active, configured call server to receive and send SIP messages

You can find additional information about the UC Software 5.5.1 release at the [Polycom United Communications Resource Center](#).

## What Is Polycom UC Software?

The Polycom Unified Communications (UC) Software manages the protocol stack, the digital signal processor (DSP), the user interface, and the network interaction. UC Software implements the following functions and features on the systems:

- VoIP signaling for a wide range of voice and video telephony functions using SIP signaling for call setup and control
- SIP signaling
- Industry standard security techniques for ensuring that all provisioning, signaling, and media transactions are robustly authenticated and encrypted
- Advanced audio signal processing for speaker system communications using a wide range of audio codecs
- Flexible provisioning methods to support single system, small business, and large multi-site enterprise deployments

UC software is a binary file and contains a digital signature that prevents tampering or the loading of rogue software images.

## Overview of Configuration Files

Polycom UC Software package contains template configuration files, which are valid XML files that you can edit. These template files contain a number of parameters that provision the system's features and settings. The template configuration files are flexible, and enable you to rearrange the parameters within the template, move parameters to new files, or create your own configuration files from only those parameters you want. This flexibility is useful when you want to apply the same features and settings to a large number of systems.

Configuration files enable you to store a single set of configuration files on a central provisioning server and configure all of your systems to read the same set of files.

---

## ***Overview of Resource Files***

In addition to the software and configuration files, the Polycom UC Software package contains resource files, which include some additional features you can use to configure your systems.

Examples of resource files include:

- Language dictionaries
- Custom fonts
- Ringtones
- Contact directories

# Set Up Your Device Network

---

The Polycom CX5500 system operates on an Ethernet local area network (LAN) connection. After the system is connected to the LAN, a startup sequence is initiated. The system uses the following startup sequence:

- 1 The system establishes network connectivity.  
Wired systems will establish a 10M/100M/1000M network link with an Ethernet switch device. Telephony will not function until this link is established. If the system cannot establish a link to the LAN, an error message *Network link is down* will display.
- 2 Apply appropriate security and Quality of Service (QoS) settings (optional).  
Assign the system to a VLAN and/or 802.1X authentication.
- 3 Establish DHCP negotiation with the network and IP address, network addressing options, network gateway address, and time server.
- 4 Provision server discovery.  
To facilitate boot time, contacting the provisioning server is delayed until the system is operational. You can also disable contacting the provisioning server, for example, to reduce the server load after a power failure.

Only step 1 in the sequence is required and automatic, except for systems on a WLAN. The following steps are optional as all these settings can be manually configured on the device.

These steps are described in more detail in the following sections:

- [Establish Link Connectivity](#)
- [Security and Quality of Service Settings](#)
- [IP Communication Settings](#)
- [Provisioning Server Discovery](#)
- [System Network Menus](#)

## Digest Authentication for Microsoft Internet Information Services

If you want to use digest authentication against the Microsoft Internet Information Services server, consider using Microsoft Internet Information Server 6.0 or later. Digest authentication needs the username and password to be saved in reversible encryption. The user account on the server must have administrative privileges.

The wildcard must be set as MIME type; otherwise, the system will not download \*.cfg, \*.ld and other required files. This is because the Microsoft Internet Information Server cannot recognize these extensions and will return a "File not found" error. To configure wildcard for MIME type, see IIS 6.0 does not serve unknown MIME types.

For more information, see [Digest Authentication in IIS 6.0 on Microsoft TechNet](#).

## Establish Link Connectivity

Typical network equipment supports one of the following Ethernet line rates: 10Mbps, 100Mbps, and 1000Mbps. The systems are configured to automatically negotiate the Ethernet rate so that no special configuration is required. You do have the option to change the line rates and/or duplex configuration. Polycom recommends that you keep the default settings. If you want to change the system's configuration, do so prior to connecting the devices.

## Security and Quality of Service Settings

You have the option of using several layer-2 mechanisms to increase network security and minimize audio latency. This section describes each of the network security options.

### *VLANs and Wired Devices*

You can use a Virtual LAN (VLAN) to separate and assign higher priority to a voice VLAN as a way of minimizing latency. There are several methods in which you can configure the system to work on a particular VLAN:

- **LLDP** 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. To change these parameters, go to VLAN Menu.
- **CDP Compatible** Cisco Discovery Protocol (CDP) is a proprietary Data Link Layer network protocol. CDP Compatible follows the same set of rules. To change this parameter, go to VLAN Menu.
- **DHCP** Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. To change this parameter, go to DHCP Menu.

To use DHCP for assigning VLANs, see [Assign a VLAN ID Using DHCP](#). Using DHCP for assigning VLANs is not well standardized and is recommended only if the switch equipment does not support LLDP or CDP Compatible methods.

- **Static** The VLAN ID can be manually set from the system UI or from a configuration file. To change this parameter, go to VLAN Menu. This will set the device setting parameter only.

If the system receives a VLAN setting from several of the above methods, the priority is as follows (from highest to lowest):

- LLDP
- CDP
- Device settings
- DHCP VLAN discovery

### **802.1X Authentication**

802.1X authentication is a technology that originated for authenticating Wi-Fi links. It has also been adopted for authenticating computers within fixed LAN deployments. When VoIP systems (with a secondary Ethernet port) are used to connect computers on a network, the 802.1X authentication process becomes more complex since the computer is not directly connected to the 802.1X switch.



### Web Info: 802.1X References

For more information on 802.1X authentication, see Introduction to IEEE 802.1X and Cisco® Identity-Based Networking Services (IBNS) at [Cisco 802.1X](#).

See also [IEEE 802.1X Multi-Domain Authentication on Cisco Catalyst Layer 3 Fixed Configuration Switches Configuration Example](#).

There are several ways to configure 802.1X authentication of devices connected to the PC port of the system:

- You can configure many switches to automatically trust or accept a VoIP system based on its MAC address, which is sometimes referred to as MAC Address Bypass (MAB).
- Some switches support a feature whereby they automatically trust a device that requests a VLAN using the CDP protocol.
- Some deployments support Multiple Device Authentication (MDA) where both the system and the computer authenticate themselves separately.

In this scenario, where the system is closest to the 802.1X switch, the system needs to notify the switch when the computer is disconnected. This can be achieved using an 802.1X EAPOL-Logoff message.

To change these parameters, see the section [802.1X Menu](#).

## IP Communication Settings

When the system has established network connectivity, it needs to acquire several IP network settings to proceed with provisioning. These settings are typically obtained automatically from a DHCP server. You have the option to set the IP communication settings manually from the system UI, or to pre-provision using a `device.set` capability.

When making the DHCP request, the system includes information in Option 60 that can assist the DHCP server in delivering the appropriate settings to the device. Polycom recommends using DHCP where possible to eliminate repetitive manual data entry. For more information, see [Technical Bulletin 54041: Using DHCP Vendor Identifying Options with Polycom Systems](#).

The following table details the settings that are supported through the DHCP menu.

### DHCP Network Parameters

Parameter	DHCP Option	DHCP	DHCP INFORM	Configuration File (application only)	Device Settings
IP address	-	•	-	-	•
Subnet mask	1	•	-	-	•
IP gateway	3	•	-	-	•
Boot server address	See <a href="#">DHCP Menu</a> or <a href="#">Provisioning Server Discovery</a> .	•	•	-	•

Parameter	DHCP Option	DHCP	DHCP INFORM	Configuration File (application only)	Device Settings
SIP server address	151 Note: You can change this value by changing the device setting. See <a href="#">&lt;device/&gt;</a> .	•	-	-	•
SNTP server address	Look at option 42, then option 4.	•	-	•	•
SNTP GMT offset	2	•	-	•	•
DNS server IP address	6	•	-	-	•
DNS INFORM server IP address	6	•	-	-	•
DNS domain	15	•	-	-	•
VLAN ID	See <a href="#">DHCP Menu</a> .				

**Warning:** Link Layer Discovery Protocol (LLDP) overrides Cisco Discovery Protocol (CDP). CDP overrides Local Flash which overrides DHCP VLAN Discovery.



#### Web Info: RFC Information on DHCP Options

For more information on DHCP options, see [RFC 2131](#) and [RFC 2132](#).



#### Note: Overriding the DHCP Value

The configuration file value for **SNTP server address** and **SNTP GMT offset** can be configured to override the DHCP value: see [tcplpApp.snntp.address.overrideDHCP](#).  
The CDP Compatibility value can be obtained from a connected Ethernet switch if the switch supports CDP.

If you do not have control of your DHCP server or do not have the ability to set the DHCP options, enable the system to automatically discover the provisioning server address. One way is to connect to a secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server value. For more information, see [RFC 3361](#) and [RFC 3925](#).

## Provisioning Server Discovery

In many deployments, a centralized provisioning server is used for the software update and configuration functions. The system supports several methods to discover the provisioning server:

- **Static** You can manually configure the server address from the system's user interface or the Web Configuration Utility, or you can pre-provision the system. The server address is manually configured from the system's user interface, the Web Configuration Utility, or pre-provisioned using `device.set` in a configuration file.
- **DHCP** A DHCP option is used to provide the address or URL between the provisioning server and the system.
- **DHCP INFORM** The system makes an explicit request for a DHCP option, which can be answered by a server that is not the primary DHCP server.
- **Quick Setup** This feature offers a soft key to the user that takes them directly to a screen to enter the provisioning server address and information. This is simpler than navigating the menus to the relevant places to configure the provisioning parameters. For more information, see the section [Quick Setup of the CX5500 System](#).

To change these parameters, go to [Provisioning Server Menu](#).



#### Web Info: Provisioning Polycom Systems

For more information on best practices with respect to provisioning, see [White Paper 60806: UC Software Provisioning Best Practices](#).

## Supported Provisioning Protocols

By default, systems are shipped with FTP enabled as the provisioning protocol. UC Software is only compatible with passive FTP.

You can change the provisioning protocol by updating the *Server Type* option, or you can specify a transfer protocol in the *Server Address*. For example, `http://usr:pwd@server` (see [Provisioning Server Menu](#)). The *Server Address* can be an IP address, domain string name, or URL, and it can be obtained through DHCP.

Configuration file names in the `<MACaddress>.cfg` file can include a transfer protocol, for example, `https://usr:pwd@server/dir/file.cfg`. If a username and password are specified as part of the server address or file name, they are used only if the server supports them. If a username and password are required but not specified, the device settings are sent to the server.



#### Tip: Choosing a Valid URL

A URL should contain forward slashes instead of back slashes and should not contain spaces. Escape characters are not supported. If a user name and password are not specified, the Server User and Server Password from device settings will be used (see [Provisioning Server Menu](#)).



#### Note: HTTP/HTTPS Authentication

Both digest and basic authentication are supported when using HTTP/HTTPS for UC Software. Only digest authentication is supported when using HTTP by the Updater.



# System Network Menus

You have the option of modifying the system network configuration.

You can update the network configuration parameters after your system starts and is running CX5500 Software. The network configuration menu is accessible from the system's main menu. Select **Settings > Advanced > Admin Settings > Network Configuration**. To access the Advanced menu, you will have to enter the administrator's password (see [Local User and Administrator Passwords](#)).

You have the option to modify the system network configuration parameters in the following menus and sub-menus:

- [Main Menu](#)
- [Provisioning Server Menu](#)
- [DHCP Menu](#)
- [Ethernet Menu](#)
- [VLAN Menu](#)
- [802.1X Menu](#)
- [PAC File Information](#)
- [Login Credentials Menu](#)
- [TLS Security](#)
- [TLS Profile Menu](#)
- [Applications Menu](#)
- [Syslog Menu](#)

Note that certain parameters are read-only due to the value of other parameters. For example, if the DHCP client parameter is enabled, the System IP Address and Subnet Mask parameters are read-only since the DHCP server automatically supplies these parameters and the statically assigned IP address and subnet mask will never be used in this configuration.



#### Tip: Resetting Network Configurations

The basic network configuration referred to in the subsequent sections can be reset to factory default settings using the system's main menu: Select **Settings > Advanced > Admin Settings > Reset to Defaults > Reset Device Settings**.

## Main Menu

You can modify the configuration parameters shown in the following table from the setup menu while the system boots, or from the Advanced Settings menu.

**Main Menu**

<i>Name</i>	<i>Possible Values</i>
<b>Provisioning Menu</b>	
See <a href="#">Provisioning Server Menu</a> .	
<b>Network Interfaces Menu or Ethernet Menu</b>	
See <a href="#">Ethernet Menu</a> .	
<b>TLS Security Menu</b>	
See <a href="#">TLS Security Menu</a> .	
<b>SNTP Address</b>	<b>Dotted-decimal IP address OR Domain name string</b>
The Simple Network Time Protocol (SNTP) server the system obtains the current time from.	
<b>GMT Offset</b>	<b>-13 through +12</b>
The offset of the local time zone from Greenwich Mean Time (GMT) in half hour increments.	
<b>DNS Server</b>	<b>Dotted-decimal IP address</b>
The primary server the system directs Domain Name System (DNS) queries to.	
<b>DNS AltServer</b>	<b>Dotted-decimal IP address</b>
The secondary server to which the system directs DNS queries.	
<b>DNS Domain</b>	<b>Domain name string</b>
The system's DNS domain.	
<b>Hostname</b>	<b>hostname</b>
The DHCP client hostname.	
<b>Syslog Menu</b>	
See <a href="#">Syslog Menu</a> .	
<b>Quick Setup</b>	<b>Enabled, Disabled</b>
If enabled, a QSetup soft key displays on the idle screen when you are in Lines View. When you tap this soft key, a menu displays enabling you to configure the parameters required to access the provisioning server.	
<b>Note:</b> The Quick Setup option is not available in the Updater.	
<b>Reset to Defaults</b>	
There are five ways to reset or clear system features and settings, including settings from web or local override files.	
<b>Base Profile</b>	<b>Generic, Lync</b>
Use this to enable Lync-compatible systems to register with Lync Server. When set to Lync, the system automatically provisions with the minimum parameters required to register with Lync Server. You cannot modify or customize the Base Profile. By default, the Base Profile is set to Generic.	



### Settings: Preventing Invalid Parameter Values

If you insert incorrect parameter values into the configuration file, the system ignores the invalid values and uses the previous configuration. Before you complete your configuration, make sure you set values for these parameters.

## Provisioning Server Menu

You can set the configuration parameters shown in the following table in the Provisioning Server Menu.

### Provisioning Server Menu

Name	Possible Values
<b>DHCP Menu</b>	
See <a href="#">DHCP Menu</a> . <b>Note:</b> This menu is disabled when the DHCP client is disabled.	
<b>Server Type</b>	<b>0=FTP, 1=TFTP, 2=HTTP, 3=HTTPS, 4=FTPS</b>
The protocol that the system uses to obtain configuration and system application files from the provisioning server. See <a href="#">Supported Provisioning Protocols</a> .	
<b>Note:</b> Active FTP is not supported for BootROM version 3.0 or later. Passive FTP is supported. Only implicit FTPS is supported.	
<b>Server Address</b>	<b>Dotted-decimal IP address OR URL</b>
Domain name string or a URL. All addresses can be followed by an optional directory. The address can also be followed by the file name of a <b>.cfg</b> master configuration file, which the system will use instead of the default <b>&lt;MACaddress&gt;.cfg</b> file. The provisioning server to use if the DHCP client is disabled, if the DHCP server does not send a boot server option, or if the <b>Boot Server</b> parameter is set to <b>Static</b> .	
The system can contact multiple IP addresses per DNS name. These redundant provisioning servers must all use the same protocol. If a URL is used, it can include a user name and password. See <a href="#">Supported Provisioning Protocols</a> . For information on how to specify a directory and use the master configuration file, see <a href="#">Master Configuration File</a> .	
<b>Note:</b> ":", "@", or "/" can be used in the user name or password if they are correctly escaped using the method specified in <a href="#">RFC 1738</a> .	
<b>Server User</b>	<b>String</b>
The user name requested when the system logs into the server (if required) for the selected <b>Server Type</b> .	
<b>Note:</b> If the Server Address is a URL with a username, this will be ignored.	
<b>Server Password</b>	<b>String</b>
The password requested when the system logs in to the server if required for the selected <b>Server Type</b> .	
<b>Note:</b> If the Server Address is a URL with username and password, this will be ignored.	
<b>File Transmit Tries</b>	<b>1 to 10 Default 3</b>
The maximum number of attempts to transfer a file. (An attempt is defined as trying to download the file from all IP addresses that map to a particular domain name.)	

<i>Name</i>	<i>Possible Values</i>
<b>Retry Wait</b>	<b>0 to 300 seconds Default 1</b>
<p>The minimum amount of time that must elapse before retrying a file transfer. The time is measured from the start of a transfer attempt, which is defined as the set of upload/download transactions made with the IP addresses that map to a given provisioning server's DNS. If the set of transactions in an attempt is equal to or greater than the Retry Wait value, then there will be no further delay before the next attempt is started.</p> <p>For more information, see <a href="#">Deploy and Update the CX5500 System with a Provisioning Server</a>.</p>	
<b>Tag SN to UA</b>	<b>Disabled, Enabled</b>
<p>If enabled, the system's serial number is included in the User-Agent header of HTTP/HTTPS transfers and communications to the browser.</p> <p>The default value is Disabled.</p>	
<b>Upgrade Server</b>	<b>String</b>
<p>The address/URL that will be accessed for software updates requested from the systems Web configuration utility.</p>	
<b>ZTP</b>	<b>Disabled, Enabled</b>
<p>See <a href="#">Zero-Touch Provisioning Solution</a> on <a href="#">Polycom Voice Support</a>.</p>	



**Tip: Changing the Default Passwords**

Change Server User and Server Password parameters from the default values.

## DHCP Menu

The DHCP menu is accessible only when the DHCP client is enabled. You can update DHCP configuration parameters shown in the following table.

### DHCP Menu

Name	Possible Values
<b>Boot Server</b>	<b>0=Option 66, 1=Custom, 2=Static, 3=Custom+Option 66</b>
<p><b>Option 66</b> The system will look 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 <i>Server Address</i> in <a href="#">Provisioning Server Menu</a>.</p> <p><b>Custom</b> The system will look for the option number specified by the <i>Boot Server Option</i> parameter (below), and the type specified by the <i>Boot Server Option Type</i> parameter (below) in the response received from the DHCP server.</p> <p><b>Static</b> The system will use the boot server configured through the <i>Server Menu</i>. For more information, see <a href="#">Provisioning Server Menu</a>.</p> <p><b>Custom + Option 66</b> The system will use the custom option first or use Option 66 if the custom option is not present.</p> <p>Note: If the DHCP server sends nothing, the following scenarios are possible:</p> <ul style="list-style-type: none"> <li>• If a boot server value is stored in flash memory and the value is not 0.0.0.0, then the value stored in flash is used.</li> <li>• Otherwise the system sends out a DHCP INFORM query. <ul style="list-style-type: none"> <li>➢ If a single DHCP INFORM server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid boot server value.</li> <li>➢ If no DHCP INFORM server responds, the INFORM query process will retry and eventually time out.</li> </ul> </li> <li>• If the server address is not discovered using DHCP INFORM then the system will contact the ZTP server if the ZTP feature is enabled.</li> </ul>	
<b>Boot Server Option</b>	<b>128 through 254 (Cannot be the same as VLAN ID Option)</b>
<p>When the <i>Boot Server</i> parameter is set to Custom, this parameter specifies the DHCP option number in which the system will look for its boot server.</p>	
<b>Boot Server Option Type</b>	<b>0=IP Address, 1=String</b>
<p>When the <i>Boot Server</i> parameter is set to Custom, this parameter specifies the type of DHCP option in which the system will look for its provisioning server. The IP Address provided must specify the format of the provisioning server. The String provided must match one of the formats described for <i>Server Address</i> in <a href="#">Provisioning Server Menu</a>.</p>	
<b>Option 60 Format</b>	<b>0=RFC 3925 Binary, 1=ASCII String</b>
<p>RFC 3925 Binary: Vendor-identifying information in the format defined in <a href="#">RFC 3925</a>.</p> <p>ASCII String: Vendor-identifying information in ASCII.</p> <p>For more information, see <a href="#">Technical Bulletin 54041: Using DHCP Vendor Identifying Options With Polycom Systems</a>.</p> <p><i>Note:</i> DHCP option 125 containing the RFC 3295 formatted data will be sent whenever option 60 is sent. DHCP option 43 data is ignored.</p>	

**Note: Multiple DHCP INFORM Servers**

If multiple DHCP INFORM servers respond, the system should gather the responses from these DHCP INFORM servers. If configured for Custom+Option66, the system will select the first response that contains a valid *custom* option value. If none of the responses contain a *custom* option value, the system will select the first response that contains a valid *option66* value.

## Ethernet Menu

The Ethernet menu displays only if there are multiple network interfaces to the system. You can configure network options shown in the following table.

### Ethernet Menu

<i>Name</i>	<i>Possible Values</i>
<b>DHCP</b>	<b>Enabled, Disabled</b>
If enabled, DHCP will be used to obtain the parameters discussed in <a href="#">IP Communication Settings</a> .	
<b>IP Address</b>	<b>Dotted-decimal IP address</b>
The system's IP address. <b>Note:</b> This parameter is disabled when DHCP is enabled.	
<b>Subnet Mask</b>	<b>Dotted-decimal subnet mask</b>
The system's subnet mask. <b>Note:</b> This parameter is disabled when DHCP is enabled.	
<b>IP Gateway</b>	<b>Dotted-decimal IP address</b>
The system's default router.	
<b>VLAN</b>	
See <a href="#">VLAN Menu</a> .	
<b>802.1X Authentication</b>	<b>Enabled, Disabled</b>
If enabled, the system will use the 802.1 Authentication parameters to satisfy the negotiation requirements for each EAP type.	
<b>802.1X Menu</b>	
See <a href="#">802.1X Menu</a> .	
<b>LAN Port Mode</b>	<b>0 = Auto, 1 = 10HD, 2 = 10FD, 3 = 100HD, 4 = 100FD, 5 = 1000FD</b>
The network speed over Ethernet. The default value is Auto. HD means half duplex and FD means full duplex. <b>Note:</b> Polycom recommends that you do not change this setting.	

<i>Name</i>	<i>Possible Values</i>
<b>PC Port Mode</b>	<b>0 = Auto, 1 = 10HD, 2 = 10FD, 3 = 100HD, 4 = 100FD, 5 = 1000FD, -1 = Disabled</b>
<p>The network speed over Ethernet. The default value is Auto. HD means half duplex and FD means full duplex.                      Note: Polycom recommends that you do not change this setting unless you want to disable the PC port.</p>	
<b>1000BT LAN Clock</b>	<b>0=Auto 1=Slave 2=Master</b>
<p>The mode of the LAN clock.                      The default value is Slave (this device receives its clock timing from a master device).  <b>Note:</b> Polycom recommends that you do not change this setting unless you have Ethernet connectivity issues. This setting was chosen to give the best results from an EMI perspective.</p>	
<b>1000BT PC Clock</b>	<b>0=Auto 1=Slave 2=Master</b>
<p>The mode of the PC clock. The default value is Auto.  <b>Note:</b> Polycom recommends that you do not change this setting unless you have Ethernet connectivity issues. This setting was chosen to give the best results from an EMI perspective.</p>	

## VLAN Menu

You can modify the parameters shown in the following table.

### VLAN Menu

<i>Name</i>	<i>Possible Values</i>
<b>VLAN ID</b>	<b>Null, 0 through 4094</b>
<p>The system's 802.1Q VLAN identifier. The default value is Null.  <b>Note:</b> Null = no VLAN tagging</p>	
<b>LLDP</b>	<b>Enabled, Disabled</b>
<p>If enabled, the system will use the LLDP protocol to communicate with the network switch for certain network parameters. Most often this will be used to set the VLAN that the system should use for voice traffic. It also reports power management to the switch. The default value is Enabled.                      For more information on how to set VLAN and LLDP, see <a href="#">LLDP and Supported TLVs</a>.</p>	
<b>CDP Compatibility</b>	<b>Enabled, Disabled</b>
<p>If enabled, the system will use CDP-compatible signaling to communicate with the network switch for certain network parameters. Most often this will be used to set the VLAN that the system should use for Voice Traffic, and for the system to communicate its PoE power requirements to the switch. The default value is Enabled.</p>	
<b>VLAN Discovery</b>	<b>0=Disabled, 1=Fixed (default), 2=Custom</b>
<p>For a detailed description, see <a href="#">Assign a VLAN ID Using DHCP</a>.  <b>Disabled:</b> No VLAN discovery through DHCP.  <b>Fixed:</b> Use predefined DHCP vendor-specific option values of 128, 144, 157 and 191. If one of these is used, VLAN ID Option will be ignored  <b>Custom:</b> Use the number specified for VLAN ID Option as the DHCP private option value.</p>	

<i>Name</i>	<i>Possible Values</i>
<b>VLAN ID Option</b>	<b>128 through 254 (Cannot be the same as Boot Server Option) (default is 129)</b>

The DHCP private option (when VLAN Discovery is set to Custom).  
For more information, see [Assign a VLAN ID Using DHCP](#).

## 802.1X Menu

The 802.1X Menu displays when 802.1X authentication is enabled. You can modify configuration parameters shown in the following table.

### 802.1X Menu

<i>Name</i>	<i>Possible Values</i>
<b>EAP Method</b>	<b>0 = None, 1=EAP-TLS, 2=EAP-PEAPv0/MSCHAPv2, 3=EAP-PEAPv0/GTC, 4=EAP-TTLS/EAP-MSCHAPv2, 5=EAP-TTLS/EAP-GTC, 6=EAP-FAST, 7=EAP-MD5</b>
The selected EAP type to be used for authentication. For more information, see <a href="#">Support 802.1X Authentication</a> .	
<b>Identity</b>	<b>UTF-8 encoded string</b>
The identity (or user name) required for 802.1X authentication.	
<b>Password</b>	<b>UTF-8 encoded string</b>
The password required for 802.1X authentication. The minimum length is 6 characters.	
<b>Anonymous ID</b>	<b>UTF-8 encoded string</b>
The anonymous user name for constructing a secure tunnel for tunneled authentication and FAST authentication.	
<b>PAC File Info</b>	
See <a href="#">PAC File Information</a> .	
<b>EAP-FAST Inband Provisioning</b>	<b>Enabled, Disabled</b>
A flag to determine whether EAP-FAST Inband Provisioning is enabled. This parameter is used only if EAP Method is EAP-FAST.	



## ***PAC File Information***

You can modify Protected Access Credential (PAC) File Information shown in the following table.

### **PAC File Information Menu**

<i>Name</i>	<i>Possible Values</i>	<i>Description</i>
<b>PAC File Password</b>	<b>UTF-8 encoded string</b>	<b>The password required to decrypt the PAC file.</b>
PAC File Name	UTF-8 encoded string	The path or URL of the PAC file for download.
<b>Remove PAC File</b>	<b>UTF-8 encoded string</b>	<b>A flag to determine whether or not to delete the PAC file from the system.</b>

## ***Login Credentials Menu***

You can modify the parameters shown in the following table.

### **Login Credentials Menu**

<i>Name</i>	<i>Possible Values</i>
<b>Domain</b>	<b>UTF-8 encoded string</b>
The domain name used by a server.	
<b>User</b>	<b>UTF-8 encoded string</b>
The user name used to authenticate to a server.	
<b>Password</b>	<b>UTF-8 encoded string</b>
The password used to authenticate to a server.	

## ***TLS Security Menu***

This section refers to the TLS Security menu available in the software. You can modify the parameters shown in the following table.

### **TLS Security Menu**

<i>Name</i>	<i>Possible Values</i>
<b>OCSP</b>	<b>Enabled, Disabled</b>
The Online Certificate Status Protocol checks the revocation status of X.509 digital certificates downloaded during negotiation of a TLS connection.	

<i>Name</i>	<i>Possible Values</i>
<b>FIPS</b>	<b>Enabled, Disabled</b>
The Federal Information Processing Standard enables the validation and usage of FIPS-140 certified encryption algorithms.	
<b>Install Custom CA Cert</b>	<b>URL</b>
A CA certificate that is installed on the system to be used for TLS authentication.	
<b>Install Custom Device Cert</b>	<b>URL</b>
A device certificate installed on the system to be used for Mutual TLS authentication.	
<b>Clear Certificate</b>	<b>Yes, No</b>
A flag to determine whether or not the device certificate can be removed from the system.	
<b>TLS Profile x</b>	
There are currently two TLS Platform profiles. See <a href="#">TLS Profile Menu</a> .	
<b>Applications</b>	
See <a href="#">Applications Menu</a> .	

## ***TLS Profile Menu***

You can modify the parameters shown in following table.

### **TLS Profile Menu**

<i>Name</i>	<i>Possible Values</i>
<b>SSL Cipher Suite</b>	<b>String</b>
The global cipher suite.	
<b>Custom SSL Cipher Suite</b>	<b>String</b>
A custom cipher suite.	
<b>CA Cert List</b>	<b>String</b>
The CA certificate sources that are valid for this profile.	
<b>Device Cert List</b>	<b>String</b>
The device certificate sources that are valid for this profile.	

## Applications Menu

You can modify the parameters shown in the following table.

### Applications Menu

<i>Name</i>	<i>Possible Values</i>
<b>802.1X</b>	<b>1 or 2</b>
The TLS Profile to use for 802.1X authentication.	
<b>Provisioning</b>	<b>1 or 2</b>
The TLS Profile to use for provisioning authentication.	
<b>Provisioning</b>	<b>Enable or Disable</b>
The TLS Profile to enable or disable common name validation.	
<b>Syslog</b>	<b>1 or 2</b>
The TLS Profile to use for syslog authentication.	

## Syslog Menu

The syslog protocol is a simple protocol: the syslog sender sends a small textual message (less than 1024 bytes) to the syslog receiver. The receiver is commonly called *syslogd*, *syslog daemon*, or *syslog server*. Syslog messages can be sent through UDP, TCP, or TLS. The data is sent in clear text.

Because syslog is supported by a wide variety of devices and receivers, syslog can be used to integrate log data from many different types of systems into a central repository. For more information on the syslog protocol, see [RFC 3164](#).

You can modify the parameters shown in the following table.

### Syslog Menu

<i>Name</i>	<i>Possible Values</i>
<b>Server Address</b>	<b>Dotted-decimal IP address OR Domain name string</b>
The syslog server IP address. The default value is Null.	
<b>Server Type</b>	<b>None=0, UDP=1, TCP=2, TLS=3</b>
The protocol that the system will use to write to the syslog server. If set to None (or 0), transmission is turned off, but the server address is preserved.	
<b>Facility</b>	<b>0 to 23</b>
A description of what generated the log message. For more information, see section 4.1.1 of RFC 3164. The default value is 16, which maps to local 0.	

---

<i>Name</i>	<i>Possible Values</i>
<b>Render Level</b>	<b>0 to 6</b>
Specifies the lowest class of event that will be rendered to syslog. It is based on <code>log.render.level</code> and can be a lower value. See <a href="#">&lt;log/&gt;</a> .	
Note: Use left and right arrow keys to change values.	
<b>Prepend MAC Address</b>	<b>Enabled, Disabled</b>
If enabled, the system's MAC address is prepended to the log message sent to the syslog server.	

---

# Configuration Methods

---

This section explains configuration methods you can use to configure settings and features on the systems:

- Local system user interface (*for a single system*)
- Web Configuration Utility (*for a single system*)
- Centralized provisioning method (*for multiple systems*)

The methods explained in this section configure many of the system features and settings detailed in this administrator guide. However, not all of the features and settings are available using each configuration method. You can use a single method or you can use a combination of methods depending on your preferences and your corporate security.

Polycom recommends using the centralized provisioning method to provision and configure settings for multiple systems. Typically, settings you make using configuration files apply to multiple systems. Settings made using the Web Configuration Utility and the system's user interface are applied on a per-system basis and are available to individual system users.

This section explains each of the following configuration methods:

- [Centralized Provisioning](#)
- [Web Configuration Utility](#)
- [System User Interface](#)

## Centralized Provisioning

Polycom provides template configuration files in XML format that you can use to create a set of system features and settings specific to your organization. The UC Software configuration files you use to configure the systems are very flexible. These files dictate the behavior of the system after it is running the Polycom UC Software.

The configuration files have default values set, and the system uses the default values for a configuration parameter as long as the parameter has not been configured from any other source. Parameters can be changed using the local system user interface, the Web configuration utility, and configuration files hosted on a central provisioning server.

Applying configuration files to systems from a central provisioning server enables you to apply a single set of parameters and settings to all of the systems in your deployment. The configuration files maximize flexibility in installing the UC Software, configuring the systems, and in upgrading and maintaining the system settings over time.

The CX5500 system can boot up without any configuration files; however, certain parameters need to be changed for your system to be usable within your organization. If a system cannot locate a provisioning server upon boot up, the system operates with internally stored default settings. To send and receive calls, you must specify a SIP server address and a registration address in the configuration files.

You can create user-specific configuration files that enable system users to use features and settings from any system including those outside of your organization. To create a user-specific file, create a **<user>.cfg** file on the provisioning server for the user. For more information, see [Set User Profiles](#).

## Master Configuration File

The centralized provisioning method requires you to use a master configuration file. You can use the default master configuration file included in the software package or you can create and rename a master configuration file to apply to systems in a network in one of the following ways:

- **Default master configuration file** For deployments in which the configuration is identical for all systems, you can use the default master configuration file, which is **000000000000.cfg** in the UC Software package, to configure all the systems in a deployment. 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. If you do create and use a per-system master configuration file, make a copy of the default file and rename it.
- **Group and per-system master configuration file** If you want to apply features or settings to a group of systems within your deployment or to a single system, make a copy of the default file and rename it. For a system group, rename the file in a way that specifies the group-specific features or settings. For single systems, rename the file based on the system's MAC address **<MACaddress>.cfg**. Note that you can use only lower-case digits in the title of a master configuration file; for example, **0004f200106c.cfg**.

You can find the MAC address of the system on a label on the back of the power data box or on the device's menu system at **Settings > Status > Platform > System > S/N:**

- **Specified master configuration file** You can specify a master configuration file in the provisioning server address; for example, *http://usr:pwd@server/dir/example1.cfg*. The filename must end with .cfg and be at least five characters long. If this file cannot be downloaded, the system will search for a per-system master configuration file, described next.

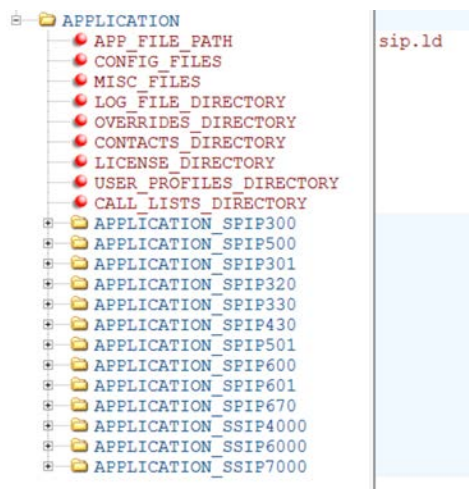


### Settings: Pay Attention to Per-System File Names

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

The following figure shows default available fields in the master configuration file.

### Default Fields in the Master Configuration File



The following describes each of the master configuration file XML attributes and the APPLICATION directories.

- **APP\_FILE\_PATH** Not applicable for CX5500 systems.
- **CONFIG\_FILES** Enter the names of your configuration files here as a comma-separated list. Each file name has a maximum length of 255 characters and the entire list of file names has a maximum length of 2047 characters, including commas and white space. 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`.
- **MISC\_FILES** A comma-separated list of files. You can use this to list volatile files that you want systems to download, for example, fonts, background images, or ringtone .wav files. The system downloads files you list here when booted, which can decrease access time.
- **LOG\_FILE\_DIRECTORY** An alternative directory to use for log files if required. A URL can also be specified. This is blank by default.
- **CONTACTS\_DIRECTORY** An alternative directory to use for user directory files if required. A URL can also be specified. This is blank by default.
- **OVERRIDES\_DIRECTORY** An alternative directory to use for configuration overrides files if required. A URL can also be specified. This is blank by default.
- **LICENSE\_DIRECTORY** An alternative directory to use for license files if required. A URL can also be specified. This is blank by default.
- **USER\_PROFILES\_DIRECTORY** An alternative directory for the `<user>.cfg` files.
- **CALL\_LISTS\_DIRECTORY** An alternative directory to use for user call lists if required. A URL can also be specified. This is blank by default.
- **COREFILE\_DIRECTORY** An alternative location for systems that can upload a core file containing debugging with diagnostic when they fail. This is blank by default.

The directories labeled **APPLICATION\_SPIPXXX** indicate system models that are not compatible with the latest UC Software version. If you are using any of the system models listed in these directories, open

the directory for the system model you are deploying, and use the available fields to provision and configure those systems.

## Variable Substitutions

The master configuration template file, included in the UC Software files you download from the Polycom Voice Support Web site, is particularly important to the central provisioning method, which Polycom recommends using for large-scale deployments. There are two methods you can use to provision or configure systems with the master configuration file. The method you use depends on your deployment scenario. Understanding both methods enables you to deploy and manage your systems efficiently. For a detailed explanation of the two methods and their advantages, see [Best Practices 35361: Provisioning with the Master Configuration File](#).

You can also use variable substitution if you need to use different application loads on different systems on the same provisioning server by creating a variable in the master configuration file that is replaced by the MAC address of each system when it reboots. You can use any of the following substitution strings:

- SYSTEM\_MODEL
- SYSTEM\_PART\_NUMBER
- SYSTEM\_MAC\_ADDRESS

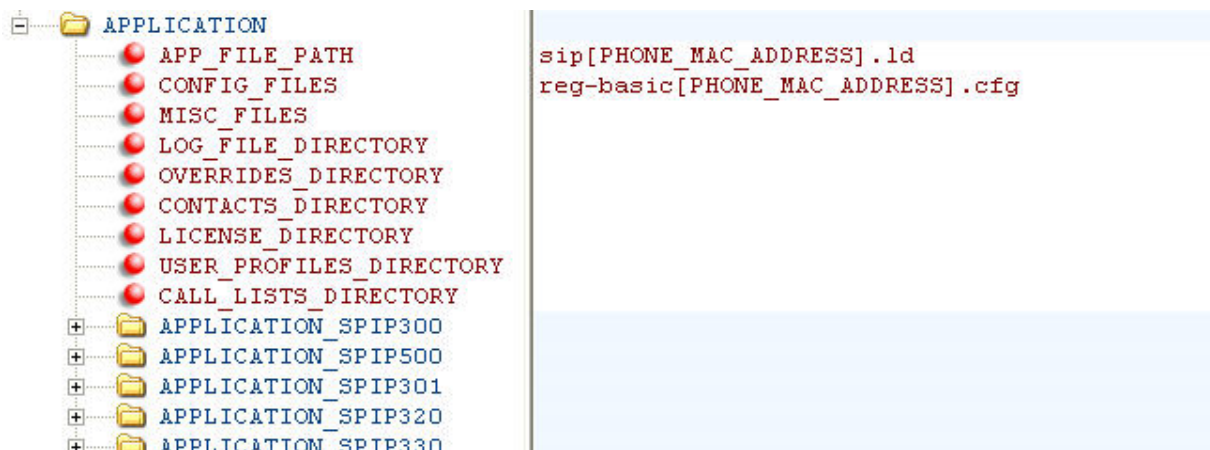
To find out the model number or part number of a product, see the section [Product, Model, and Part Number Mapping](#).

The following two examples illustrate the use of a variable substitution.

### Example One

You can create a variable in the master configuration file that is replaced by the MAC address of each system when it reboots as shown in the figure [MAC Address Variable](#).

#### MAC Address Variable





## Example Two

You can direct system update to a UC software build and configuration files based on the system model number and part number as shown in the following figure. All XML attributes can be modified in this manner.

### Provisioning with Model and Part Numbers

## Template Configuration Files

You will find a number of template configuration files when you expand the Polycom CX5500 software download. Most configuration parameters are located in only one template file; however, some do appear in two or more files. If you are using a parameter that is duplicated in another file, be aware that configuration files are read from left to right and the system uses the file it reads first.



### Troubleshooting: Locating Duplicate Parameters

To check whether a parameter is located in more than one template file, locate the parameter in the reference section [Configuration Parameters](#).

The following table outlines each template file included with the CX5500 software.

### Configuration File Templates

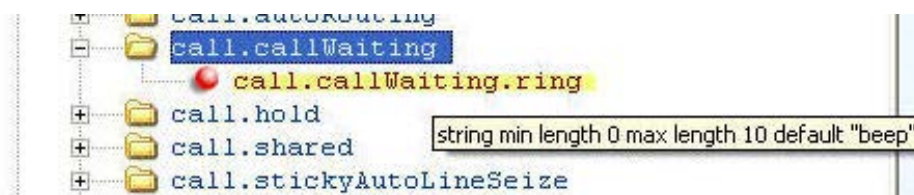
Name	Description	Deployment Scenarios
applications.cfg	For applications, browser, microbrowser, XMP-API	Typical Hosted Service Provider Typical IP-PBX
features.cfg	Features related enabling corp directory USB recording, CMA, presence, ACD, for example	Typical Hosted Service Provider Typical IP-PBX

Name	Description	Deployment Scenarios
reg-advanced.cfg	Advanced call server, multi-line systems	Typical Hosted Service Provider Typical IP-PBX
reg-basic.cfg	Basic registration	Simple SIP device Typical Hosted Service Provider
region.cfg	Non-North American geographies	Typical Hosted Service Provider Typical IP-PBX
sip-basic.cfg	Basic call server	Simple SIP device Typical Hosted Service Provider
sip-interop.cfg	Advanced call server, multi-line systems	Typical Hosted Service Provider Typical IP-PBX
site.cfg	Multi-site operations	Typical Hosted Service Provider Typical IP-PBX
techsupport.cfg	Available by special request from Polycom Customer Support.	Troubleshooting

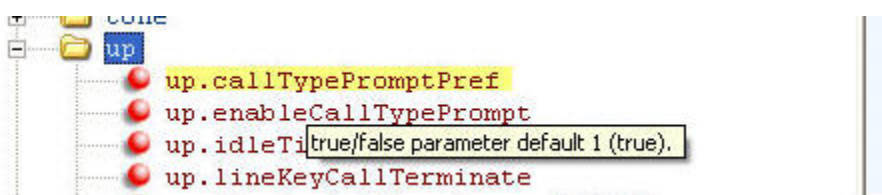
Along with the templates, the CX5500 software download includes an XML schema file—`polycomConfig.xsd`—that provides information like parameters type (boolean, integer, string, and enumerated type), permitted values, default values, and all valid enumerated type values. View this template file with an XML editor.

A string parameter, boolean, and enumerated parameters are shown in the following figures.

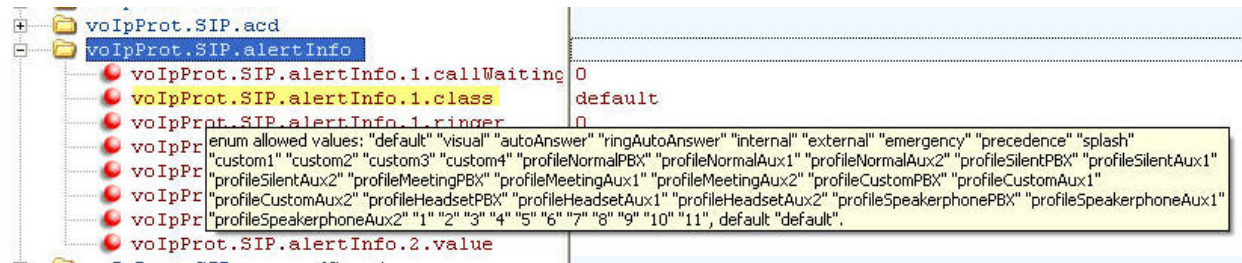
**String Parameter**



**Boolean Parameter**



## Enumerated Parameter



## Changing Configuration Parameter Values

The configuration parameters available in the UC Software use a variety of values, including Boolean, integer, enumerated types, and arrays (a table of values). Each parameter available in the UC Software is listed in alphabetical order in Configuration Parameters, along with a description, the default value, and the permissible values.

Note that the values for boolean configuration parameters are not case sensitive. The values 0, false, and off are inter-changeable and supported. The values 1, true, and on are interchangeable and supported. This Administrator's Guide documents only 0 and 1.

The following rules apply when you set a parameter with a numeric value outside of its valid range:

- If the configuration file's value is greater than the allowable range, the maximum value is used.
- If the configuration file's value is less than the allowable range, the minimum value is used.
- If a parameter's value is invalid, the value is ignored. Invalid parameters values can occur when enumerated type parameters do not match a pre-defined value, when numeric parameters are set to a non-numeric values, when string parameters are either too long or short, or when using null strings in numeric fields. All such situations are logged in the system's log files.



### Tip: Using Blank Values and Special Characters in the Configuration Files

The UC Software interprets Null as empty; that is, `attributeName=""`.

To enter special characters in a configuration file, enter the appropriate sequence using an XML editor:

- & as `&amp;`;
- " as `&quot;`;
- ' as `&apos;`;
- < as `&lt;`;
- > as `&gt;`;
- random numbers as `&0x12;`

## Customizing Parameters for a System Model

You can customize a set of parameter values for the CX5500 system by appending the SYSTEM MODEL NUMBER descriptor to the parameter. For a list of all system model names that you can use to create system-specific configurations, see [Product, Model, and Part Number Mapping](#).

For example, you can add CX5500 to end of the `dir.local.contacts.maxNum` to customize the parameter for the CX5500 system as so: `dir.local.contacts.maxNum.CX5500`. The maximum number of contacts for the local Contact Directory on the CX5500 system is 500.

Some configuration parameters cause the system to reboot or restart when change its value. To find out if a parameter reboots or restarts a system when changed, locate the parameter in Configuration Parameters. Parameters that reboot or restart the system are marked with a superscript (<sup>1</sup> or <sup>2</sup>).



### Caution: Deprecated Configuration Parameters

Polycom may deprecate configuration parameters that some organizations may still be using—deprecated parameters will not work. To check whether or not you are using deprecated configuration parameters, see the latest Polycom UC Software Release Notes on [Latest Polycom UC Software Release](#) or check the Release Notes for earlier software versions on [Polycom UC Software Support Center](#).

## 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: Using Web Configuration Utility

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.

## ***Choose Language Files for the Web Configuration Utility Interface***

You can choose a language for viewing the Web Configuration Utility interface. Polycom provides a number of XML language files that you can download from the Polycom CX5500 software package to your provisioning server. By default, the system displays the Web Configuration Utility in English. If you want the system to display the Web Utility interface in a language other than English, copy the corresponding XML language file from the languages folder to your provisioning server. This section shows you how to copy the Web Configuration Utility language files to your provisioning server so that system users can use the Web Configuration Utility interface in the language of their choice.

Certain languages available on the CX5500 system use an expanded character set and more memory than other language files. On average, the XML language files for the Web Configuration Utility interface are about 250KB in size. To conserve memory resources, Polycom recommends using only those XML language files for the languages you need. If you want to make multiple languages available to your users, you may need to manage the system's memory resources. For tips on how to do this, see [Manage the System's Memory Resources](#).

## To save XML language files to your provisioning server:

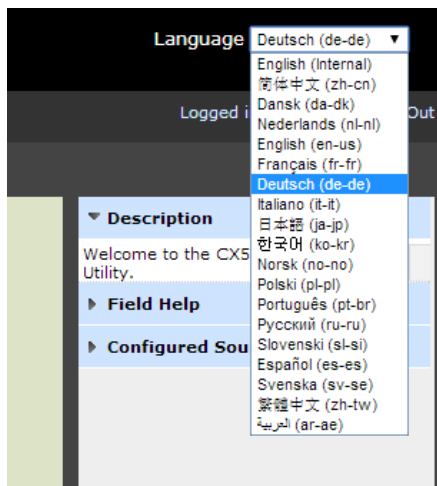
- 1 Create a new folder named *languages* on your provisioning server. This is the folder the provisioning server reads to apply language files to the interface of the Web Configuration Utility. For help setting up your provisioning server, see [Set Up the Provisioning Server](#).
- 2 Download and unzip the UC software package. You can find all of the language files for the Web Configuration Utility interface in a folder named *languages*.



### Note: Don't Confuse Language Files

The *languages* folder located in both the combined and split UC Software versions is not to be confused with the *language files* for the system interface, which are located in the SoundPointIPLocalization folder. To save memory on the system, Polycom recommends that you save only the Web Configuration Utility language files that you need to the *languages* folder you created in your provisioning server.

- 3 Copy the XML language file from the *languages* folder you downloaded from the software files to the *languages* folder you created on your provisioning server. For example, if you want the Web Configuration Utility to support French and German, copy `Website_dictionary_language_fr-fr.xml` and `Website_dictionary_language_de-de.xml` to the *languages* folder you created on your provisioning server.
- 4 Log in to the Web Configuration Utility and select a language from the **Languages** drop-down menu at the top-right of the screen, as shown next.



The interface of the Web Configuration Utility displays in the language you select. If the language does not display, ensure that you have extracted and saved the correct language file, or try rebooting the system.



### Troubleshooting: Managing the System's Memory Resources

If your selected language will not display, even after you have placed it on the provisioning server and you have rebooted the system, your system may have reached its available memory limit. If this occurs, you may need to take steps to manage your system's available memory resources. For tips on how to manage the system's memory, refer to [Manage the System's Memory Resources](#).

## System User Interface

The system menu system makes some settings available to users and further settings available to administrators.

To access administrator settings, such as provisioning values, enter an administrative password in the **Settings** menu on the LCD panel. Note that you can use an administrator password where a user password is required, but a user cannot access administrator settings with a user password. The default user password is **123** and the default administrative password is **456**. To secure the administrative settings from the system's user interface, change the default administrative password. See [Local User and Administrator Passwords](#).



### Timesaver: System User Interface Menu System

For a map diagram of all menu settings available from the system user interface, see [Polycom UC Software Menu System](#).



# Set Up the Provisioning Server

---

This section focuses on one particular way that the Polycom® CX5500 Software and the required external systems might initially be installed and configured in your network.

This section consists of the following sections:

- [Why Use a Provisioning Server?](#)
- [Provisioning Server Security Notes](#)
- [Set up an FTP Server as Your Provisioning Server](#)
- [Download Polycom CX5500 Software Files to the Update Server](#)
- [Deploy and Update the CX5500 System with a Provisioning Server](#)
- [Using RealPresence Resource Manager to Provision CX5500](#)
- [Upgrade Polycom UC Software](#)

## Why Use a Provisioning Server?

Polycom strongly recommends that you use a provisioning server to install and maintain your Polycom systems. You can set up a provisioning server on the local LAN or anywhere on the Internet. 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. The system is designed such that if it cannot locate a provisioning server when it boots up, it will operate with internally saved parameters. This is useful when the provisioning server is not available.

You can configure multiple, redundant provisioning servers 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. For more information on the protocol used, see [Supported Provisioning Protocols](#).

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 use the parameters described in the section [Provisioning Server Menu](#) to configure the number of times each server will be 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.

## Provisioning Server Security Notes

For organizational purposes, Polycom recommends configuring a separate log file directory, an override directory, a contact directory, and a license directory, though this is not required. You should ensure that the file permissions you create provide the minimum required access and that the account has no other rights on the server.

The system's server account needs to be able to add files that it can write to in the log file directory and the provisioning directory. It must also be able to list files in all directories mentioned in the



<**MACaddress**>.cfg file. 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.

The system will attempt to upload log files, a configuration override file, and a directory file to the server if changed. This requires that the system's account has delete, write, and read permissions. The system will still function without these permissions, but will not be able to upload files.

Polycom recommends that you allow file uploads to the provisioning server where the security environment permits. File uploads allow event log files to be uploaded. Log files provide backup copies of changes users make to the directory, and to the system's configuration through the Web server and/or local user interface. These log files help Polycom provide customer support when diagnosing issues that may occur with the system operation.

If you know the system is going to download a file from the server, you should mark the file as read-only.

## Set up an FTP Server as Your Provisioning Server

A simple provisioning configuration uses File Transfer Protocol or FTP. By default, Polycom sets FTP as the provisioning protocol on all Polycom systems. This guide focuses on the FTP provisioning protocol. Other supported protocols include: TFTP, HTTP, and HTTPS.

A free and popular server, [FileZilla Server](#), is available for Windows. FileZilla Server (version 0.9.xx) has been tested with the CX5500 Software.

### To set up an FTP server using FileZilla Server:

- 1 Download and install the latest version of [FileZilla Server](#).
- 2 After installation, a *Connect to Server* pop-up displays on your computer. Click **OK** to open the administrative user interface.
- 3 To configure a user, select **Edit > Users** in the status bar.
- 4 Click **Add**.
- 5 Enter the user name for the system and select **OK**.  
For example, *bill123*.
- 6 Select the **Password** checkbox and enter a password.  
For example, *1234*. The system will use this password to log in.
- 7 Select **Page > Shared folders** to specify the server-side directory where the provisioning files will be located (and the log files uploaded).
- 8 Select **Add** and pick the directory.
- 9 To allow the system to upload logs onto the provisioning server, select **Shared Folders > Files**, then select **Write** and **Delete** checkboxes, and then click **OK**.
- 10 Determine the IP address of the FTP server by entering **cmd** in the **Run** dialog on your **Start** menu, and enter **ipconfig** in the command prompt.  
The IP Address of the FTP server is shown.

## Download Polycom CX5500 Software Files to the Update Server

The software package for the CX5500 system is provided in a .tar file that you can download from the CX5500 system on the [CX5500 Support](#) page and place on the update server.

To enable the CX5500 system to check for updates when new software is placed on the update server, use the parameter `device.local.updateServer` to set the location of the update server. See [Device Parameters](#) for information on setting this parameter.

### To download the software package for the CX5500 system:

- 1 On the [CX5500 Support](#) page, click the latest version of software available.
- 2 Click **Save** to download the software package.
- 3 Open and extract the .tar file.
- 4 Copy all files from the distribution .tar file to the home directory on the update server, maintaining the same folder hierarchy. To simplify provisioning, Polycom recommends editing copies of each file as a best practice to ensure that you have unedited template files containing the default values.
  - The software package contains individual files for the CX5500 system as well as all of the template configuration files included in the combined software package.

For a list and brief description of all available template files included with Polycom CX5500 Software, see the section [Template Configuration Files](#).



### **Note: See the Release Notes for a Description of all Parameters for a UC Software Release**

For a description of each file in a UC Software distribution, see the *UC Software Release Notes* for a particular UC Software release on the [Polycom UC Software Support Center](#).

## Deploy and Update the CX5500 System with a Update Server

If you are provisioning the system using a provisioning server for the first time, follow the provisioning process shown in the section [Deploy CX5500 Systems with a Provisioning Server](#). The CX5500 system can boot up without any configuration files; however, you must configure certain parameters in the configuration files - for example, a registration address, label, and SIP server address – to use the system.

You can create as many configuration files as you need, and your configuration files can contain any combination of parameters. For detailed information on how to use the configuration files, see the section [Template Configuration Files](#).

For large-scale deployments, the centralized provisioning method using configuration files is strongly recommended. For smaller scale deployments, the Web Configuration Utility or local interface can be

used, but administrators need to be aware that settings made using these methods can override settings made using configuration files.

## Deploy CX5500 Systems with a Provisioning Server

You can deploy a group of CX5500 systems using the provisioning server.



### Settings: Configuring Your System for Local Conditions

Most of the default settings are typically adequate; however, if SNTP settings are not available through DHCP, edit the SNTP GMT offset, and possibly the SNTP server address for the correct local conditions. Changing the default daylight savings parameters will likely be necessary outside of North America. Disable the local Web (HTTP) server or change its signaling port if the local security policy dictates (see [<httpd/>](#)). Change the default location settings for user interface language and time and date format (see [<lcl/>](#)).

### To deploy the system with a provisioning server:

- 1 Obtain a list of MAC addresses for the systems you want to deploy.  
The MAC address is a 12-digit hexadecimal number on a label on the back of the power data box and on the outside of the shipping box.
- 2 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`, or `<MACAddress>-license.cfg`. These file names are used by the system itself to store user preferences (overrides) and logging information.
- 3 Add the system registration parameters to the file, for example `reg.1.address`, `reg.1.label`, and `reg.1.type`.
- 4 Create a per-site **site<location>.cfg** file.  
For example, add the SIP server or feature parameters such as `voIpProt.server.1.address` and `feature.corporateDirectory.enabled`.
- 5 Create a master configuration file by performing the following steps:
  - a Enter the name of each per-system and per-site configuration files 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 [Understand 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 so that it points to the log file directory.
  - c (Optional) Edit the `CONTACT_DIRECTORY` attribute of master configuration file so that it points to the organization's contact directory.
  - d (Optional) Edit the `USER_PROFILES_DIRECTORY` attribute of master configuration file if you intend to enable the User Login feature.  
For more information, see [Set User Profiles](#).

- e (Optional) Edit the `CALL_LISTS_DIRECTORY` attribute of master configuration file so that it points to the user call lists.
- 6 Perform the following steps to configure the system to point to the IP address of the provisioning server and set up the user:
  - a On the system's Home screen, select **Settings > Advanced > Admin Settings > Network Configuration > Provisioning Server**.

When prompted for the administrative password, enter **456**. The Provisioning Server entry is highlighted.
  - b Tap the **Select** soft key.
  - c Scroll down to **Server Type** and ensure that it is set to **FTP**.
  - d Scroll down to **Server Address** and enter the IP address of your provisioning server.
  - e Tap the **Edit** soft key to edit the value and the **OK** soft key to save your changes.
  - f Scroll down to **Server User** and **Server Password** and enter the user name and password of the account you created on your provisioning server, for example, *bill1234* and *1234*, respectively.
  - g Tap the **Back** soft key twice.
  - h Tap **Save & Reboot**.

The system reboots.

At this point, the system 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.

For more information, see [Parse Vendor ID Information](#).
- 7 Ensure that the configuration process completed correctly.
- 8 On the system, select **Status > Platform > Application > Main** to see the UC Software version and **Status > Platform > Configuration** to see the configuration files downloaded to the system.
- 9 Monitor the provisioning server event log and the uploaded event log files (if permitted). All configuration files used by the provisioning server are logged.

## Using the RealPresence Resource Manager to Provision CX5500 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 CX5500 system. Make sure to set the base profile to **Generic**.

The following parameters support the RealPresence Resource Manager to provision the CX5500 system:

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

For more information on these parameters, see [Configuration Parameters](#).

## ***Configure the RealPresence Resource Manager to Provision the CX5500 System***

Before you begin to configure the RealPresence Resource Manager (RPRM) to provision the CX5500 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 CX5500 system device settings configuration file through Web Configuration Utility to set the value of the parameter.
- The Base Profile for the CX5500 unified conference station is set to `Generic`.
- The RealPresence Resource Manager, 10.1 and above, supports provisioning the CX5500 unified conference station.



### **Note: Device Settings Configuration**

You won't find the `device.prov.lyncDeviceUpdateEnabled` parameter in the CX5500 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 CX5500 system, allowing you to perform a software upgrade and monitor the online/offline devices using the following methods:

- Provision the CX5500 system using FTP
- Provision the CX5500 system using the Web Configuration Utility

## Provision the CX5500 System using FTP

You can configure the RPRM server to provision the CX5500 system through FTP by storing the configuration files in the FTP root directory.

### To provision the CX5500 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.cfgIf 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 CX5500 systems status.

For more information on configuring the FTP server, see [Set up an FTP Server as Your Provisioning Server](#).

## Provision the CX5500 System using the Web Configuration Utility

You can configure the RPRM server to provision the CX5500 system using Web Configuration Utility by importing the edited configuration file to the CX5500 system.

### To provision the CX5500 system using 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 CX5500 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**.

Login to the RPRM server to view the CX5500 system's status.  
For more information on Web Configuration Utility, see [Web Configuration Utility](#).

## Update CX5500 Software using a USB Flash Drive

In addition to using centralized provisioning to update software, you can also update the software for a single CX5500 system using USB flash drive, external hard-disk drive, or other type of USB storage media with the latest software package. When a flash drive is attached, the system scans the drive for a software repository – if a valid, different software update file is found, a notification displays enabling you to choose to apply or cancel the update. If you do not cancel within 30 seconds, the update begins automatically.

### To update your software using a USB drive:

- 1 Format a USB flash drive as FAT32.

If you are using a drive that is already formatted, ensure that previous software updates are deleted from the USB drive.

- 2 Download the software package to the USB drive. Update files have a .tar extension.
- 3 Connect the USB flash drive to the USB port on the tabletop unit or on the power data box.
- 4 On the CX5500 system, choose to apply the software update request displayed on the LCD screen.

The system detects the new software on the USB drive and starts the update within 30 seconds.

The indicator lights begin to flash, indicating that the update has started. The system reboots up to four times during the update, and the indicator lights flash in several different patterns.

The update is complete when the indicator lights stop flashing.

Additionally, you can use the Web Configuration Utility to set up automatic software updates for a single CX5500 system. Note that configuration changes made to individual systems using the Web Configuration Utility overrides configuration settings made using central provisioning. For instructions on how to update UC Software using the Web Configuration Utility, see [Feature Profile 67993: Use the Software Upgrade Tool in the Web Configuration Utility](#).



# Set Up Basic System Features

---

After you set up your Polycom® systems with a default configuration on the network, system users will be able to place and receive calls. However, you may want to add features to the default configuration to suit your organization and user's needs. Polycom provides basic and advanced features that you can configure for the systems to add efficiency and convenience. This section will show you how to configure all available basic system features and call management features.

Before you begin configuring system features, take the time to read the short introductory section [Read the Feature Parameter Tables](#), which provides important information you need to know in order to successfully perform configuration changes.

This section shows you how to make configuration changes for the following features:

- [Configure Call Logs](#) Contains call information such as remote party identification, time and date, and call duration in three separate lists, missed calls, received calls, and placed calls.
- [Understand the Call Timer](#) Maintains a timer, in hours, minutes, and seconds, for each call in progress.
- [Configure Call Waiting Alerts](#) Visually presents an incoming call on the screen, and plays a configurable sound effect, when you're in another call.
- [Called Party Identification](#) Displays and logs the identity of the party in an outgoing call.
- [Configure Calling Party Identification](#) Displays a caller's identity, derived from the network signaling, when an incoming call is presented—if the information is provided by the call server.
- [Connected Party Identification](#) Displays and logs the identity of the party to whom you are connected to (if the name is provided by the call server).
- [Distinctive Incoming Call Treatment](#) Automatically applies distinctive treatment to calls containing specific attributes.
- [Apply Distinctive Ringing](#) Enables you to select a ring tone for each line, as well as a ring tone for contacts in the contact directory.
- [Apply Distinctive Call Waiting](#) Enables you to map calls to distinct call waiting types.
- [Configure Do Not Disturb](#) Temporarily stops incoming calls.
- [Use the Local Contact Directory](#) The system maintains a local contact directory that can be downloaded from the provisioning server and edited locally. Any edits to the Contact Directory made on the system are saved to the provisioning server as a backup.
- [Configure the Local Digit Map](#) The system has a local set of rules to automate the setup phase of number-only calls.
- [Microphone Mute](#) Mutes the system's microphone so other parties cannot hear you. When the microphone mute feature is activated, the mute buttons on the system glow red.
- [Configure the Speed Dial Feature](#) Enables you to place calls quickly from dedicated keys as well as from a speed dial menu.
- [Set the Time and Date Display](#) Time and date can be displayed in certain operating modes such as when the system is idle and during a call.
- [Set a Graphic Display Background](#) Enables you to display a picture or graphic on the screen's background.



- [Set the Idle Screen Display](#) Enables you to choose which screen displays when the system is idle.
- [Enable Automatic Off-Hook Call Placement](#) Supports an optional automatic off-hook call placement feature for each registration.
- [Enable Skype for Business User Interface](#) Enables you to choose the new user interface where the colors and icons are consistent with that of Skype for Business.
- [Configure Call Hold](#) Pauses activity on one call so that you can use the system for another task, such as making or receiving another call.
- [Use Call Transfer](#) Transfers a call in progress to some other destination.
- [Create Local and Centralized Conferences](#) You can host or join local conferences or create centralized conferences using conference bridge numbers. The advanced aspects of conferencing, like managing parties, are part of the Productivity Suite.
- [Enable Conference Management](#) Add, hold, mute, and remove conference participants, and obtain information about participants.
- [Configure Call Forwarding](#) Provides a flexible call forwarding feature to forward calls to another destination.
- [Configure Lync Call Forwarding](#) Provides a flexible call forwarding feature for CX5500 systems registered with Microsoft Lync Server.
- [Configure Directed Call Pick-Up](#) and [Enable Group Call Pickup](#) Enables you to pick up calls to another system by dialing the extension of the other system. Calls to another system within a pre-defined group can be picked up without dialing the extension of the other system.
- [Configure Call Park and Retrieve](#) Park an active call—puts it on hold to a specific location, so it can be retrieved by any system.
- [Enable Last Call Return](#) Automatically redials the number of the last received call.

## Configure Call Logs



The system records and maintains system events to a call log, also known as a call list. These call logs contain call information such as remote party identification, time and date of the call, and call duration. The log is stored as a file in XML format named **<MACaddress>calls.xml** to your provisioning server. If you want to route the call logs to another server, use the `CALL_LISTS_DIRECTORY` field in the master configuration file. You can use the call logs to redial previous outgoing calls, return incoming calls, and save contact information from call log entries to the contact directory. All call logs are enabled by default. See the table [Configure the Call Logs](#) for instructions on how to enable or disable the call logs.

The systems automatically maintain the call logs in three separate call lists: Missed Calls, Received Calls, and Placed Calls. Each of these call lists can be cleared manually by individual system users. You can delete individual records or all records in a group (for example, all missed calls). You can also sort the records or filter them by line registration.



**Tip: Merged Call Lists**

On some systems, missed and received calls display in one call list. In these combined lists, you can identify call types by the icons:

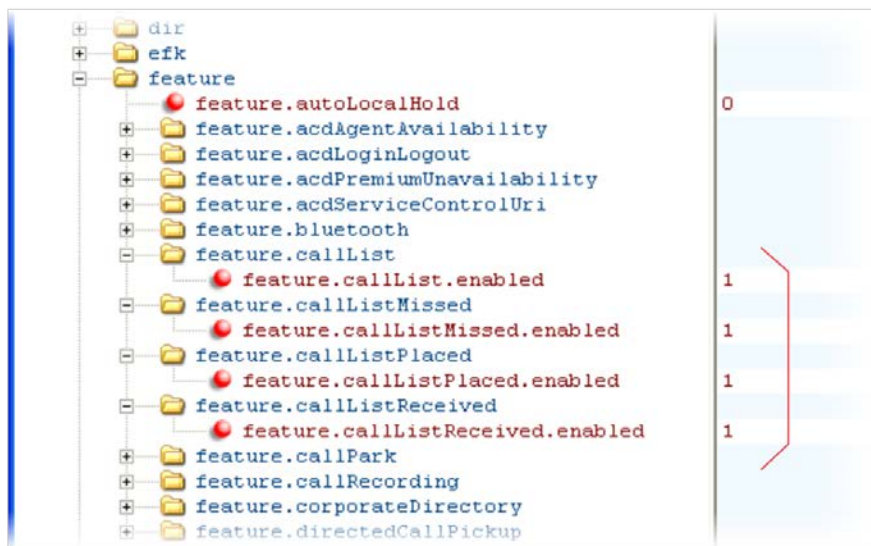
- Missed call icon 
- Received call icon 

**Configure the Call Logs**

<b>Central Provisioning Server</b>	<code>template &gt; parameter</code>
Enable or disable the missed call list	<code>features.cfg &gt; feature.callListMissed.enabled</code>
Enable or disable the placed call list.	<code>features.cfg &gt; feature.callListPlaced.enabled</code>
Enable or disable the received call list	<code>features.cfg &gt; feature.callListReceived.enabled</code>

**Example Call Log Configuration**

The following illustration shows you each of the call log parameters you can enable or disable in the `features.cfg` template file.



The following table describes each element and attribute that displays in the call log. Polycom recommends using an XML editor such as XML Notepad 2007 to view and edit the call log. Note that you can place the elements and attributes in any order in your configuration file.

---

## Call Log Elements and Attributes

<i>Element</i>	<i>Permitted Values</i>
<b>direction</b> Call direction with respect to the user.	<b>In, Out</b>
<b>disposition</b> What happened to the call. When a call entry is first created, the disposition is set to Partial.	<b>Busy, Forwarded, Normal, Partial, Preempted, Rejected, RemotelyHandled, Transferred</b>
<b>line</b> The line (or registration) index.	<b>Positive integer</b>
<b>protocol</b> The line protocol.	<b>SIP</b>
<b>startTime</b> The start time of the call. For example: 2010-01-05T12:38:05 in local time.	<b>String</b>
<b>duration</b> The duration of the call, beginning when it is connected and ending when the call is terminated. For example: PT1H10M59S.	<b>String</b>
<b>count</b> The number of consecutive missed and abandoned calls from a call destination.	<b>Positive Integer</b>
<b>destination</b> The original destination of the call. For outgoing calls, this parameter designates the outgoing call destination; the name is initially supplied by the local system (from the name field of a local contact entry) but may later be updated via call signaling. This field should be used for basic redial scenarios. For incoming calls, the called destination identifies the requested party, which may be different than any of the parties that are eventually connected (the destination may indicate a SIP URI which is different from any SIP URI assigned to any lines on the system).	<b>Address</b>
<b>source</b> The source of the call (caller ID from the call recipient's perspective).	<b>Address</b>
<b>Connection</b> An array of connected parties in chronological order. As a call progresses, the connected party at the far end may change, for example, if the far end transfers the call to someone else. The connected element allows the progression of connected parties, when known, to be saved for later use. All calls that contain a connected state must have at least one connection element created.	<b>Address</b>
<b>finalDestination</b> The final connected party of a call that has been forwarded or transferred to a third party.	<b>Address</b>

---

---

## Understand the Call Timer

A call timer displays on the system's screen. A separate call duration timer displays the hours, minutes, and seconds of each call in progress.

There are no related configuration changes.

## Configure Call Waiting Alerts

By default, the system will alert you to incoming calls while you are in an active call. As shown in the following table, you can disable call waiting alerts and you can specify the ringtone of incoming calls.

### Configuring Call Waiting Alerts

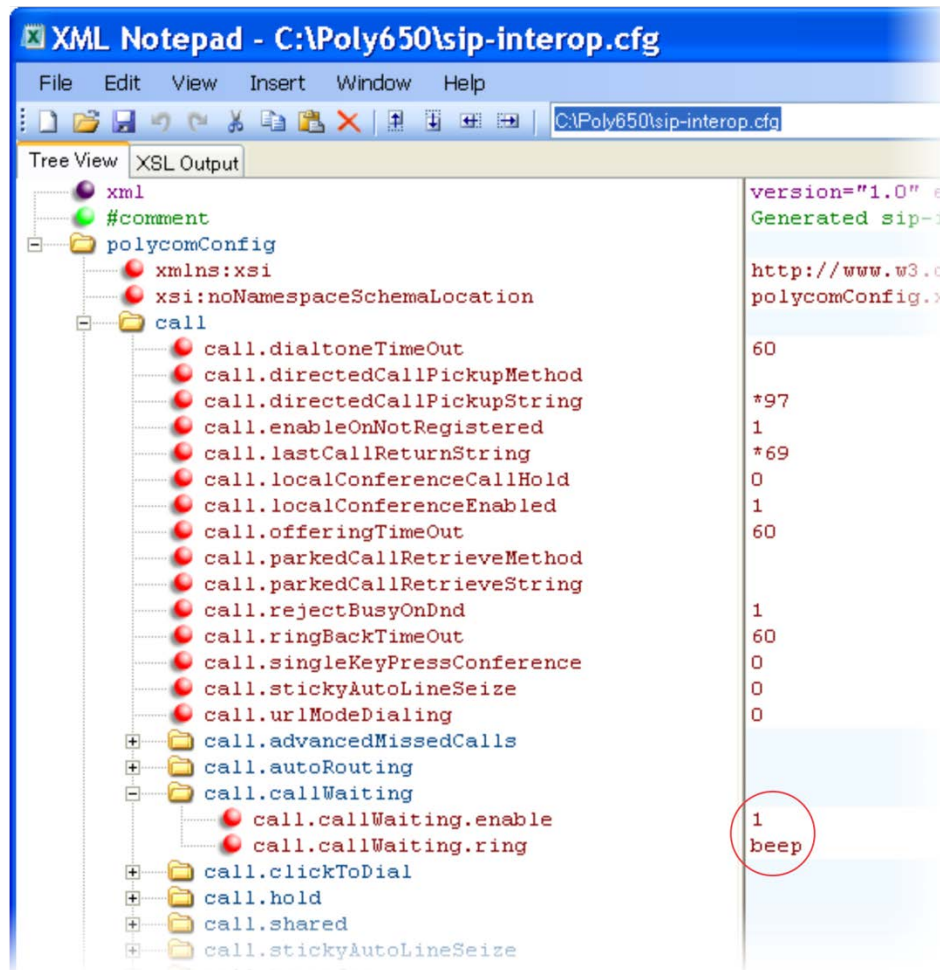
---

Central Provisioning Server	template > parameter
Enable or disable call waiting	<b>sip-interop.cfg</b> > <a href="#">call.callWaiting.enable</a>
Specify the ringtone of incoming calls when you are in an active call	<b>sip-interop.cfg</b> > <a href="#">call.callWaiting.ring</a>

---

## Example Call Waiting Configuration

The following illustration shows you where to disable call waiting alerts and how to change the ringtone of incoming calls in the `sip-interop.cfg` template.



## Called Party Identification

By default, the system displays and logs the identity of parties called from the system. The system obtains called party identity from the network signaling. Because Called Party Identification is a default state, the system will display caller IDs matched to the call server and does not match IDs to entries in the Local Contact Directory or Corporate Directory.

There are no related configuration changes.

## Configure Calling Party Identification

By default, the system displays the identity of incoming callers if available to the system through the network signal. If the incoming call address has been assigned to the contact directory, you can choose

to display the name you assigned there, as shown in the following table. Note that the system cannot match the identity of calling parties to entries in the Corporate Directory.

**Configuring Calling Party Identification**

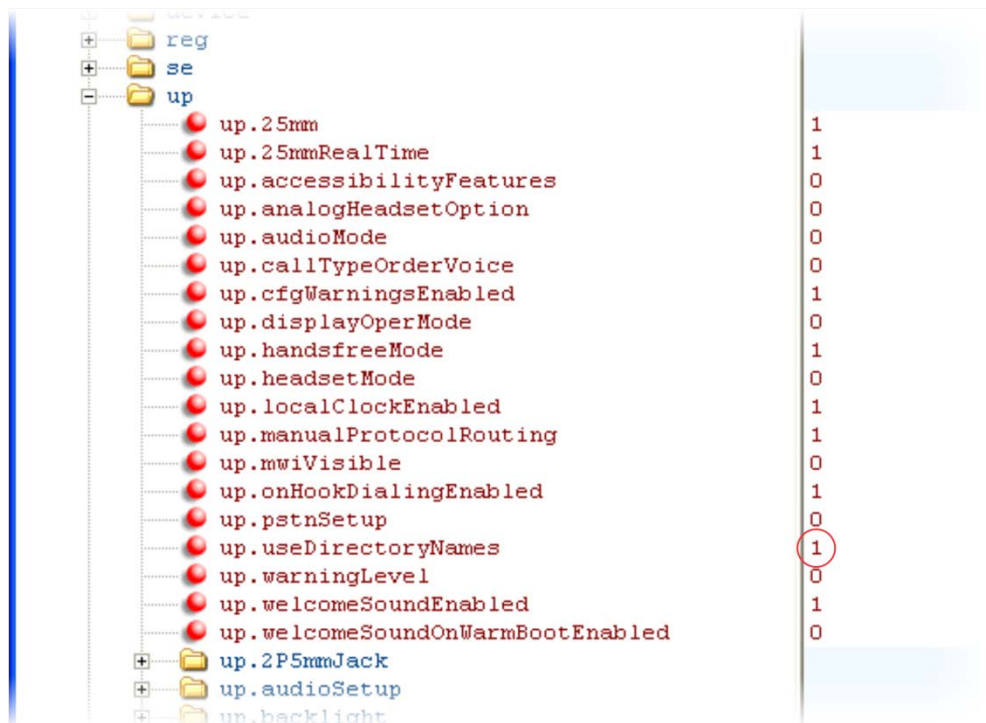
<b>Central Provisioning Server</b>	<code>template &gt; parameter</code>
Substitute the network address ID with the Contact Directory name	<code>reg-advanced.cfg &gt; up.useDirectoryNames</code>
Override the default number of calls per line key for a specific line	<code>reg-advanced.cfg &gt; reg.x.callsPerLineKey</code>

**Web Configuration Utility**

Specify whether or not to substitute the network address with the Contact Directory name. Navigate to **Preferences > Additional Preferences > User Preferences**.

**Example Calling Party Configuration**

The following illustration shows you how to substitute the network address caller ID with the name you assigned to that contact in the contact directory. The ID of incoming call parties will display on the system screen.



**Enable Missed Call Notification**

You can display on the system’s screen a counter that shows the number of missed calls. To reset the counter, view the Missed Calls list on the system. As the following table indicates, you can also configure

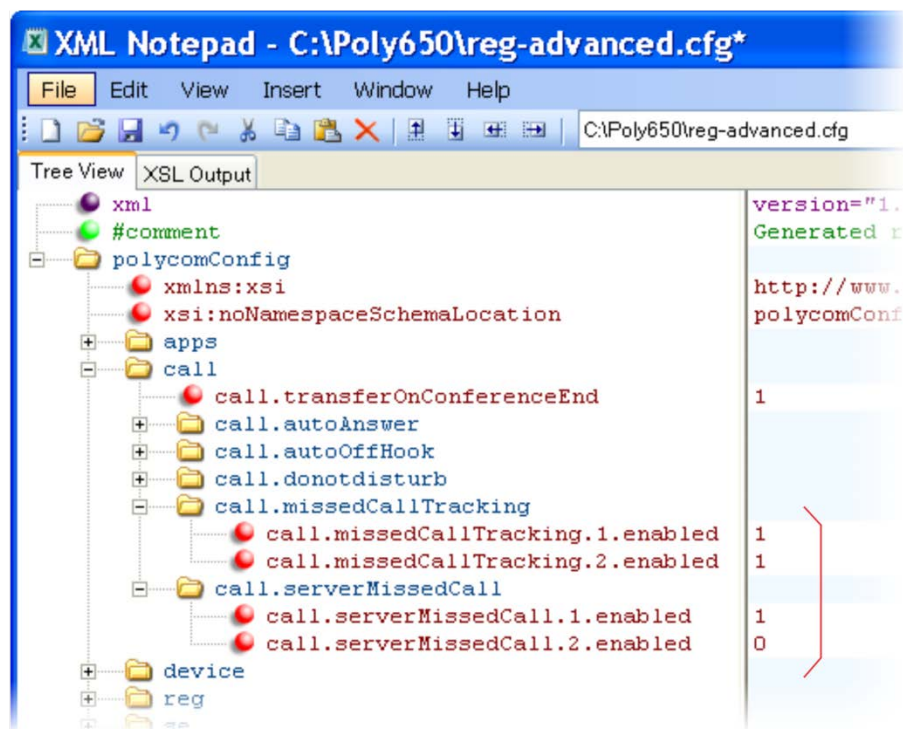
the system to record all missed calls or to display only missed calls that arrive through the Session Initiation Protocol (SIP) server. You can enable Missed Call Notification for each registered line on a system.

### Enabling Missed Call Notification

Central Provisioning Server	template > parameter
Enable or disable the missed call counter for a specific registration	reg-advanced.cfg > call.missedCallTracking.x.enabled
Specify, on a per-registration basis, whether to display all missed calls or only server-generated missed calls	reg-advanced.cfg > call.serverMissedCall.x.enabled

## Example Missed Call Notification Configuration

In the following example, the missed call counter is enabled by default for registered lines 1 and 2, and only server-generated missed calls will be displayed on line 1.



## Connected Party Identification

By default, the system displays and logs the identity of remote parties you connect to if the call server can derive the name and ID from the network signaling. Note that in cases where remote parties have set up certain call features, the remote party you connect to—and the caller ID that displays on the system—may be different than the intended party. For example, Bob places a call to Alice, but Alice has call



---

diversion configured to divert Bob's incoming calls to Fred. In this case, the system will log and display the connection between Bob and Fred. Note that the system does not match party IDs to entries in the contact directory or the corporate directory.

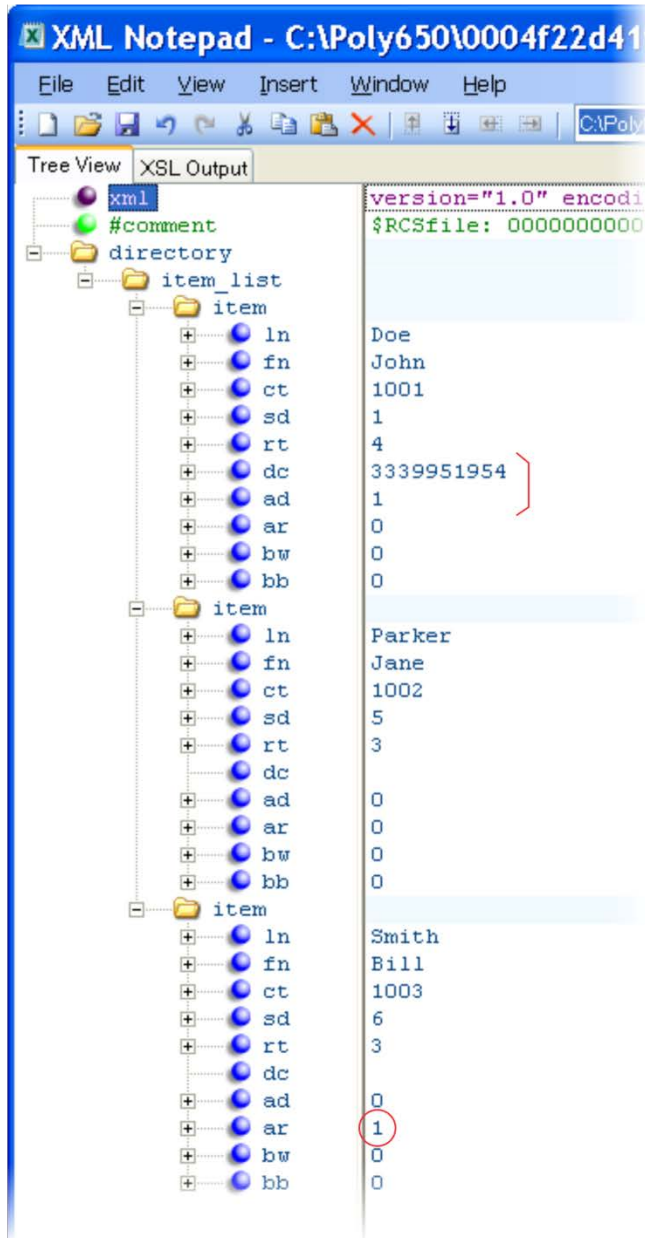
## Distinctive Incoming Call Treatment

You can apply distinctive treatment to specific calls and contacts in your contact directory. You can set up distinctive treatment for each of your contacts by specifying a *Divert Contact*, enabling *Auto-Reject*, or by enabling *Auto-Divert* for a specific contact in the local contact directory (see [Use the Local Contact Directory](#)). You can also apply distinctive treatment to calls and contacts through the system's user interface.



## Example Call Treatment Configuration

In the following example, the Auto Divert feature has been enabled in `ad` so that incoming calls from John Doe will be diverted to SIP address 3339951954 as specified in `dc`. Incoming calls from Bill Smith have been set to Auto Reject in `ar` and will be sent to voicemail.



Note that if you enable both the Auto Divert and Auto Reject features, Auto Divert has precedence over Auto Reject. For a list of all parameters you can use in the contact directory, see the table [Understanding the Local Contact Directory](#).

## Apply Distinctive Ringing

The distinctive ringing feature enables you to apply a distinctive ringtone to a registered line, a specific contact, or type of call.

There are three ways to set distinctive ringing, and the following table shows the parameters for each. If you set up distinctive ringing using more than one of the following methods, the system will use the highest priority method.

- You can assign ringtones to specific contacts in the Contact Directory. For more information, see [Distinctive Incoming Call Treatment](#). This option is first and highest in priority.
- You can use the `voIpProt.SIP.alertInfo.x.value` and `voIpProt.SIP.alertInfo.x.class` parameters in the `sip-interop.cfg` template to map calls to specific ringtones. The value you enter depends on the call server. This option requires server support and is second in priority.
- You can select a ringtone for each registered line on the system. Select **Settings > Basic > Ring Type**. This option has the lowest priority.

### Apply Distinctive Ringing

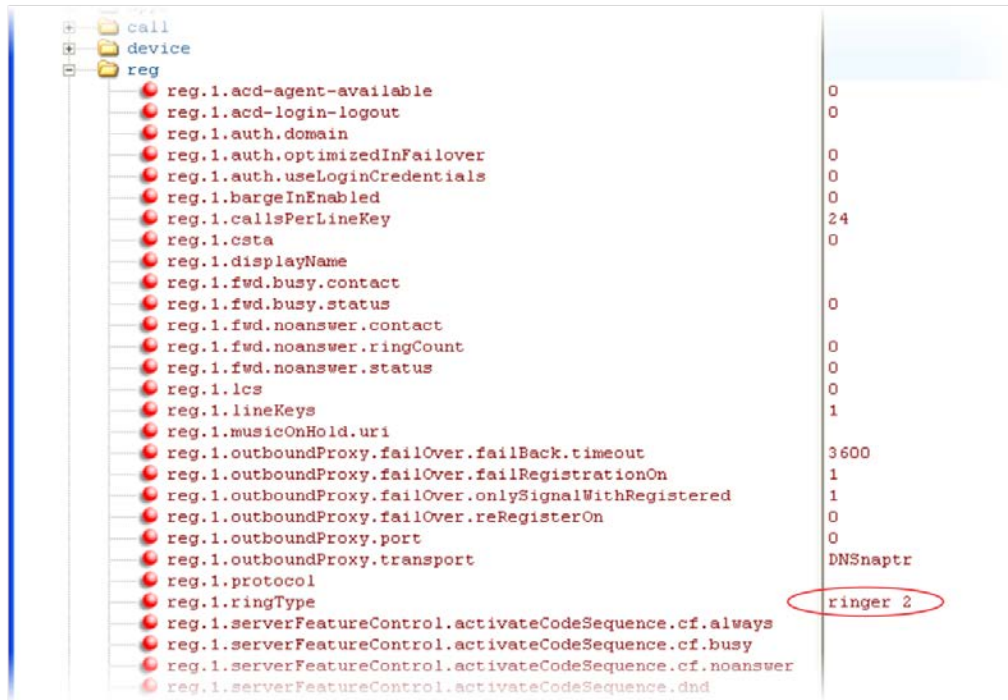
Central Provisioning Server	template > parameter
Map alert info string in the SIP header to ringtones	<code>sip-interop.cfg &gt; voIpProt.SIP.alertInfo.x.class</code> <code>sip-interop.cfg &gt; voIpProt.SIP.alertInfo.x.value</code>
Specify a ringtone for a specific registered line	<code>reg-advanced.cfg &gt; reg.x.ringType</code>
Specify ringtones for contact directory entries	<code>000000000000-directory~.xml</code>

### Local System User Interface

You can edit the ringtone of each registered line by navigating to **Settings > Basic > Ring Type**. To edit the ringtone for a specific contact, navigate to **Settings > Features > Contact Directory**, highlight a contact, tap the **Edit** soft key, and specify a value for the **Ring Type**.

## Example Distinctive Ringing Configuration

The following illustration shows that the ring type `ringer2` has been applied to incoming calls to line 1.



For a list of all parameters and their corresponding ringtones, see [Ringtone Pattern Names](#).

## Apply Distinctive Call Waiting

You can use the alert-info values and class fields in the SIP header to map calls to distinct call-waiting types. You can apply three call waiting types: beep, ring, and silent. The following table shows the parameters you can configure for this feature. This feature requires call server support.

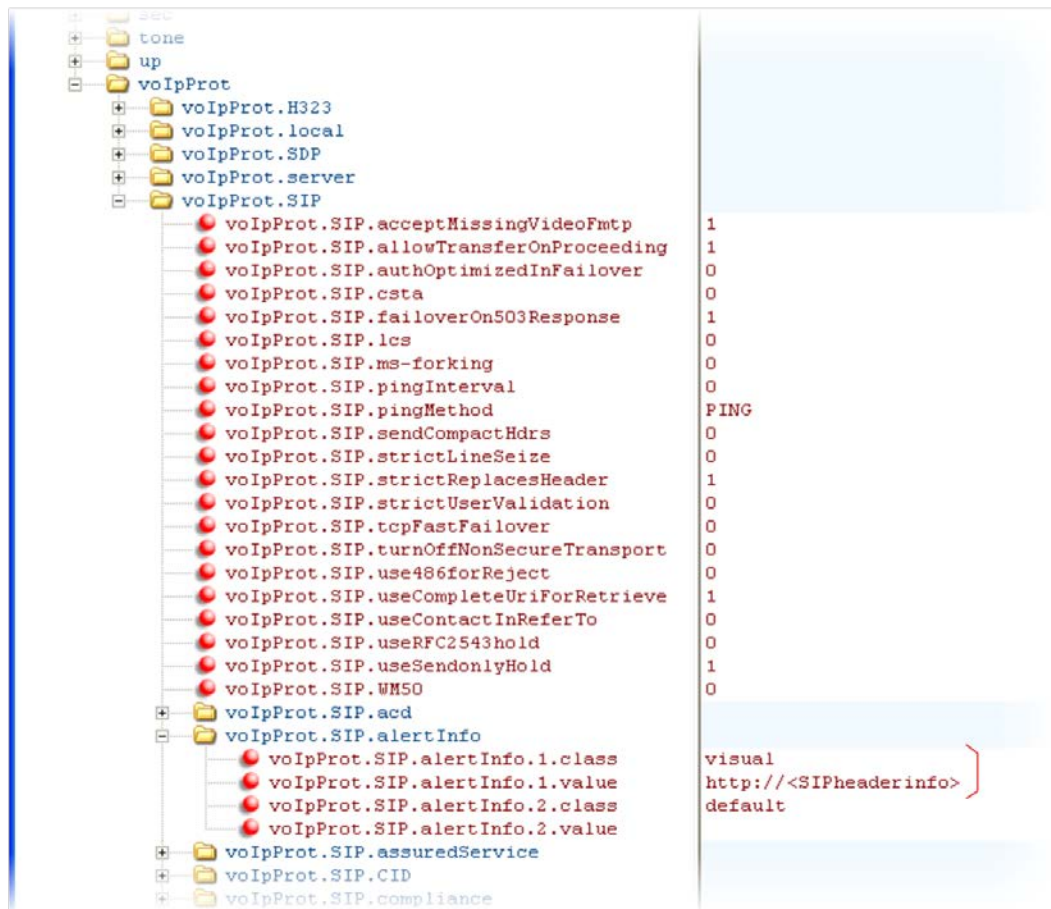
### Apply Distinctive Call Waiting

Central Provisioning Server	template > parameter
Enter the string which displays in the SIP alert-info header	sip-interop.cg > volpProt.SIP.alertInfo.x.value
Enter the ring class name	sip-interop.cfg > volpProt.SIP.alertInfo.x.class

## Example Distinctive Call Waiting Configuration

In the following illustration, `voIpProt.SIP.alertInfo.1.value` is set to `http://<SIP headerinfo>`. An incoming call with this value in the SIP alert-info header will cause the system to ring in a manner

specified by `voIpProt.SIP.alertInfo.x.class`. In this example, the system will display a visual LED notification, as specified by the value `visual`.



## Configure Do Not Disturb

You can use the Do Not Disturb (DND) feature to temporarily stop incoming calls. You can also turn off audio alerts and receive visual call alerts only, or you can make your system appear busy to incoming callers. Incoming calls received while DND is turned on are logged as missed.

DND can be enabled locally through the system or through a server. The table [Configure Do Not Disturb](#) lists parameters for both methods. The local DND feature is enabled by default, and you have the option of disabling it. When local DND is enabled, you can turn DND on and off using the **Do Not Disturb** button on the system. Local DND can be configured only on a per-registration basis. If you want to forward calls while DND is enabled, see [Configure Call Forwarding](#).



### Note: Using Do Not Disturb on Shared Lines

A system that has DND enabled and activated on a shared line will visually alert you to an incoming call, but the system will not ring.

If you want to enable server-based DND, you must enable the feature on both a registered system and on the server. The benefit of server-based DND is that if a system has multiple registered lines, you can apply DND to all line registrations on the system; however, you cannot apply DND to individual registrations on a system that has multiple registered lines. Note that although server-based DND disables the local Call Forward and DND features, if an incoming is not routed through the server, you will still receive an audio alert.

Server-based DND behaves the same way as the pre-SIP 2.1 per-registration feature with the following exceptions:

- You cannot enable server-based DND if the system is configured as a shared line.
- If server-based DND is enabled but not turned on, and you press the DND key or select DND on the system's Features menu, the "Do Not Disturb" message will display on the system and incoming calls will continue to ring.

### Configure Do Not Disturb

#### Central Provisioning Server

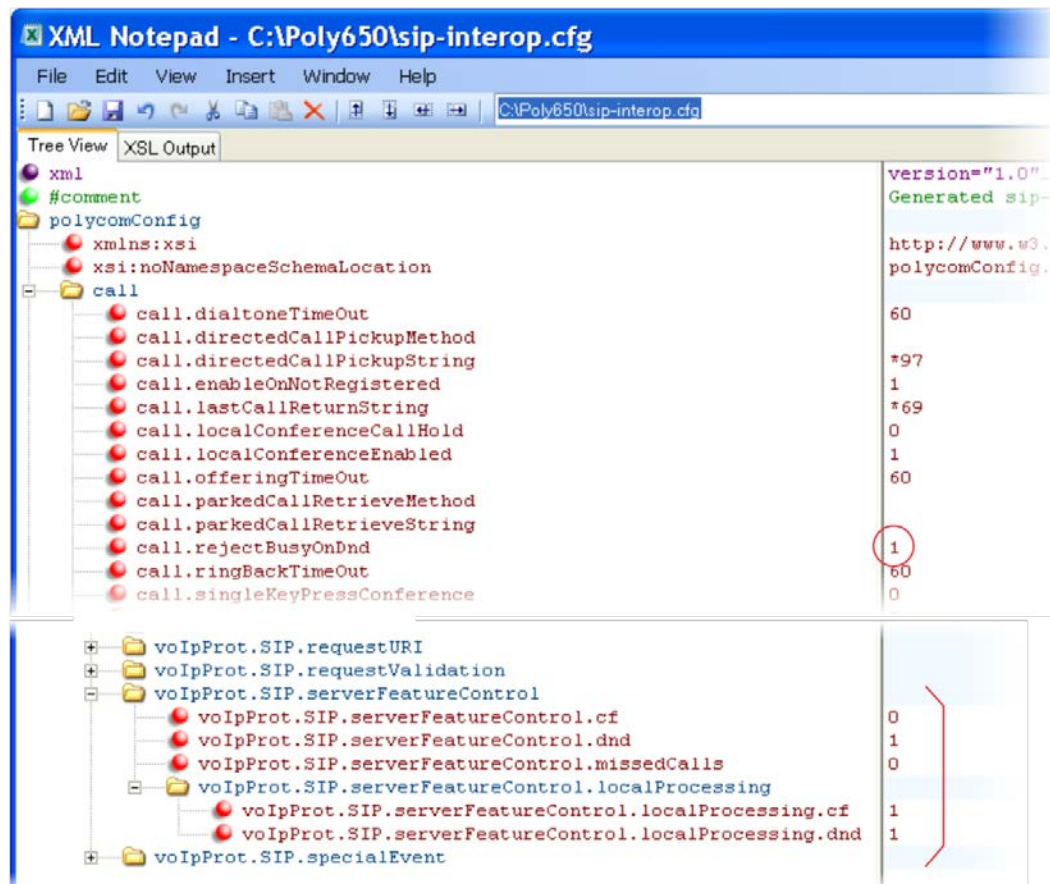
Enable or disable server-based DND	<b>template</b> > <a href="#">parameter</a>  <b>sip-interop.cfg</b> > <a href="#">volpProt.SIP.serverFeatureControl.dnd</a>
Enable or disable local DND behavior when server-based enabled	<b>sip-interop.cfg</b> > <a href="#">volpProt.SIP.serverFeatureControl.localProcessing.dnd</a>
Specify whether, when DND is turned on, the system rejects incoming calls with a busy signal or gives you a visual and no audio alert.	<b>sip-interop.cfg</b> > <a href="#">call.rejectBusyOnDnd</a>
Enable DND as a per-registration feature or use it as a global feature for all registrations	<b>reg-advanced.cfg</b> > <a href="#">call.donotdisturb.perReg</a>

#### Local System User Interface

If DND is enabled, you can turn DND on or off using the Do Not Disturb key or the Do Not Disturb menu option in the Features menu

## Example Do Not Disturb Configuration

In the following example, taken from the `sip-interop.cfg` template, server-based DND has been enabled in `serverFeatureControl.dnd`, and `rejectBusyOnDnd` has been set to 1—enabled—so that when you turn on DND on the system, incoming callers will receive a busy signal.



## Use the Local Contact Directory

The systems feature a contact directory you can use to store frequently used contacts.

Note that the system follows a precedence order when looking for a contact directory. A system will look first for a local directory in its own memory, next for a `<MACaddress>-directory.xml` that is uploaded to the server, and finally for a seed directory `00000000000-directory~.xml` that is included in your UC software download.

Changes you make to the contact directory from the system are stored on the system drive and uploaded to the provisioning server in `<MACaddress>-directory.xml`. This enables you to preserve a contact directory during reboots.

If you want to use the seed directory, locate `00000000000-directory~.xml` in your UC Software files on the server and remove the tilde (~) from the file name. The system will substitute its own MAC address for `<00000000000>`.



The contact directory is the central database for several system features including speed dial (see [Configure the Speed Dial Feature](#)), distinctive incoming call treatment (see [Distinctive Incoming Call Treatment](#)), and presence (see [Use the Presence Feature](#)). The following table lists the directory parameters you can configure. The CX5500 system supports up to 999 contacts. If you want to conserve system memory, you can configure the systems to support a lower maximum number of contacts.



**Tip: Deleting the Per-System Contact Directory**

If you created a per-system <MACaddress>-directory.xml for a system and you want that system to use a global contact directory 000000000000-directory.xml, remove the <MACaddress>-directory.xml file you created from the server.

**Use the Local Contact Directory**

**Central Provisioning Server**

Enable or disable the local contact directory	<code>template &gt; parameter</code>
Specify if the local contact directory is read-only	<code>features.cfg &gt; feature.directory.enabled</code>
Specify the maximum number of contact entries for each system	<code>features.cfg &gt; dir.local.readonly</code>
Specify whether to search the directory by first name or last name	<code>features.cfg &gt; dir.local.contacts.maxNum</code>
The template contact directory file	<code>features.cfg &gt; dir.search.field</code>
	<code>000000000000-directory~.xml</code>

**Example Configuration**

The following illustration shows four contacts configured in a directory file.

```

version="1.0" standalone="yes"

    <item>
      <ln>Gates</ln>
      <fn>Lauren</fn>
      <ct>555-555-5556</ct>
      <sd>13</sd>
      <rt>ringer1</rt>
    </item>

    <item>
      <ln>Blue</ln>
      <fn>Don</fn>
      <ct>1144</ct>
      <sd>2</sd>
    </item>

    <item>
      <ln>Chen</ln>
      <fn>George</fn>
      <ct>5678</ct>
      <sd>11</sd>
    </item>

    <item>
      <ln>Clement</ln>
      <fn>Francois</fn>
      <ct>2589</ct>
      <sd>9</sd>
    </item>
  
```

The following table describes each of the parameter elements and permitted values that you can use in the local contact directory.

### Understanding the Local Contact Directory

<i>Element</i>	<i>Definition</i>	<i>Permitted Values</i>
<b>fn</b>	<b>First Name</b>	<b>UTF-8 encoded string of up to 40 bytes<sup>1</sup></b>
	The contact's first name.	
<b>ln</b>	<b>Last Name</b>	<b>UTF-8 encoded string of up to 40 bytes<sup>1</sup></b>
	The contact's last name.	
<b>ct</b>	<b>Contact</b>	<b>UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL</b>
	Used by the system to address a remote party in the same way that a string of digits or a SIP URL are dialed manually by the user. This element is also used to associate incoming callers with a particular directory entry. The maximum field length is 128 characters. Note: This field cannot be null or duplicated.	
<b>sd</b>	<b>Speed Dial Index</b>	<b>Null, 1 to 9999</b>
	Associates a particular entry with a speed dial key for one-touch dialing or dialing from the speed dial menu. Note:	
<b>lb</b>	<b>Label</b>	<b>UTF-8 encoded string of up to 40 bytes<sup>1</sup></b>
	The label for the contact. Note: The label of a contact directory item is by default the label attribute of the item. If the label attribute does not exist or is Null, then the first and last names will form the label. A space is added between first and last names.	
<b>pt</b>	<b>Protocol</b>	<b>SIP, or Unspecified</b>
	The protocol to use when placing a call to this contact.	
<b>rt</b>	<b>Ring Tone</b>	<b>Null, 1 to 21</b>
	When incoming calls match a directory entry, this field specifies the ringtone that will be used.	
<b>dc</b>	<b>Divert Contact</b>	<b>UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL</b>
	The address to forward calls to if the Auto Divert feature is enabled.	
<b>ad</b>	<b>Auto Divert</b>	<b>0 or 1</b>
	If set to 1, callers that match the directory entry are diverted to the address specified for the divert contact element. Note: If auto-divert is enabled, it has precedence over auto-reject.	
<b>ar</b>	<b>Auto Reject</b>	<b>0 or 1</b>
	If set to 1, callers that match the directory entry specified for the auto-reject element are rejected. Note: If auto divert is also enabled, it has precedence over auto reject.	
<b>bw</b>	<b>Buddy Watching</b>	<b>0 or 1</b>
	If set to 1, this contact is added to the list of watched systems.	



Element	Definition	Permitted Values
<b>bb</b>	<b>Buddy Block</b>	<b>0 or 1</b>

If set to 1, this contact is blocked from watching this system.

<sup>1</sup> In some cases, this will be less than 40 characters due to UTF-8's variable bit length encoding.

## Configure the Local Digit Map

The system has a local digit map feature that, when configured, will automatically call a dialed number, eliminating the need to press the **Dial** or **Send** soft key to place outgoing calls. Note that digit maps do not apply to on-hook dialing.

Digit maps are defined by a single string or a list of strings. If a number you dial matches any string of a digit map, the call is automatically placed. If a number you dial matches no string—an impossible match—you can specify the system's behavior. If a number ends with #, you can specify the system's behavior, called trailing # behavior. You can also specify the digit map timeout, the period of time after you dial a number that the call will be placed. The parameter for each of these options is outlined in the following table. The configuration syntax of the digit map is based on recommendations in section 2.1.5 of [RFC 3435](#).



### Web Info: Changing the Local Digit Map on Polycom Systems

For instructions on how to modify the Local Digit Map, see [Technical Bulletin 11572: Changes to Local Digit Maps on SoundPoint IP, SoundStation IP, and Polycom VVX 1500 Systems](#).

### Configure the Local Digit Map

Central Provisioning Server	template > parameter
Apply a dial plan to dialing scenarios	site.cfg > dialplan.applyTo*
Specify the digit map to use for the dial plan	site.cfg > dialplan.digitmap
Specify the timeout for each segment of the digit map	site.cfg > dialplan.digitmap.timeOut
Specify the behavior if an impossible dial plan match occurs	site.cfg > dialplan.impossibleMatchHandling
Specify if trailing # digits should be removed from digits sent out	site.cfg > dialplan.removeEndOfDial
Specify the details for emergency dial plan routing	site.cfg > dialplan.routing.emergency.x.*
Specify the server that will be used for routing calls	site.cfg > dialplan.routing.server.x.*
Configure the same parameters as above for a specific registration (overrides the global parameters above)	site.cfg > dialplan.x.*
Specifies the time in seconds that the system waits before dialing a number when you dial on-hook	site.cfg > dialplanuserDialtimeOut

---

## Web Configuration Utility

Specify impossible match behavior, trailing # behavior, digit map matching strings, and time-out value by navigating to **Settings > SIP** and expanding the **Local Settings** menu.

---

## Understand Digit Map Rules

The following is a list of digit map string rules. If you are using a list of strings, each string in the list can be specified as a set of digits or timers, or as an expression which the gateway will use to find the shortest possible match.

Digit map extension letter *R* indicates that certain matched strings are replaced. Using a *RRR* syntax, you can replace the digits between the first two *Rs* with the digits between the last two *Rs*. For example, **R555R604R** would replace 555 with 604. Digit map timer letter *T* indicates a timer expiry. Digit map protocol letters *S* and *H* indicate the protocol to use when placing a call. The following examples illustrate the semantics of the syntax:

- **R9R604Rxxxxxxx**—Replaces 9 with 604
- **xxR601R600Rxx**—When applied to 1160122 gives 1160022
- **R9RRxxxxxxx**—Remove 9 at the beginning of the dialed number (replace 9 with *nothing*)
  - For example, if a customer dials 914539400, the first 9 is removed when the call is placed.
- **RR604Rxxxxxxx**—Prepend 604 to all seven-digit numbers (replace *nothing* with 604)
  - For example, if a customer dials 4539400, 604 is added to the front of the number, so a call to 6044539400 is placed.
- **xR60xR600Rxxxxxxx**—Replace any 60x with 600 in the middle of the dialed number that matches
  - For example, if a customer dials 16092345678, a call is placed to 16002345678.
- **911xxx.T**—A period (.) that matches an arbitrary number, including zero, of occurrences of the preceding construct
  - For example:
    - 911123 with waiting time to comply with *T* is a match
    - 9111234 with waiting time to comply with *T* is a match
    - 91112345 with waiting time to comply with *T* is a match
    - and the number can grow indefinitely given that pressing the next digit takes less than *T*.
- **0xxxS**—All four digit numbers starting with a 0 are placed using the SIP protocol.

Take note of the following guidelines:

- The following letters are case sensitive: *x*, *T*, *R*, *S*, and *H*.
- You must use only \*, #, +, or 0–9 between the second and third *R*.
- If a digit map does not comply, it is not included in the digit plan as a valid map. That is, no match will be made.
- There is no limit to the number of *R* triplet sets in a digit map. However, a digit map that contains less than a full number of triplet sets (for example, a total of 2 *Rs* or 5 *Rs*) is considered an invalid digit map.

- If you use *T* in the left part of *RRR*'s syntax, the digit map will not work. For example, R0TR322R will not work.

## Microphone Mute

When you activate microphone mute, the Mute keys glow red. The Mute keys can be configured to mute audio and video when the CX5500 system is connected to a computer. No configuration changes can be made to the microphone mute feature when using the CX5500 system as a standalone system not connected to a computer.

## Configure the Speed Dial Feature

You can link entries in your local contact directory to speed dial contacts on the system. The speed dial feature enables you to place calls quickly using dedicated line keys or from a speed dial menu. To set up speed dial through the system's contact directory, see [Use the Local Contact Directory](#). Speed dial configuration is also explained briefly in [Configure the Speed Dial Feature](#). In order to set up speed dial contacts become familiar with parameters in the following table, which identifies the directory XML file and the parameters you need to set up your speed dial contacts.

The speed dial index range is 1 to 9999.

On some call servers, enabling Presence for an active speed dial contact will display that contact's status on the speed dial's line key label. For information on how to enable Presence for contacts, see [Use the Presence Feature](#).

### Configure the Speed Dial Feature

#### Central Provisioning Server

template > parameter

Enter a speed dial index number in the `<sd>x</sd>` element in the `<MAC address>-directory.xml` file to display a contact directory entry as a speed dial key on the system. Speed dial contacts are assigned to unused line keys and to entries in the system's speed dial list in numerical order.

The template contact directory file

**00000000000-directory~.xml**

#### Local System User Interface

New directory entries are assigned to the Speed Dial Index in numerical order. To assign a speed dial index to a contact, navigate go to **Contact Directory**, highlight the contact, press the **Edit** soft key, and specify a Speed Dial Index.

## Example Speed Dial Configuration

The first time you deploy and reboot the systems with UC Software, a template contact directory file named **00000000000-directory~.xml** is loaded to the provisioning server. You can edit and use this template file as a global contact directory for a group of systems or you can create your own per-system directory file. To create a global directory, locate the **00000000000-directory~.xml** template in your UC Software files and remove the tilde (~) from the file name. When you reboot, the system substitutes the global file with its own `<MACaddress>-directory.xml` which is uploaded to the server. If you want to

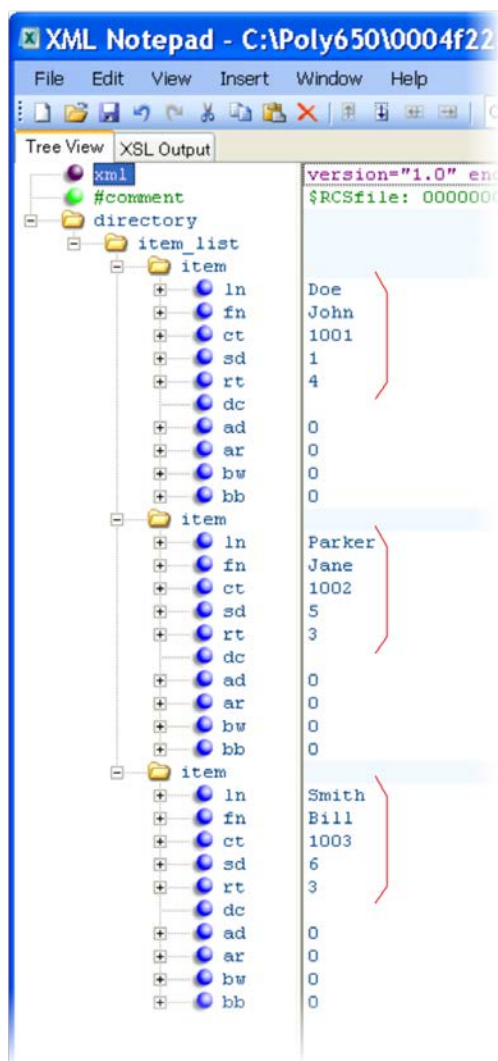
create a per-system directory, replace `<000000000000>` in the global file name with the system's MAC address, for example, `<MACAddress>directory.xml`.

On each subsequent reboot, the system will look for its own `<MACAddress>directory.xml` and then look for the global directory. Contact directories stored locally on the system may or may not override the `<MACAddress>directory.xml` on the server depending on your server configuration. The system will always look for a local directory or `<MACAddress>directory.xml` before looking for the global directory.

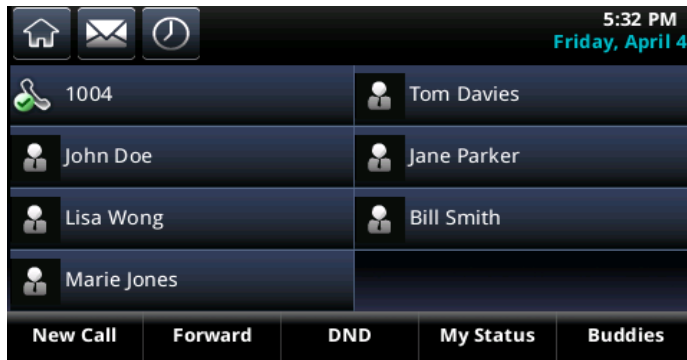
For more information on how to use the template directory file `000000000000-directory~.xml`, see [Use the Local Contact Directory](#).

Once you have renamed the directory file as a per-system directory, enter a number in the speed dial `<sd>` field to display a contact directory entry as a speed dial contact on the system. Speed dial entries automatically display on unused line keys on the system and are assigned in numerical order.

The example local contact directory file shown next is saved with the system's MAC address and shows the contact *John Doe* with extension number *1001* as speed dial entry *1* on the system.



This configuration results in the following speed dial keys on the system.



## Set the Time and Date Display

A clock and calendar are enabled by default. You can display the time and date for your time zone in several formats, or you can turn it off altogether. You can also set the time and date format to display differently when the system is in certain modes. For example, the display format can change when the system goes from idle mode to an active call. You will have to synchronize the system to the Simple Network Time Protocol (SNTP) time server. Until a successful SNTP response is received, the system will continuously flash the time and date to indicate that they are not accurate.

The time and date display on systems in PSTN mode will be set by an incoming call with a supported Caller ID standard, or when the system is connected to Ethernet and you enable the turn on the date and time display.

### Set the Time and Date Display

#### Central Provisioning Server

`template > parameter`

Turn the time and date display on or off.

`reg-advanced.cfg` and `site.cfg > up.localClockEnabled`

Set the time and date display format.

`site.cfg > lcl.datetime.date.*`

Display time in the 24-hour format

`site.cfg > lcl.datetime.time.24HourClock`

Set the basic SNTP settings and daylight savings parameters.

`site.cfg > tcplpApp.snntp.*`

#### Web Configuration Utility

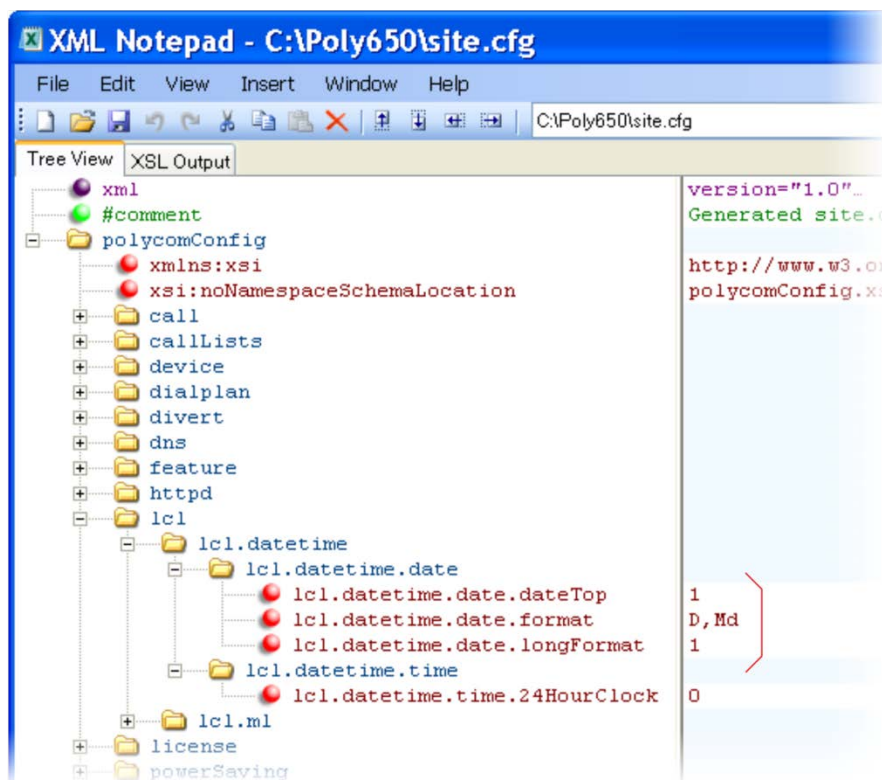
To set the basic SNTP and daylight savings settings navigate to **Preferences > Date & Time**.

#### Local System User Interface

Basic SNTP settings can be made in the Network Configuration menu—see DHCP Menu or Ethernet Menu. To set the time and date format and enable or disable the time and date display, tap **Settings > Basic > Preferences > Time & Date**.

## Example Configuration

The following illustration shows an example configuration for the time and date display format. In this illustration, the date is set to display over the time and in long format. The D, Md indicates the order of the date display, in this case, day of the week, month, and day. In this example, the default time format is used, or you can enable the 24-hour time display format.



Use the following table to choose values for the `lcl.datetime.date.format` and `lcl.datetime.date.longformat` parameters. The table shows values for the date Friday, August 19, 2011.

### Date Formats

<code>lcl.datetime.date.format</code>	<code>lcl.datetime.date.longformat</code>	Date Displayed on System
dM,D	0	19 Aug, Fri
dM,D	1	19 August, Friday
Md,D	0	Aug 19, Fri
Md,D	1	August 19, Friday
D,dM	0	Fri, 19 Aug
D,dM	1	Friday, August 19

<i>lcl.datetime.date.format</i>	<i>lcl.datetime.date.longformat</i>	<i>Date Displayed on System</i>
DD/MM/YY	n/a	19/08/11
DD/MM/YYYY	n/a	19/08/2011
MM/DD/YY	n/a	08/19/11
MM/DD/YYYY	n/a	08/19/2011
YY/MM/DD	n/a	11/08/19
YYYY/MM/DD	n/a	2011/08/11

## Set a Graphic Display Background

You can display a .PNG or .BMP image on the background of the touch screen. The following table links you to parameters and definitions in the reference section. Note that a Graphic Display Background displays across the entire screen and the time and date and line and soft key labels display over the backgrounds.



### Note: Choosing a Graphic Display Background

Depending on the image you use, the graphic display background may affect the visibility of text and numbers on the system screen. As a general rule, backgrounds should be light in shading for better system and feature usability.

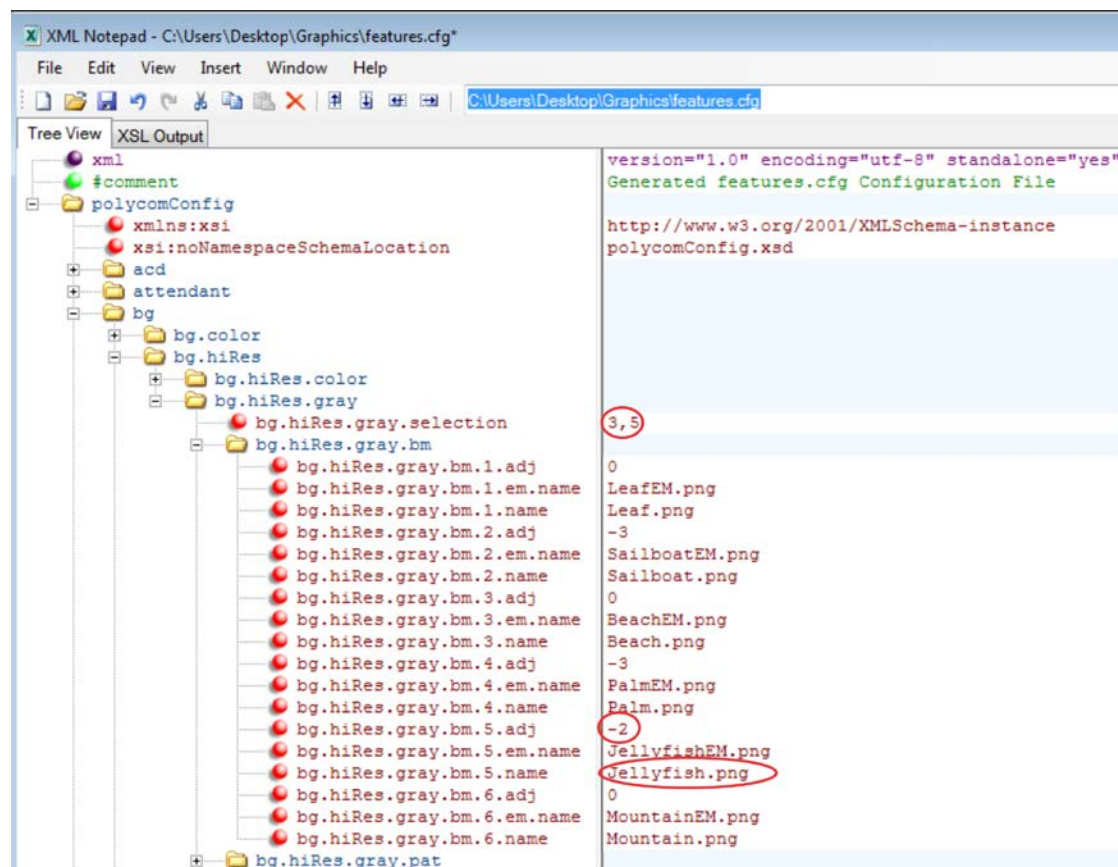
### Set a Graphic Display Background

<b>Central Provisioning Server</b>	<b>template &gt; parameter</b>
Specify a background to display for your system type	<b>features.cfg &gt; bg.*</b>
Modify the color of the line and soft keys	<b>features.cfg &gt; button.*</b>
<b>Web Configuration Utility</b>	
Specify which background to display by navigating to <b>Preferences &gt; Background</b>	
<b>Local System User Interface</b>	
To select a background, on the system, navigate to <b>Settings &gt; Basic &gt; Preferences &gt; Background &gt; Select Background</b> .	



## Example Graphic Display Background Configuration

This example configuration shows a background image applied to the CX5500 system. The default background in the `features.cfg` template file, specified in the `bg.hiRes.gray.selection` parameter, is set to 2,1. Where 2 = `bg.hiRes.gray.pat.solid.*` and 1 = `bg.hiRes.gray.pat.solid.1.*`, the system will display the solid color specified by the RGB color pattern, in this case the color named *White*. In this example, the `bg.hiRes.gray.selection` parameter has been set to 3,5. Where 3 = `bg.hiRes.gray.bm.*` and 5 = `bg.hiRes.gray.bm.5.*`, the system will display the image named *Jellyfish.png*. In addition, the `bg.hiRes.gray.bm.6.adj` parameter has been changed to -2 to lighten the background image so as not to conflict with the time and date display.





This example configuration will result in the following graphic display background on the system screen. Note that line and soft key labels will display over the background image.



## Set the Idle Screen Display

By default, the Lines screen displays when the CX5500 unified conference station is idle and not in use. You can choose to have either the Lines screen, the Home screen, or the dialpad display when the system is idle.

If the Lines or Home screen are set as the default view, users can tap the **Home** soft key to access the Lines or Home screen. If the dialpad is set as the default view, users can tap the Home soft key to display the Home screen and the dialpad.

### Enable Automatic Off-Hook Call Placement

#### Central Provisioning Server

**template** > [parameter](#)

Specify the screen that displays when the system is idle and not in use.

**features** > [up.idleStateView](#)

## Enable Automatic Off-Hook Call Placement

You can configure the system to automatically place a call to a specified number when you go off-hook. This feature is sometimes referred to as *hot dialing*. The system goes off-hook when you press the New Call soft key. As shown in the following table, you can specify an off-hook call contact and enable or disable the feature for specific line registrations.

### Enable Automatic Off-Hook Call Placement

#### Central Provisioning Server

**template** > [parameter](#)

Specify the contact to dial when the system goes off-hook

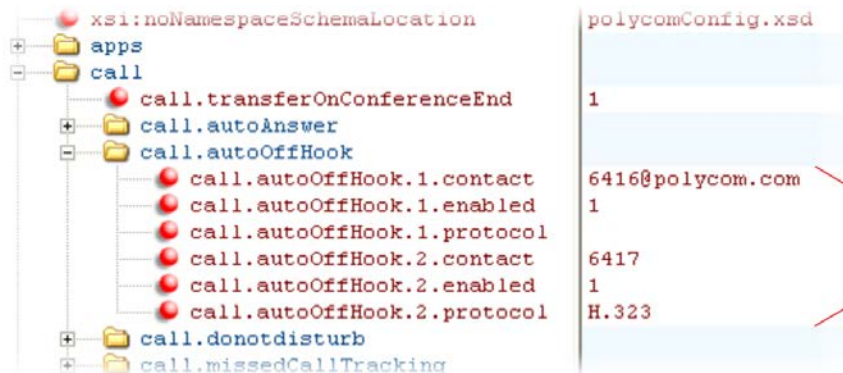
**reg-advanced** > [call.autoOffHook.x.contact](#)

Enable or disable automatic off-hook call placement on registration  
x

**reg-advanced** > [call.autoOffHook.x.enabled](#)

## Example Automatic Off-Hook Placement Configuration

In the example configuration shown next, the automatic off-hook call placement feature has been enabled for registration 1 and registration 2. If registration 1 goes off-hook, a call is placed automatically to `6416@polycom.com`, the contact that has been specified for registration 1 in `call.autoOffHook.1.contact`. Similarly, if registration 2 goes off-hook, a call is placed automatically to 6417.



## Configure Call Hold

The purpose of call hold is to pause activity on one call so that you can use the system for another task, for example, to place or receive another call or to search your system’s menu for information. See the table [Enable Call Hold](#) for a list of available parameters you can configure for this feature. When you place an active call on hold, a message will inform the held party that they are on hold. You can also configure a call hold alert to remind you after a period of time that a call is still on hold.

As of SIP 3.1, if supported by the call server, you can enter a music-on-hold URI. For more information, see [Session Initiation Protocol Service Example - Music on Hold](#).

### Enable Call Hold

Central Provisioning Server	template > parameter
Specify whether to use RFC 2543 (c=0.0.0.0) or RFC 3264 (a=sendonly or a=inactive) for outgoing hold signaling	<b>sip-interop.cfg</b> > <b>volpProt.SIP.useRFC2543hold</b>
Specify whether to use sendonly hold signaling	<b>sip-interop.cfg</b> > <b>volpProt.SIP.useSendonlyHold</b>
Configure local call hold reminder options	<b>sip-interop.cfg</b> > <b>call.hold.localReminder.*</b>
Specify the music-on-hold URI	<b>sip-interop.cfg</b> > <b>volpProt.SIP.musicOnHold.uri</b>

### Local System User Interface

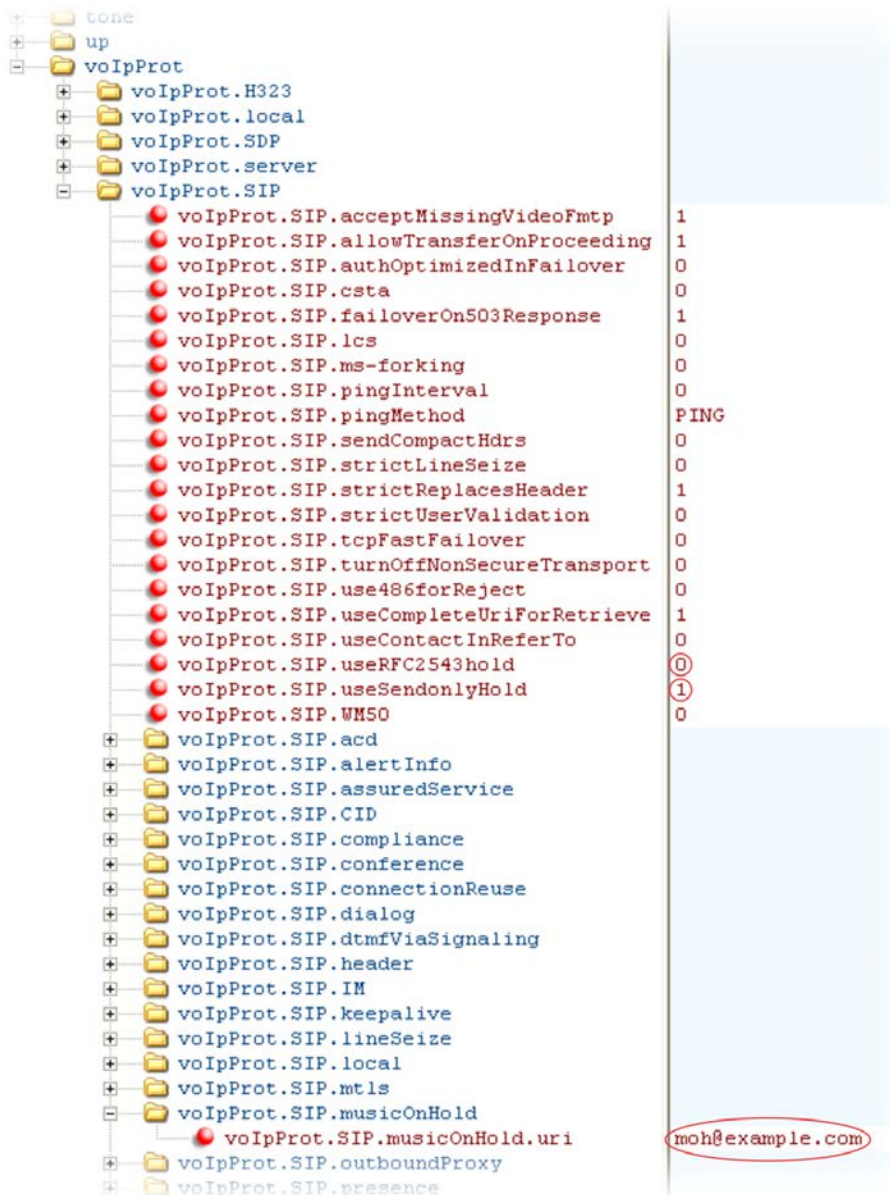
Navigate to **Settings > Advanced > Administration Settings > SIP Server Configuration** to specify whether or not to use RFC 2543 (c=0.0.0.0) outgoing hold signaling. The alternative is RFC 3264 (a=sendonly or a=inactive).

## Example Call Hold Configuration

The following two illustrations show a sample configuration for the call hold feature. Both illustrations are taken from the **sip-interop.cfg** template. In the first illustration, the three `localReminder.*` parameters have been configured to play a tone to remind you of a party on hold, that the tone will begin to play 45 seconds after you put a party on hold, and that the tone will repeat every 30 seconds.

Parameter	Value
call.dialtoneTimeOut	60
call.directedCallPickupMethod	
call.directedCallPickupString	*97
call.enableOnNotRegistered	1
call.lastCallReturnString	*69
call.localConferenceCallHold	0
call.localConferenceEnabled	1
call.offeringTimeOut	60
call.parkedCallRetrieveMethod	
call.parkedCallRetrieveString	
call.rejectBusyOnDnd	1
call.ringBackTimeOut	60
call.singleKeyPressConference	0
call.sticky&AutoLineSeize	0
call.urlModeDialing	0
call.advancedMissedCalls	
call.autoRouting	
call.callWaiting	
call.clickToDial	
call.hold	
call.hold.localReminder	
call.hold.localReminder.enabled	1
call.hold.localReminder.period	30
call.hold.localReminder.startDelay	45
call.hold.remoteNotification	
call.shared	

In the second illustration, the `musicOnHold.uri` parameter has been configured so the party on hold will hear music played from SIP URI `moh@example.com`.



## Use Call Transfer

The Call Transfer feature enables you to transfer an existing active call to a third-party address using a Transfer soft key. For example, if party A is in an active call with party B, party A can transfer party B to party C (the third party). In this case, party B and party C will begin a new call and party A will disconnect. The table [Use Call Transfer](#) shows you how to specify call transfer behavior.

You can perform two types of call transfers:

- **Blind Transfer** Party A transfers the call without speaking to party C.
- **Consultative Transfer** Party A speaks to party C before party A transfers the call.

By default, a Transfer soft key will display when party A calls Party C and Party C's system is ringing, the proceeding state. In this case, party A has the option to complete the transfer before party C answers, which ends party A's connection to party B and C. You can disable this option so that the Transfer soft key does not display during the proceeding state. In this case, party A can either wait until party C answers or press the Cancel soft key and return to the original call.

### Use Call Transfer

#### Central Provisioning Server

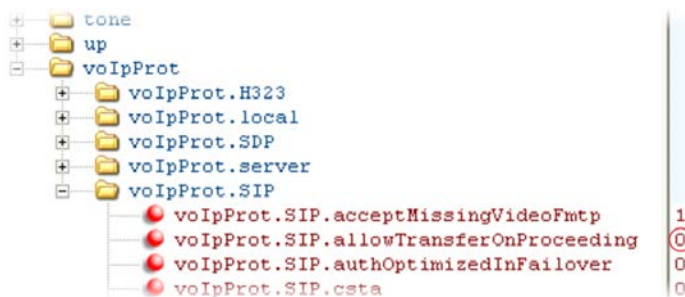
template > parameter

Specify whether to allow transfers while calls are in a proceeding state

sip-interop.cfg > voIpProt.SIP.allowTransferOnProceeding

## Example Call Transfer Configuration

In the following example configuration, the parameter `allowTransferOnProceeding` has been disabled so that the Transfer soft key will not display while the third-party system is ringing, the proceeding state. Once you have connected to the third-party, the Transfer soft key will display. If the third-party does not answer, you can press the Cancel soft key to return to the active call.



## Create Local and Centralized Conferences

You can set up local or centralized conferences. Local conferences require a host system, which processes the audio of all parties. All systems support three-party local conferencing. Alternatively, you can use an external audio bridge, available via a central server, to create a centralized conference call. Polycom recommends using centralized conferencing to host four-party conferences, though some systems do enable to host four-party conferences locally.

See the parameters in the table [Create Local and Centralized Conferences](#) to set up a conference type and the options available for each type of conference. You can specify whether, when the host of a three-party local conference leaves the conference, the other two parties remain connected or disconnected. If you want the other two parties remain connected, the system will perform a transfer to keep the remaining parties connected. If the host of four-party local conference leaves the conference, all parties are disconnected and the conference call ends. If the host of a centralized conference leaves the conference, each remaining party remains connected. For more ways to manage conference calls, see [Enable Conference Management](#).

---

## Create Local and Centralized Conferences

---

**Central Provisioning Server****template** > [parameter](#)

Specify whether, during a conference call, the host can place all parties or only the host on hold

**sip-interop.cfg** > [call.localConferenceCallHold](#)

Specify whether or not the remaining parties can communicate after the conference host exits the conference

**sip-interop.cfg** > [call.transferOnConferenceEnd](#)

Specify whether or not all parties hear sound effects while setting up a conference

**sip-interop.cfg** > [call.singleKeyPressConference](#)

Specify which type of conference to establish and the address of the centralized conference resource

**sip-interop.cfg** > [volpProt.SIP.conference.address](#)


---

## Enable Conference Management

This feature enables you to add, hold, mute, and remove conference participants, as well as obtain additional information about participants. Use the parameters listed in the following table to configure how you want to manage conferences.

**Manage Conferences****Central Provisioning Server****template** > [parameter](#)

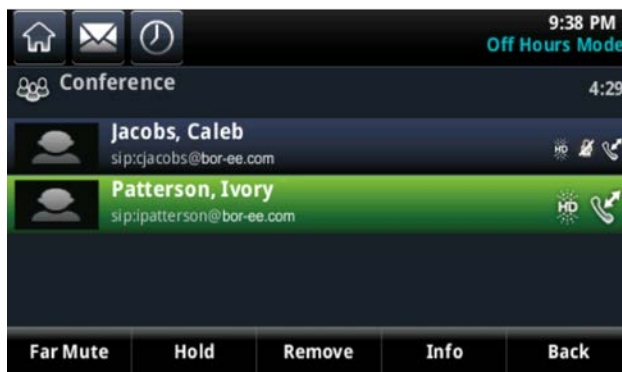
Enable or disable the conference management feature.

**features.cfg** > [feature.nWayConference.enabled](#)


---

## Example Conference Management Configuration

When you enable conference management, a **Manage** soft key will display on the system during a conference. When you press the **Manage** soft key, the **Manage Conference** screen, shown next, will display with soft keys you can use to manage conference participants.





# Configure Call Forwarding

The system provides a flexible call forwarding feature that enables you to forward incoming calls to another destination. You can apply call forwarding in the following ways:

- To all calls
- To incoming calls from a specific caller or extension
- When your system is busy
- When Do Not Disturb is enabled
- When the system has been ringing for a specific period of time
- You can have incoming calls forwarded automatically to a predefined destination you choose or you can manually forward calls to a destination.

You will find parameters for all of these options in the table [Configure Call Forwarding](#).

To enable server-based call forwarding, you must enable the feature on both a registered system and on the server and the system is registered. If you enable server-based call forwarding on one registration, other registrations will not be affected. Server-based call forwarding disables local Call Forward and DND features.



### Troubleshooting: Call Forwarding Does Not Work on My System

The server-based and local call forwarding features do not work with the Shared Call Appearance (SCA) and Bridged Line Appearance (BLA) features. If you have SCA or BLA enabled on your system, disable the feature before you can use call forwarding.

The call server uses the Diversion field with a SIP header to inform the system of a call's history. For example, when you enable call forwarding, the Diversion header allows the receiving system to indicate who the call was from, and the system number it was forwarded from.

## Configure Call Forwarding

Central Provisioning Server	template > parameter
Enable or disable server-based call forwarding	<b>sip-interop.cfg</b> > <a href="#">volpProt.SIP.serverFeatureControl.cf</a>
Enable or disable local call forwarding behavior when server-based call forwarding is enabled	<b>sip-interop.cfg</b> > <a href="#">volpProt.SIP.serverFeatureControl.localProcessing.cf</a>
Enable or disable the display of the Diversion header and the order in which to display the caller ID and number	<b>sip-interop.cfg</b> > <a href="#">volpProt.SIP.header.diversion.*</a>
Set all call diversion settings including a global forward-to contact and individual settings for call forward all, call forward busy, call forward no-answer, and call forward do-not-disturb	<b>site.cfg</b> > <a href="#">divert.*</a>
Enable or disable server-based call forwarding as a per-registration feature	<b>reg-advanced.cfg</b> > <a href="#">reg.x.fwd.*</a>

---

### Web Configuration Utility

To set all call diversion settings navigate to **Settings > Lines**, select a line from the left pane, and expand the **Call Diversion** menu.

---

### Local System User Interface

To enable and set call forwarding from the system, navigate to **Settings > Features > Forward**.

---

## ***Example Call Forwarding Configuration***

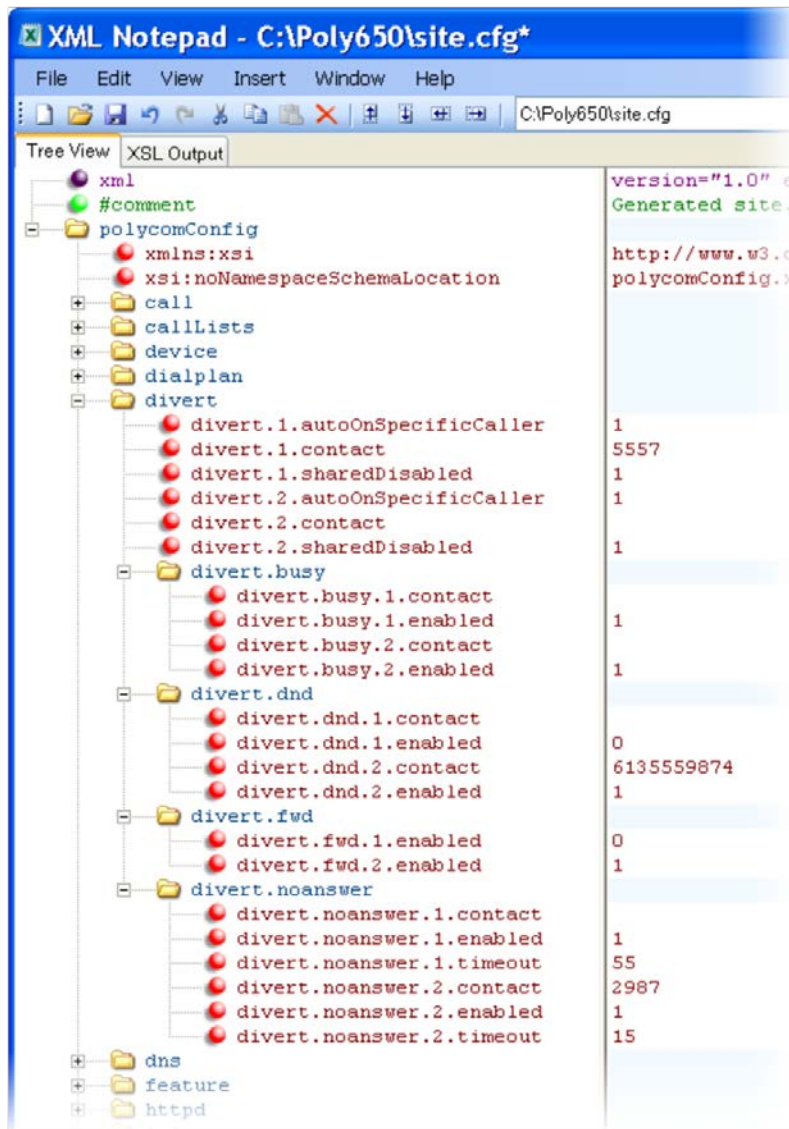
In the example configuration shown next, the call forwarding parameters for registration 1 have been changed from the default values. The forward-always contact for registration 1 is 5557 and this number will be used if the parameters `divert.busy`, `divert.dnd`, or `divert.noanswer` are not set. Parameters you set in those fields will override `divert.1.contact`.

To enable these three divert options for each registration, enable the `divert.fwd.x.enabled` parameter and the `.enabled` parameter for each of the three forwarding options you want to enable.

In this example, `divert.fwd.1.enabled` has been disabled; all calls to registration 1 will be diverted to 5557 and you do not have the option of enabling any of the three forwarding options on the system. The three divert options are enabled for registration 2 in the `divert.fwd.2.enabled` parameter, giving you the option to enable or disable any one of the three forwarding options on the system.



When do not disturb (DND) is turned on, you can set calls to registration 2 to be diverted to 6135559874 instead of 5557. The parameter `divert.noanswer.2.enabled` is enabled so that, on the system, you can set calls to registration 2 that ring for more than 15 seconds, specified in `divert.noanswer.2.timeout`, to be diverted to 2987, as set in `divert.noanswer.2.contact`.



## Configure Lync Call Forwarding

The following types of call forwarding are available on Lync-enabled Polycom systems:

- Disable Call Forwarding
- Forward to a contact
- Forward to voicemail

No parameters are needed to enable call forwarding on Lync-enabled systems.

## Configure Directed Call Pick-Up

This feature enables you to pick up incoming calls to another system by dialing the extension of that system. This feature requires support from a SIP server and setup of this feature depends on the SIP server. For example, while some SIP servers implement directed call pick-up using a star-code sequence, others implement the feature using network signaling. The table [Configure Directed Call Pickup](#) lists the configuration parameters for the directed call pick-up feature.

### Configure Directed Call Pickup

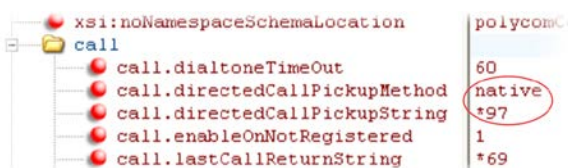
<b>Central Provisioning Server</b>	<b>template</b> > <a href="#">parameter</a>
Turn this feature on or off	<b>features.cfg</b> > <a href="#">feature.directedCallPickup.enabled</a>
Specify the star code to initiate a directed call pickup	<b>sip-interop.cfg</b> > <a href="#">call.directedCallPickupString</a>

## Example Directed Call Pickup Configuration

The configuration parameters for the directed call pickup feature are located in two template files. You enable directed call pickup in the **features.cfg** template file and configure the feature using the **sip-interop.cfg** file.

In the following configuration example, the directed call pickup feature has been enabled in the **features.cfg** template file:

Once directed call pickup is enabled, you can configure the feature using parameters located in the **sip-interop.cfg** template file. In the following illustration, the pickup method has been set to `native`, which means that the server is used for directed call pickup instead of the `PickupString`. If the pickup method was set to `legacy`, the pickup string `*97` would be used by default. The pickup string can be different for different call servers, check with your call server provider if you configure legacy mode directed call pickup.



When you enable directed call pickup, the system displays a **Pickup** soft key when you go off-hook. When you press the **Pickup** soft key, the **Directd** soft key will display.

## Enable Group Call Pickup

This feature enables you to pick up incoming calls to any system within a predefined group of systems, without dialing the extension of another system. The parameter to enable this feature is shown in the table [Enable Group Call Pickup](#). This feature requires support from a SIP server and setup of this feature depends on the SIP server. For example, while some SIP servers implement group call pick-up using a particular star-code sequence, others implement the feature using network signaling.

---

## Enable Group Call Pickup

---

<b>Central Provisioning Server</b>	<b>template</b> > <a href="#">parameter</a>
Turn this feature on or off	<b>features.cfg</b> > <a href="#">feature.groupCallPickup.enabled</a>

---

When you enable the group call pickup, the system will display a **Pickup** soft key when you go off-hook. If you select **Pickup**, the **Group** soft key is displayed.

After you press the **Group** soft key, the system performs a just-in-time subscription request to the fixed address `<groupcallpickup@<yourCallServerDomain>` for dialog details with which it can pick up the original caller using a replaces header in a new INVITE.

## Configure Call Park and Retrieve

This feature is available as Open SIP. If you want to use the Call Park feature available with Lync Server, see [Feature Profile 84538](#). You can park an active call and retrieve parked calls from any system. Whereas call hold keeps the held call on the same line, Call Park moves the call to a separate address where the call can be retrieved by any system. This feature requires support from a SIP server and setup of this feature depends on the SIP server. For example, while some SIP servers implement group call pick-up using a particular star-code sequence, others implement the feature using network signaling. See the table [Configure Call Park and Retrieve](#) for parameters you can configure.

### Configure Call Park and Retrieve for Open SIP

---

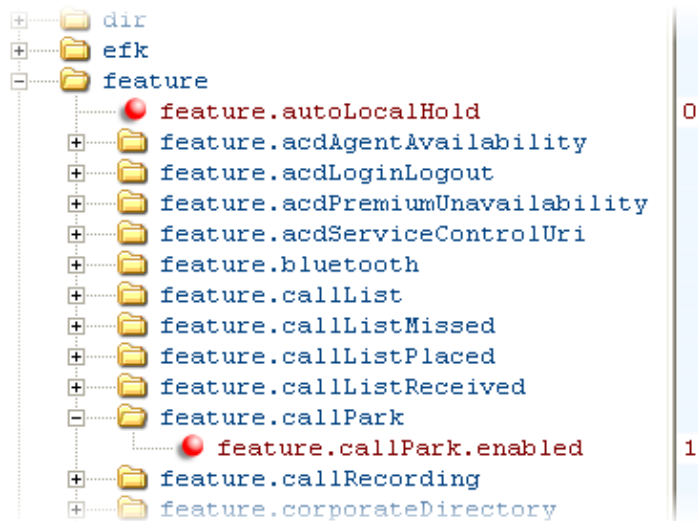
<b>Central Provisioning Server</b>	<b>template</b> > <a href="#">parameter</a>
Enable or disable call park and retrieve	<b>features.cfg</b> > <a href="#">feature.callPark.enabled</a>
Specify the star code used to retrieve a parked call	<b>sip-interop.cfg</b> > <a href="#">call.parkedCallRetrieveString</a>

---

## Example Call Park and Retrieve Configuration

The configuration parameters for the call park and retrieve feature are located in two template files. You can enable the feature using the **features.cfg** template file and configure the feature using the **sip-interop.cfg** file.

In the following configuration example, the call park feature has been enabled in the **features.cfg** template file.



You can configure the call park and call retrieve feature using parameters located in the **sip-interop.cfg** template file. The following illustration shows that the parked call retrieve method has been set to native, meaning that the system will use SIP INVITE with the Replaces header. The method can also be set to legacy, meaning that the system will use the call.parkedCallRetrieveString star code to retrieve the parked call.



When the call park and retrieve feature is enabled, the **Park** soft key displays when you are in a connected call. To park the call, press the **Park** soft key.

To retrieve a parked call, go off-hook and press the **Retrieve** soft key, or tap **New Call** soft key, enter the call orbit number, and tap **Call**.

## Enable Last Call Return

The system supports redialing of the last received call. The table [Enable Last Call Return](#) shows you the parameters to enable this feature. This feature requires support from a SIP server. With many SIP servers, this feature is implemented using a particular star code sequence. With some SIP servers, specific network signaling is used to implement this feature.

## Enable Last Call Return

### Central Provisioning Server

template > parameter

Enable or disable last call return

features.cfg > feature.lastCallReturn.enabled

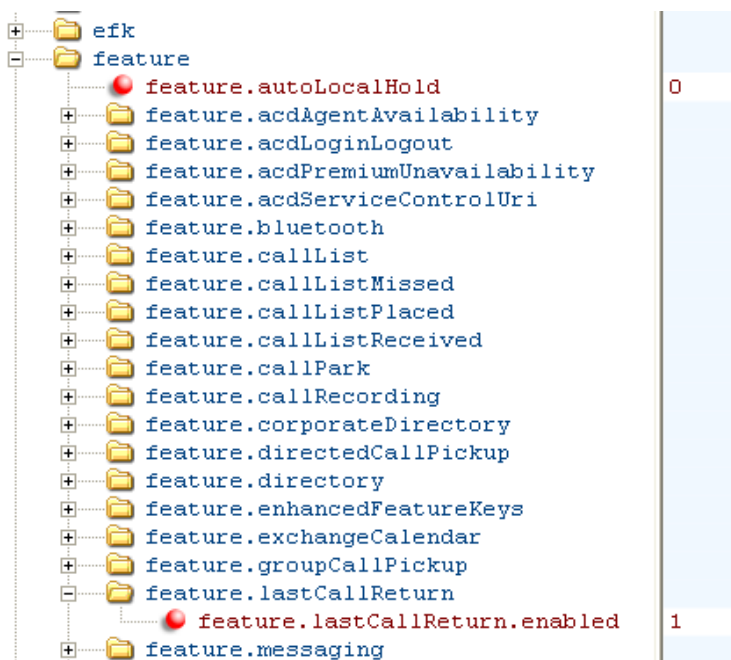
Specify the string sent to the server for last-call-return

sip-interop.cfg > call.lastCallReturnString

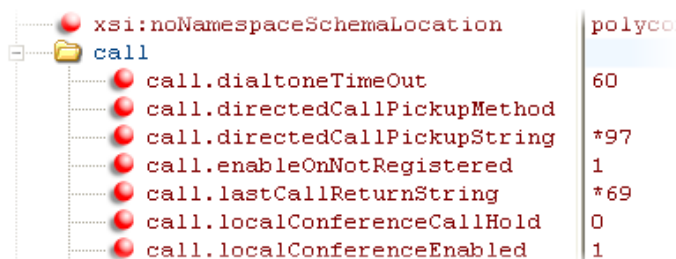
## Example Configuration for Last Call Return

The configuration parameters for last call return feature are located in two template files. You can enable the feature using the **features.cfg** template file and configure the feature using the **sip-interop.cfg** file.

In the following configuration example, the last call return feature has been enabled in the **features.cfg** template file:



Once last call return is enabled, you can configure the feature using parameters located in the **sip-interop.cfg** template file. The following shows the default value for the `call.lastCallReturnString` parameter. The last call return string value depends on the call server you use. Consult with your call server provider for the last call return string.



---

When you enable the last call return feature, the system displays an **LCR** soft key when it goes off-hook, as shown next. When you press the **LCR** soft key, you place a call to the system address that last called you.

When you select **Last Call Return**, you place a call to the system address that last called you.

# Set Up Advanced System Features

---

After you set up your Polycom systems with a default configuration on the network, system users will be able to place and receive calls; however, you may want to make some changes to optimize your configuration for your organization and user's needs. Polycom provides basic and advanced features that you can configure for the systems. This section will show you how to configure all available advanced system features, call server features, and Polycom and third-party applications.

This section shows you how to make configuration changes for the following advanced features:

- [Assign Multiple Line Keys Per Registration](#) Assign multiple line keys to a single registration.
- [Enable Multiple Call Appearances](#) All systems support multiple concurrent calls. You can place any active call on hold to switch to another call.
- [Set the System Language](#) All systems have multilingual user interfaces.
- [Synthesized Call Progress Tones](#) Match the system's call progress tones to a region.
- [Configure Real-Time Transport Protocol Ports](#) System treat all real time transport protocol (RTP) streams as bi-directional from a control perspective, and expect that both RTP endpoints will negotiate the respective destination IP addresses and ports.
- [Configure Network Address Translation](#) Systems can work with certain types of network address translation (NAT).
- [Use the Corporate Directory](#) You can configure the system to access your corporate directory if it has a standard LDAP interface. This feature is part of the Productivity Suite. Active Directory, OpenLDAP, Microsoft ADAM, and SunLDAP are currently supported.
- [Configure Enhanced Feature Keys](#) Enables you to redefine soft keys to suit your needs. In SIP 3.0, this feature required a license key. In later releases, no license key is required.
- [Configure Soft Keys](#) Enables you to create your own soft keys, and display them with or without the standard soft keys.
- [Capture Wireshark Trace to USB flash drive](#) You can capture the Wireshark trace to a USB flash drive.
- [Capture Wireshark Trace to USB flash drive using Telnet](#) You can capture the Wireshark trace to a USB flash drive using Telnet.
- [Enable the Power Saving Feature](#) Enable and set hours for the power-saving feature.
- [Configure Group Paging](#) Send one-way page broadcasts.
- [Enable Bridged Line Appearance](#) Allows a line extension or system number to appear on multiple users' systems. This feature requires call server support.
- [Enable Voicemail Integration](#) Enables access to compatible voice mail servers.
- [Enable Multiple Registrations](#) The CX5500 system supports multiple registrations.
- [Set Up Server Redundancy](#) Systems support server redundancy to ensure the continuity of system service when the call server is offline for maintenance, fails, or the connection between the system and server fails.
- [DNS SIP Server Name Resolution](#) Enter the DNS name for a proxy/registrar address.
- [Use the Presence Feature](#) Enables you to monitor the status of other users/devices, and for other users/devices to monitor you. This feature requires call server support.

- [Configure the Static DNS Cache](#) Set up a cache for DNS information and provide for negative caching.
- [Display SIP Header Warnings](#) Displays a pop-up warning message to the users from a SIP header message.
- [Quick Setup of the CX5500 System](#) Provides a simplified interface to enter provisioning server parameters while your system boots.
- [Provisional Polling of the CX5500 System](#) You can set the systems to automatically check for software downloads using a random schedule or through a predefined schedule.
- [Set Up Microsoft Lync Server 2010 and 2013](#) You can use the CX5500 with Microsoft Lync Server 2010 to immediately share ideas and information with business contacts. This feature requires call server support.
- [Enable Microsoft Exchange Calendar Integration](#) Enables users to manage meetings and reminders with your CX5500 system, and enables you to dial in to conference calls. This feature requires Microsoft Exchange Calendar Integration.

## Assign Multiple Line Keys per Registration

You can assign a single registered system line address to multiple line keys on the CX5500 system. See the table [Multiple Line Keys Per Registration](#) for the parameter you need to set. This feature can be useful for managing a high volume of calls to a line. This feature is one of several features associated with *Flexible Call Appearances*. See the following table for the maximum number of line keys per registration for each system model, and for definitions of all features associated with Flexible Call Appearances.

### Multiple Line Keys Per Registration

#### Central Provisioning Server

[template](#) > [parameter](#)

Specify the number of line keys to use for a single registration

[reg-advanced.cfg](#) > [reg.x.lineKeys](#)

#### Web Configuration Utility

To assign the number of line keys per registration, navigate **Settings > Lines**, select the number of lines from the left pane, expand **Identification**, and edit Number of **Line Keys**

#### Local System User Interface

Assign the number of line keys per registration by navigating to **Settings > Advanced > Admin Settings > Line Configuration > Line x > Line Keys > Num Line Keys**.

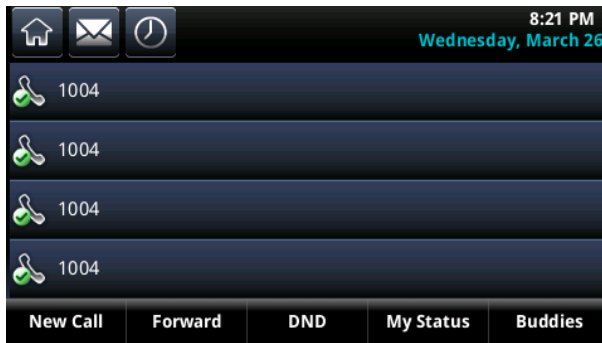


## Example Configuration

The following illustration shows you how to enable four line keys with the same registered line address. In this example, four line keys are configured with registration address *1004*.



The system displays the registered line address *1004* on four line keys, as shown next.



## Enable Multiple Call Appearances

You can enable each registered CX5500 system line to support multiple concurrent calls and have each concurrent call display on the system’s user interface. For example, you can place one call on hold, switch to another call on the same registered line, and have both calls display. As shown in the table [Enable Multiple Call Appearances](#), you can set the maximum number of concurrent calls per registered line and the default number of calls per line key.

This feature is one of several features associated with *Flexible Call Appearances*. If you want to enable multiple line keys per registration, see [Assign Multiple Line Keys Per Registration](#). Note that if you assign a registered line to multiple line keys, the default number of concurrent calls will apply to all line keys. See the following table if you want use multiple registrations on a system, and for definitions of all features associated with Flexible Call Appearances. Use this table to customize the number of registrations, line keys per registration, and concurrent calls.

### Enable Multiple Call Appearances

#### Central Provisioning Server

template > parameter

Set the default number of concurrent calls for all line keys

reg-basic.cfg > call.callsPerLineKey

Override the default number of calls per line key for a specific line

reg-advanced.cfg > reg.x.callsPerLineKey

#### Web Configuration Utility

To set the default number of concurrent calls a line key, navigate to **Settings > SIP**, expand **Local Settings**, and edit **Calls Per Line Key**.

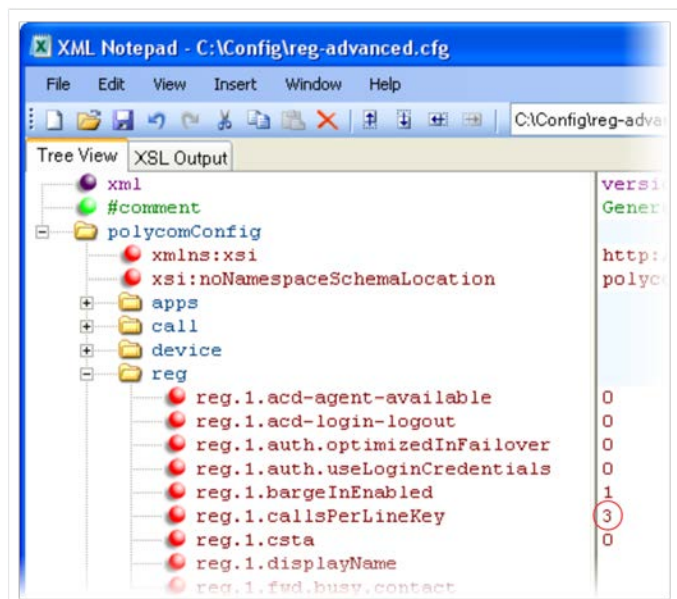
To override the number of concurrent calls for a specific line, navigate to **Settings > Lines**, select the line to modify from the left pane, expand **Identification**, and edit **Calls Per Line**.

#### Local System User Interface

Assign the default number of concurrent calls per line by navigating to **Settings > Advanced > Admin Settings > Line Configuration > Calls Per Line Key** (navigate to **Line Configuration > Line X > Line Keys > Calls Per Line Key** to change the calls per line for only line x).

## Example Multiple Call Appearances Configuration

The following illustration shows that in the **reg-advanced.cfg** template you can enable line 1 on your system with three call appearances.



Once you have set the `reg.1.callsPerLineKey` parameter to 3, you can have three call appearances on line 1. By default, additional incoming calls will be automatically forwarded to your voicemail. If you have more than two call appearances, a call appearance counter displays at the top-right corner of your system's screen.

The following table describes the features associated with Flexible Call Appearances. Use the table to

understand how you can organize registrations, line keys per registration, and concurrent calls per line key.

### Flexible Call Appearances Features

<i>Feature</i>	<i>Description</i>	<i>Limit</i>
Registrations	Maximum number of user registrations	16
Line Keys	Maximum number of line keys	16
Line Keys per Registration	Maximum number of line keys per user registration	16
Calls per Line Key	Maximum number of concurrent calls per line key	24
Concurrent Calls, including Conference Legs *	Runtime maximum number of concurrent calls (Number of conference participants minus the moderator)	24 (2)

\* Note that each conference leg counts as one call. The total number of concurrent calls in a conference indicated in this table includes all conference participants *minus* the moderator.

## Set the System Language

You can select the language that displays on the system using the parameters in the following table. Each language is stored as a language file in the **SoundPointIPLocalization** folder. This folder is included with the Polycom UC Software you downloaded to your provisioning server. If you want to edit the language files, use a Unicode-compatible XML editor such as XML Notepad 2007 and familiarize yourself with the guidelines on basic and extended character support, see [<ml/>](#).

The Polycom systems support major western European languages. The CX5500 system supports the following languages: Simplified Chinese, Traditional Chinese, Danish, Dutch, English, French, German, Italian, Japanese, Korean, Norwegian, Polish, Brazilian Portuguese, Russian, Slovenian, International Spanish, and Swedish.

### Set the System Language

<b>Central Provisioning Server</b>	<b>template &gt; parameter</b>
Obtain the parameter value for the language you want to display on the system	<b>site.cfg &gt; lcl.ml.lang.menu.*</b>
Specify the language used on the system's display screen	<b>site.cfg &gt; lcl.ml.lang</b>

### Web Configuration Utility

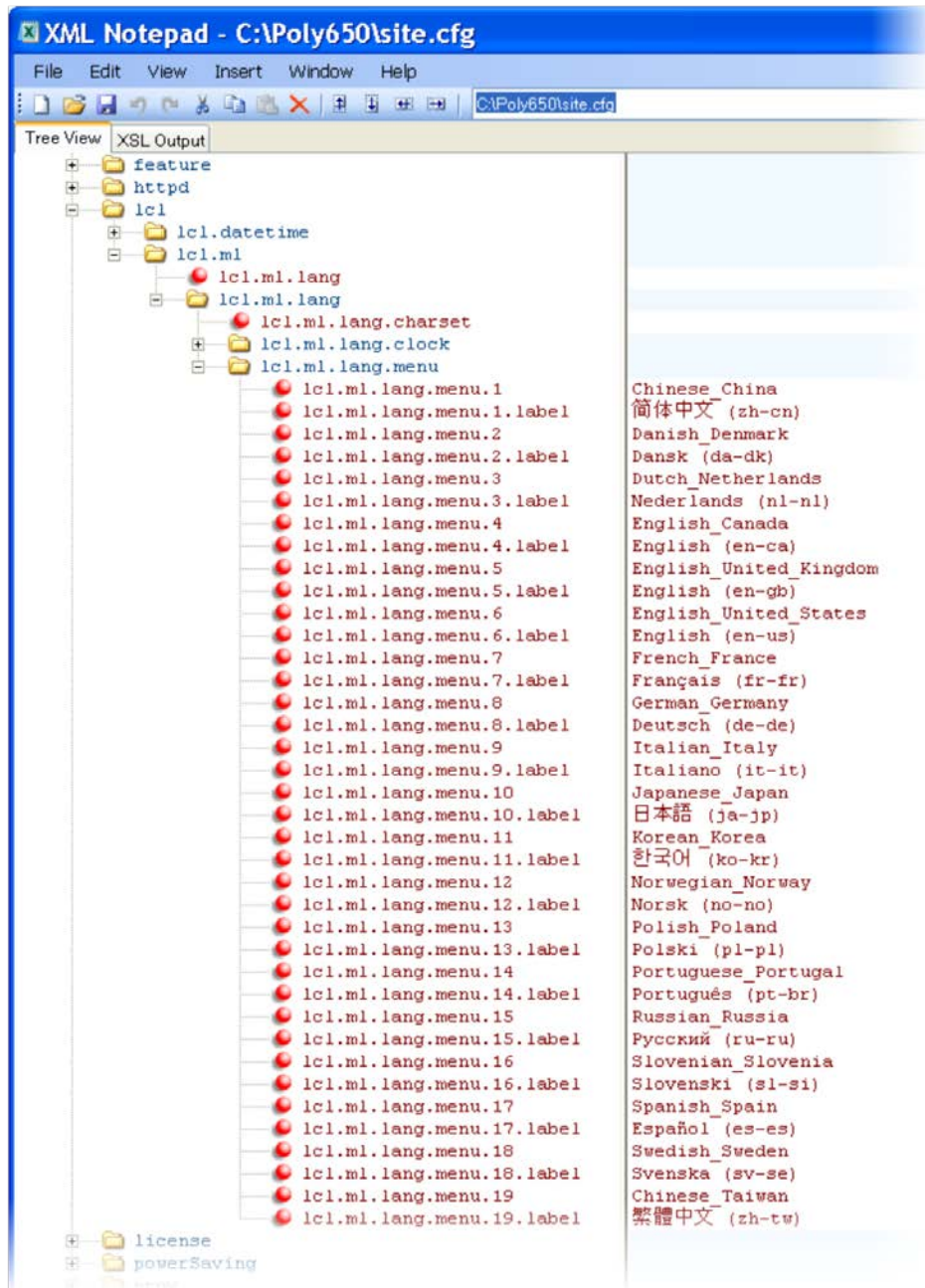
To change the language of the system's display screen, navigate to **Preferences > Additional Preferences**, change **System Language**, and click **Add > Save**.

### Local System User Interface

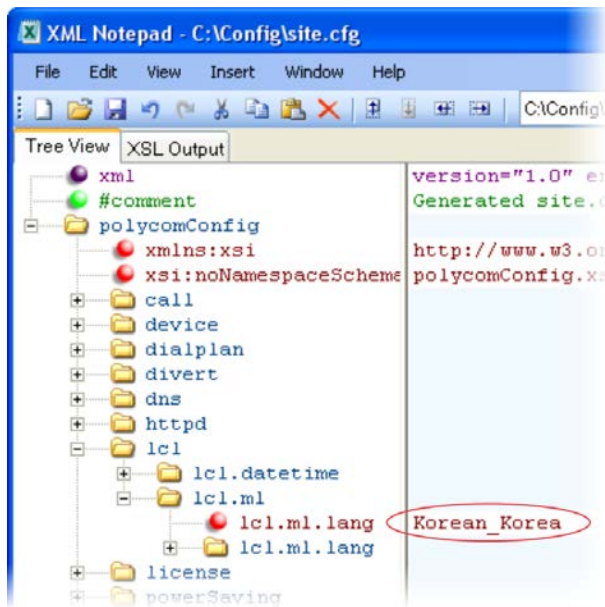
To change the language of the system's display screen, navigate to **Settings > Basic > Preferences > Language**.

## Example System Language Configuration

The following illustration shows you how to change the system language. Locate the language you want the system to display in the site.cfg template in `lcl.ml.lang.*` menu.



From the list, select the language you want to use and enter it in `lcl.ml.lang`. In the following example, the system is set to use the Korean language.



Once configured, the system uses Korean characters, as shown next.



## Synthesized Call Progress Tones

The CX5500 system plays call signals and alerts, called call progress tones, such as busy signals, ringback sounds, and call waiting tones. The built-in call progress tones on your system match standard North American tones. If you would like to customize the system's call progress tones to match the standard tones in your region, contact [Polycom Support](#).

## Configure Real-Time Transport Protocol Ports

You can configure the system to filter incoming RTP packets. You can filter the packets by IP address, or by port. For greater security, you can also configure RTP settings to reject packets arriving from a non-negotiated IP address or from an unauthorized source. You can reject packets that the system receives from a non-negotiated IP address or a non-negotiated port.

You can configure the system to enforce symmetric port operation for RTP packets. When the source port is not set to the negotiated remote sink port, arriving packets can be rejected.

You can also fix the system's destination transport port to a specified value regardless of the negotiated port. This can be useful for communicating through firewalls. When you use a fixed transport port, all RTP traffic is sent to and arrives on that specified port. Incoming packets are sorted by the source IP address and port, which allows multiple RTP streams to be multiplexed.

You can specify the system's RTP port range. Since the system supports conferencing and multiple RTP streams, the system can use several ports concurrently. Consistent with RFC 1889, the next-highest odd-numbered port is used to send and receive RTP. The table [Configure Real-Time Transport Protocol](#) provides a link to the reference section.

The system is compatible with RFC 1889 - RTP: A Transport Protocol for Real-Time Applications - and the updated RFCs 3550 and 3551. Consistent with RFC 1889, the system treats all RTP streams as bi-directional from a control perspective and expects that both RTP endpoints will negotiate the respective destination IP addresses and ports. This allows real-time transport control protocol (RTCP) to operate correctly even with RTP media flowing in only a single direction, or not at all.

### Configure Real-Time Transport Protocol Ports

---

#### Central Provisioning Server

	<b>template</b> > <a href="#">parameter</a>
Filter RTP packets by port	<b>site.cfg</b> > <a href="#">tcplpApp.port.rtp.filterByPort</a>
Force-send packets on a specified port	<b>site.cfg</b> > <a href="#">tcplpApp.port.rtp.forceSend</a>
Set the starting port for RTP packet port range	<b>site.cfg</b> > <a href="#">tcplpApp.port.rtp.mediaPortRangeStart</a>

---

#### Web Configuration Utility

Filter RTP packets by IP address, by port, force-send packets on a specified port, and set the port range start by navigating to **Settings > Network > RTP**.

---



## Example Real-Time Transport Protocol Configuration

The following illustration shows the default real-time transport protocol settings in the **site.cfg** template file. The parameter `tcpIpApp.port.rtp.filterByIp` is set to 1 so that the system will reject RTP packets sent from non-negotiated IP addresses. The parameter `tcpIpApp.port.rtp.filterByPort` is set to 0 so that RTP packets sent from non-negotiated ports will not be rejected. Enter a value in the `tcpIpApp.port.rtp.forceSend` parameter to specify the port that all RTP packets will be sent to and received from. The parameter `tcpIpApp.port.rtp.mediaPortRangeStart` shows the default starting port 2222 for RTP packets. The starting port must be entered as an even integer.



## Configure Network Address Translation

The system can work with certain types of Network Address Translation (NAT). NAT enables a local area network (LAN) to use one set of IP addresses for internal traffic and another set for external traffic. The system’s signaling and Real-Time Transport Protocol (RTP) traffic use symmetric ports. You can configure the external IP address and ports used by the NAT on the system’s behalf on a per-system basis. The table [Network Access Translation](#) lists each of the parameters you can configure. Note that the source port in transmitted packets is the same as the associated listening port used to receive packets.

### Network Access Translation

Central Provisioning Server	template > parameter
Specify the external NAT IP address	<b>sip-interop.cfg</b> > <a href="#">nat.ip</a>
Specify the external NAT keepalive interval	<b>sip-interop.cfg</b> > <a href="#">nat.keepalive.interval</a>
Specify the external NAT media port start	<b>sip-interop.cfg</b> > <a href="#">nat.mediaPortStart</a>
Specify the external NAT signaling port	<b>sip-interop.cfg</b> > <a href="#">nat.signalPort</a>

### Web Configuration Utility

Specify the external NAT IP address, the signaling port, the media port start, and the keepalive interval by navigating to **Settings > Network > NAT**.

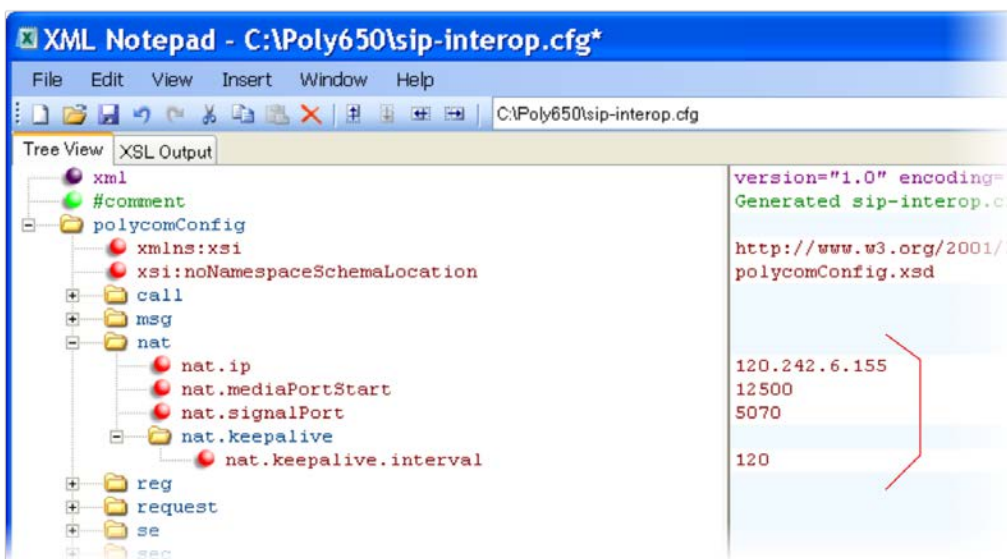
## Example Network Address Translation Configuration

The following illustration shows the default NAT parameter settings. The parameter `nat.ip` is the public IP that you want to advertise in SIP signaling. The default IP is 120.242.6.155.

The parameter `nat.mediaPortStart` is the RTP used to send media. If non-Null, this attribute will set the initially allocated RTP port and will override the value set in `tcpIpApp.port.rtp.mediaPortRangeStart`. In the example, the starting port is 12500 and the system will cycle through `start-port + 47` for systems that support audio only or `start-port + 95` for systems that support video.

The parameter `nat.signalPort` specifies the port that the system will use for SIP signaling. This parameter will override `voIpProt.local.Port`. In the example below, the system will use port 5070 for SIP traffic.

Use the `nat.keepalive.interval` to specify the keepalive interval in seconds. This parameter sets the interval at which systems will send a keepalive packet to the gateway/NAT device. The keepalive packet keeps the communication port open so that NAT can continue to function as initially set up. In the example below, the system will send the keepalive every 120 seconds.



## Use the Corporate Directory

You can connect your system to a corporate directory server that supports the Lightweight Directory Access Protocol (LDAP) version 3. The corporate directory is a flexible feature and table [Use the Corporate Directory](#) links you to the parameters you can configure. Once set up on the systems, the corporate directory can be browsed or searched. You can call numbers and save entries you retrieve from the LDAP server to the local contact directory on the system.

The CX5500 system currently supports the following LDAP servers:

- Microsoft® Active Directory 2003 SP2
- Sun ONE Directory Server 5.2 p6



- Open LDAP Directory Server 2.4.12
- Microsoft Active Directory Application Mode (ADAM) 1.0 SP1

The CX5500 system supports corporate directories that support server-side sorting and those that do not. For systems that do not support server-side sorting, sorting is performed on the system.



**Tip: Better Performance With Server-Side Sorting**

Polycom recommends using corporate directories that have server-side sorting for better performance. Consult your LDAP Administrator when making any configuration changes for the corporate directory. For more information on LDAP attributes, see [RFC 4510 - Lightweight Directory Access Protocol \(LDAP\): Technical Specification Road Map](#).



**Web Info: Supported LDAP Directories**

Configuration of a corporate directory depends on the LDAP server you use. For detailed explanations and examples of all currently supported LDAP directories, see [Technical Bulletin 41137: Best Practices When Using Corporate Directory on Polycom Systems](#).

## Use the Corporate Directory

### Central Provisioning Server

**template** > [parameter](#)

Specify the location of the corporate directory's LDAP server, the LDAP attributes, how often to refresh the local cache from the LDAP server, and other settings

**features.cfg** > [dir.corp.\\*](#)

### Local System User Interface

Specify if the corporate directory should remember the previous search filter by navigating to **Settings > Basic > Preferences > Corporate Directory > View Persistency**.

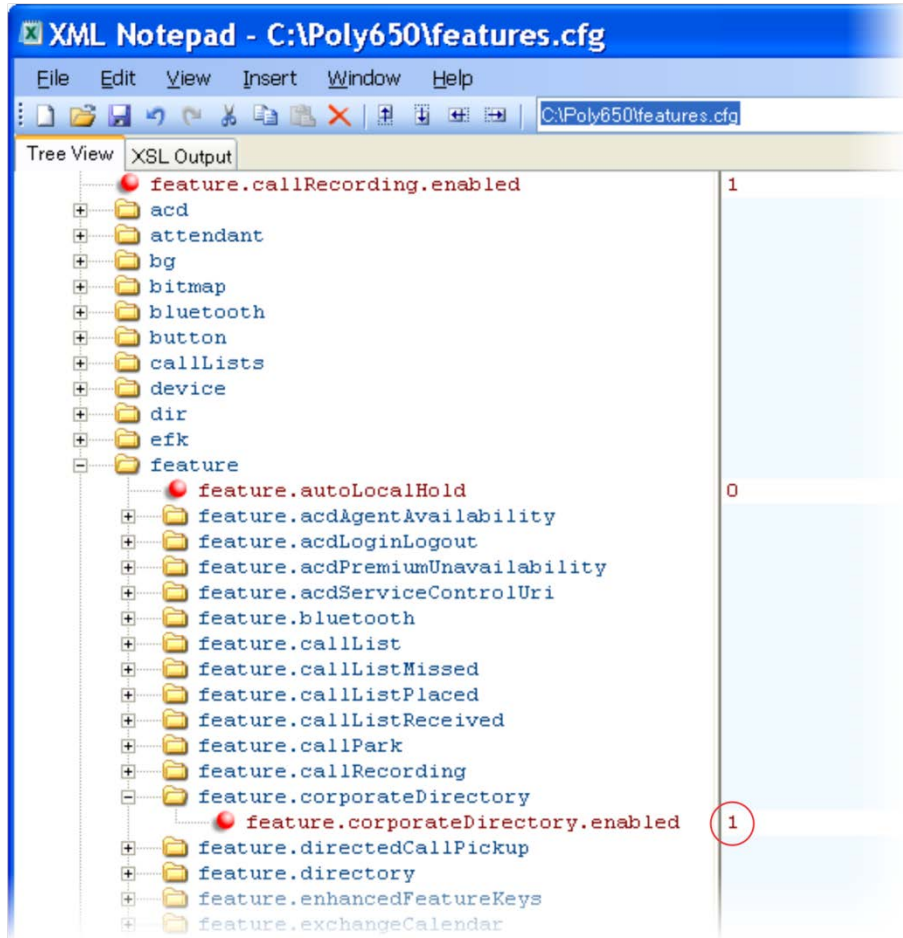
Review the corporate directory LDAP server status by navigating to **Settings > Status > CD Server Status**.

To search your corporate directory, press the **Directories** key on the system, and select **Corporate Directory**.

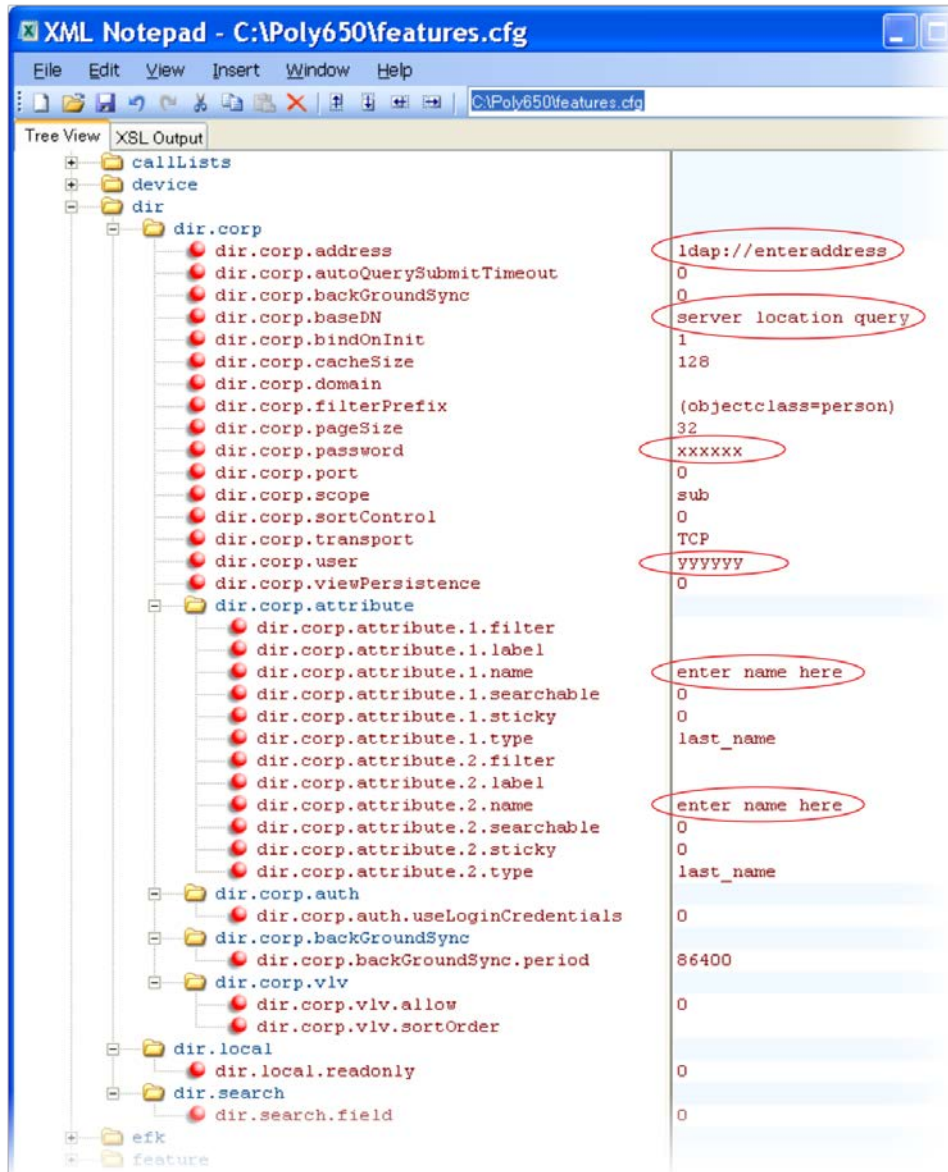
## Example Corporate Directory Configuration

The following example is a representation of the minimum parameters must set to begin using the corporate directory. The exact parameters and values you will need to configure vary with the corporate directory you are using.

First, enable the corporate directory feature in the **features.cfg** template, as shown next.



The following illustration points you to the minimum parameters you need to set. Enter a corporate directory address in `dir.corp.address`, and specify where on the corporate directory server you want to make queries in `dir.corp.baseDN`. In addition, you will require a user name and password. The `dir.corp.attribute.x.name` must match the attributes in the server.



To search the corporate directory, press the **Directories** key on the system and select **Corporate Directory**.

## Configure Enhanced Feature Keys

Enhanced Feature Keys (EFK) enables you to customize the functions of a system's line and soft keys and, as of UC Software 4.0.1, hard keys. You can use EFK to assign frequently used functions to line keys, soft keys, and hard keys or to create menu shortcuts to frequently used system settings.

See the table [Enhanced Feature Keys](#) for the parameters you can configure and a brief explanation of how to use the contact directory to configure line keys. Enhanced feature key functionality is implemented using star code sequences (like \*69) and SIP messaging. Star code sequences that define EFK functions are written as macros that you apply to line and soft keys. The EFK macro language was designed to follow current configuration file standards and to be extensible. The macros are case sensitive.

The rules for configuring EFK for line keys, soft keys, and hard keys are different. Before using EFK, you are advised to become familiar with the macro language shown in this section and in the reference section at <efk/>.



#### Web Info: Using Enhanced Feature Keys

For instructions and details on how to use Enhanced Feature Keys, refer to [Feature Profile 42250: Using Enhanced Feature Keys and Configurable Soft Keys on Polycom Systems](#).

Note that the configuration file changes and the enhanced feature key definitions can be included together in one configuration file. Polycom recommends creating a new configuration file in order to make configuration changes.

### Enhanced Feature Keys

Central Provisioning Server	template > parameter
Specify at least two calls per line key	<b>reg-basic.cfg</b> > <a href="#">reg.x.callsPerLineKey</a>
Enable or disable Enhanced Feature Keys	<b>features.cfg</b> > <a href="#">feature.enhancedFeatureKeys.enabled</a>
Specify the EFK List parameters	<b>features.cfg</b> > <a href="#">efk.efklist.x.*</a>
Specify the EFK Prompts	<b>features.cfg</b> > <a href="#">efk.efkprompt.x.*</a>

Because line keys and their functions are linked to fields in the contact directory file - **000000000000-directory.xml** (global) or **<MACaddress>-directory.xml** (per system) - you must match the contact field (ct) in the directory file to the macro name field (mname) in the configuration file that contains the EFK parameters. When you enter macro names to the contact field (ct) in the directory file, add the '!' prefix to the macro name. For more detailed information on using the contact directory, see [Use the Local Contact Directory](#). The template directory configuration file is named **000000000000-directory~.xml**.

## Some Guidelines for Configuring Enhanced Feature Keys

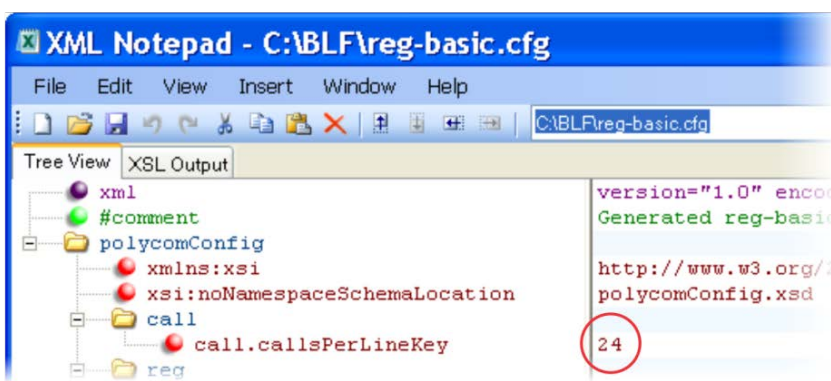
The following guidelines will help you to configure enhanced feature keys (EFKs) efficiently:

- Activation of EFK functions requires valid macro construction.
- All failures are logged at level 4 (minor).
- If two macros have the same name, the first one will be used and the subsequent ones will be ignored.
- A sequence of characters prefixed with "!" are parsed as a macro name. The exception is the speed dial reference, which starts with "!" and contains digits only.

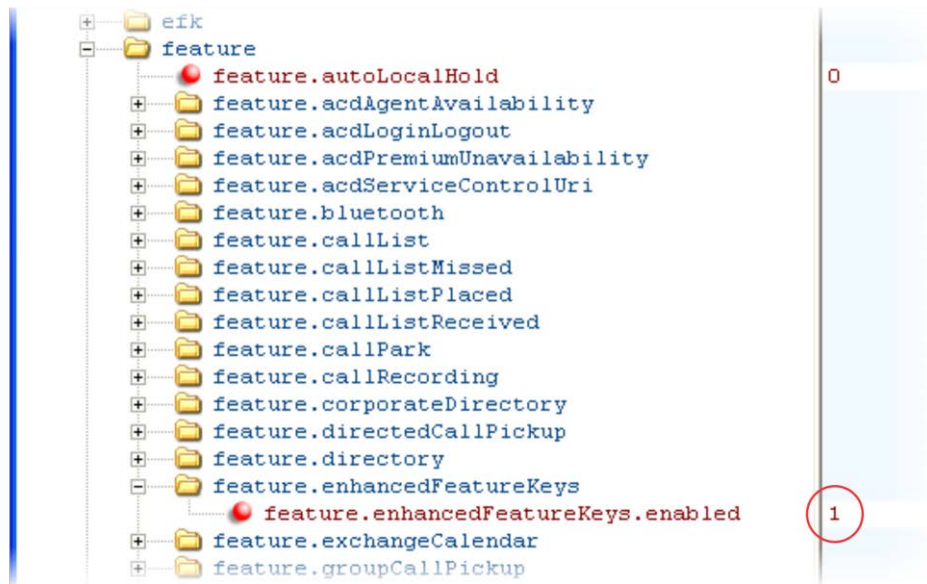
- A sequence of characters prefixed with “^” is the action string.
- “!” and “^” macro prefixes cannot be mixed in the same macro line.
- The sequence of characters must be prefixed by either “!” or “^” so it will be processed as an enhanced feature key. All macro references and action strings added to the local directory contact field must be prefixed by either “!” or “^”.
- Action strings used in soft key definitions do not need to be prefixed by “^”. However, the “!” prefix must be used if macros or speed dials are referenced.
- A sequence of macro names in the same macro is supported (for example, “!m1!m2” ).
- A sequence of speed dial references is supported (for example, “!1!2” ).
- A sequence of macro names and speed dial references is supported (for example, “!m1!2!m2” ).
- Macro names that appear in the local contact directory must follow the format “!<macro name>”, where <macro name> must match an <elklist> mname entry. The maximum macro length is 100 characters.
- A sequence of macros is supported, but cannot be mixed with other action types.
- Action strings that appear in the local contact directory must follow the format “^<action string>”. Action strings can reference other macros or speed dial indexes. Protection against recursive macro calls exists (the enhanced feature keys fails once you reach 50 macro substitutions).

## Enhanced Feature Key Examples

The following illustration shows the default value 24 calls per line key. Ensure that you specify at least two calls per line key.



Enable the enhanced feature keys feature in the **features.cfg** template file, as shown next.



In the following illustration, the EFK parameters are located in the **features.cfg** template file. In the `efk.efklist.x.*` parameters, line key 1 has been assigned a Call Park address (1955) and line key 2 a Call Retrieve function. The parameter `acton.string` shows you the macro definition for these two functions. In addition, `status` is enabled and a label has been specified to display next to the line key. The entry in the `mname` parameter corresponds to the `contact (ct)` field in the contact directory.



In the `efk.prompt.*` parameters, `status` has been enabled. The label on the user prompt has been defined as *Enter Number:* and this prompt will display on the system screen. The `type` parameter has been set to `numeric` to allow only numbers and because `userfeedback` has been specified as `visible`, you will be able to see the numbers you enter into the prompt.

<code>efk.version</code>	2
<code>efk.efklist</code>	
<code>efk.efklist.1.label</code>	Call Park
<code>efk.efklist.1.mname</code>	callpark
<code>efk.efklist.1.status</code>	1
<code>efk.efklist.1.action.string</code>	*681955
<code>efk.efklist.2.label</code>	Call Retrieve
<code>efk.efklist.2.mname</code>	callretrieve
<code>efk.efklist.2.status</code>	1
<code>efk.efklist.2.action.string</code>	*881955
<code>efk.efkprompt</code>	
<code>efk.efkprompt.1.status</code>	1
<code>efk.efkprompt.1.label</code>	Enter Number:
<code>efk.efkprompt.1.userfeedback</code>	visible
<code>efk.efkprompt.1.type</code>	numeric
<code>efk.efkprompt.1.digitmatching</code>	none
<code>efk.efkprompt.2.status</code>	1
<code>efk.efkprompt.2.label</code>	Enter Number:
<code>efk.efkprompt.2.type</code>	numeric
<code>efk.efkprompt.2.userfeedback</code>	visible
<code>efk.efkprompt.2.digitmatching</code>	none

## Understanding Macro Definitions

The `efk.efklist.x.action.string` can be defined by one of the following:

- [Macro Actions](#)
- [Prompt Macro Substitution](#)
- [Expanded Macros](#)

## Macro Actions

The action string is executed in the order it displays. User input is collected before any action is taken. The action string can contain the fields shown in the table [Macro Actions and Descriptions](#).

### Macro Actions and Descriptions

---

#### `$L<label>$`

This is the label for the entire operation. The value can be any string including the null string (in this case, no label displays). This label will be used if no other operation label collection method worked (up to the point where this field is introduced). Make this the first entry in the action string to be sure this label is used; otherwise another label may be used and this one ignored.

---

---

**digits**

The digits to be sent. The appearance of this parameter depends on the action string.

---

**\$C<command>\$**

This is the command. It can appear anywhere in the action string. Supported commands (or shortcuts) include:

hang-up (hu)

hold (h)

waitconnect (wc)

pause <number of seconds> (p <num sec>) where the maximum value is 10

---

**\$T<type>\$**

The embedded action type. Multiple actions can be defined. Supported action types include:

invite

dtmf

refer

*Note:* Polycom recommends that you always define this field. If it is not defined, the supplied digits will be dialed using INVITE (if no active call) or DTMF (if an active call). The use of refer method is call server dependent and may require the addition of star codes.

---

**\$M<macro>\$**

The embedded macro. The <macro> string must begin with a letter. If the macro name is not defined, the execution of the action string fails.

---

**\$P<prompt num>N<num digits>\$**

The user input prompt string. See [Prompt Macro Substitution](#).

---

**\$S<speed dial index>\$**

The speed dial index. Only digits are valid. The action is found in the `contact` field of the local directory entry pointed to by the index.

---

**\$F<internal function>\$**

An internal function. For more information, see [Internal Key Functions](#).

---

**URL**

A URL. Only one per action string is supported.

---

## Prompt Macro Substitution

The `efk.efklist.x.action.string` can be defined by a macro substitution string, **PnNn** where:

- *Pn* is the prompt *x* as defined by `efk.efkprompt.x`.
- *Nn* is the number of digits or letters that the user can enter. The value must be between 1 and 32 characters; otherwise the macro execution will fail. The user needs to press the **Enter** soft key to complete data entry.



The macros provide a generic and easy to manage way to define the prompt to be displayed to the user, the maximum number of characters that the user can input, and the action that the system performs once all user input has been collected. The macros are case sensitive.

If a macro attempts to use a prompt that is disabled, the macro execution fails. A prompt is not required for every macro.

## ***Expanded Macros***

Expanded macros are prefixed with the ^ character and are inserted directly into the local directory `contact` field. For more information, see [Use the Local Contact Directory](#).

## ***Special Characters***

The following special characters are used to implement the enhanced feature key functionality. Macro names and macro labels cannot contain these characters. If they do, you may experience unpredictable behavior.

- ! The characters following it are a macro name.
- ' or ASCII (0x27) This character delimits the commands within the macro.
- \$ This character delimits the parts of the macro string. This character must exist in pairs, where the delimits the characters to be expanded.
- ^ This character indicates that the following characters represent the expanded macro (as in the action string).

## ***Example Macro***

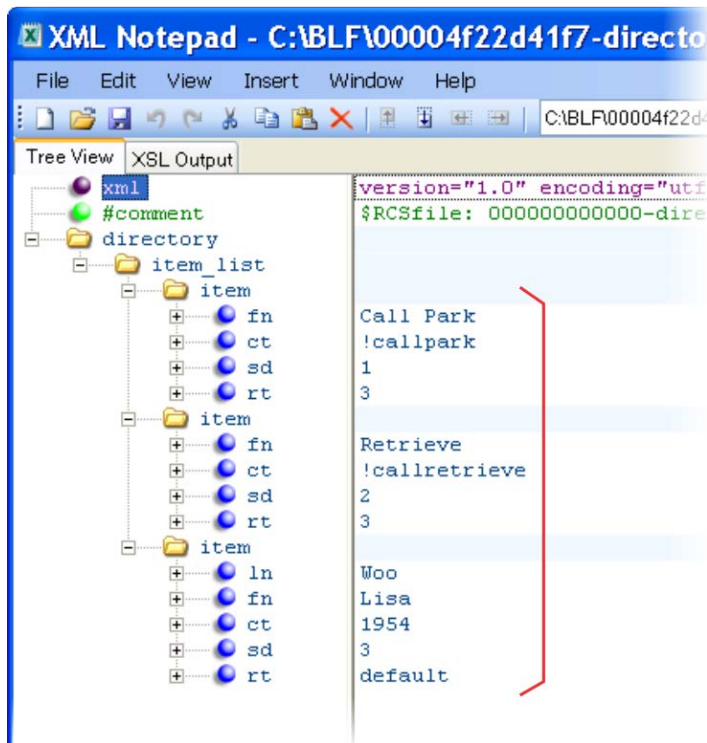
The action string

```
$Changup$*444*$P1N4$$Tinvite$$Cwaitconnect$$P2N3$$Cpause2$$Tdtmf$$Changup$
```

is executed in order as follows:

- a The user is prompted for 4 digits. For example, *1234*.
- b The user is prompted for 3 digits. For example, *567*.
- c The user's active call is disconnected.
- d The string *\*444\*1234* is sent using the INVITE method.
- e Once connected, there is a 2 second pause, and then the string *567* is sent using DTMF dialing on the active call.
- f The active call is disconnected.

Because line keys and their functions are linked to fields in the directory file, a macro name you enter in `efk.list.x.mname` must match the name you enter to the `contact (cn)` field in the directory file. The macro name you enter in the `(ct)` field of the directory file must begin with the '!' prefix. The following example directory file shows a line key configured with Call Park, Call Retrieve, and a speed dial contact Lisa Woo.



For an explanation of all fields in the directory file, see the table [Understanding the Local Contact Directory](#).

### Speed Dial Example

If your organization’s voicemail system is accessible through 7700 and your voicemail password is 2154, you can use a speed dial key to access your voicemail by entering `7700$Cpause3$2154` as the contact number in the `contact (ct)` element.



**Tip: Ensuring Users Do Not Delete Definitions in the Contact Directory**

To avoid users accidentally deleting the definitions in the contact directory, make the contact directory read only.

## Configure Soft Keys

You can customize the functions of the system's soft keys. This feature is typically used to access frequently used functions or to create menu shortcuts to frequently used system settings. The parameters that configure soft keys are shown in the table [Configure Soft Keys](#). As with EFK line keys, you assign functions to soft keys using macros. For a list of the available macros, see the topic [Understanding Macro Definitions](#) in the [Configure Enhanced Feature Keys](#) section.

You can configure the soft keys to display functions depending on the system's menu level or call state. For example, you can make a Call Park soft key available when the system is in an active call state.

Custom soft keys can be added in the following call states:

- **Idle** There are no active calls.
- **Active** This state starts when a call is connected. It stops when the call stops or changes to another state (like hold or dial tone).
- **Alerting** (or ringing or incoming proceeding) The system is ringing.
- **Dial tone** You can hear a dial tone.
- **Proceeding** (or outgoing proceeding) This state starts when the system sends a request to the network. It stops when the call is connected.
- **Setup** This state starts when the user starts keying in a system number. This state ends when the Proceeding state starts.
- **Hold** The call is put on hold locally.

You can disable the display of any default soft key to make room for custom soft keys. Or, if your system does not have a particular hard key, you may want to create a soft key. For example, if the system does not have a **Do Not Disturb** hard key, you can create a **Do Not Disturb** soft key.

New soft keys can be created as:

- An Enhanced Feature Key sequence
- A speed dial contact directory entry
- An Enhanced Feature Key macro
- A URL
- A chained list of actions

The default soft keys that can be disabled include:

- **New Call**
- **End Call**
- **Split**
- **Join**
- **Forward**
- **Directories**
- **MyStatus** and **Buddies**
- **Hold, Transfer, and Conference**



### Note: Inserting Soft Keys Between the Hold, Transfer, and Conference Soft Keys

The **Hold**, **Transfer**, and **Conference** soft keys are grouped together to avoid usability issues. You may experience errors if you try to insert a soft key between these three grouped soft keys.

If you want your system to display both default and custom soft keys, you can configure them in any order. However, the order in which soft keys display depends on the system's menu level and call state. If you have configured custom soft keys to display with the default soft keys, the order of the soft keys may change.

Up to 10 custom soft keys can be configured. If more soft keys are configured than fit on the system's screen, a **More** soft key displays. Press the **More** soft key to view the remaining soft keys.

The table [Configure Soft Keys](#) shows you the parameters for configuring soft keys. However, this feature is part of Enhanced Feature Keys (EFK) and you must enable the enhanced feature keys parameter to configure soft keys. See the section [Configuring Enhanced Feature Keys](#) for details about configuring soft keys and line keys on the system.

### Configure Soft Keys

Central Provisioning Server	template > parameter
To turn Enhanced Feature Keys on (required)	<code>features.cfg</code> > <a href="#">feature.enhancedFeatureKeys.enabled</a>
Specify the macro for a line key or soft key function	<code>features.cfg</code> > <a href="#">softkey.x.action</a>
To enable a custom soft key	<code>features.cfg</code> > <a href="#">softkey.x.enable</a>
Specify the position of the soft key on the system screen	<code>features.cfg</code> > <a href="#">softkey.x.insert</a>
Specify the text to display on the soft key label	<code>features.cfg</code> > <a href="#">softkey.x.label</a>
To position the custom soft key before the default soft keys	<code>features.cfg</code> > <a href="#">softkey.x.precede</a>
Specify which call states the soft key will display in	<code>features.cfg</code> > <a href="#">softkey.x.use.*</a>
To display soft keys for various system features, including default soft keys	<code>features.cfg</code> > <a href="#">softkey.feature.*</a>

## Example Soft Key Configurations

This section provides a few examples of available soft key configurations.



### Web Info: Using Configurable Soft Keys

For more examples, see [Feature Profile 42250: Using Enhanced Feature Keys and Configurable Soft Keys on Polycom Systems](#).

**To disable the New Call soft key:**

- 1 In the **features.cfg** template file, set `softkey.feature.newcall` to '0'.
- 2 Reboot the system.

The **New Call** soft key is not displayed and the soft key space it occupied is empty.

**To map a chained list of actions to a soft key:**

- 1 Configure speed dial index 2 in the contact directory file with a system address. For example, enter '2900' in the contact (ct) field.
- 2 In the contact directory, enter '12' in the contact (ct) field of speed dial index 1.
- 3 Update the configuration file as follows:

```
softkey.1.label = ChainAct
softkey.1.action = $S1$Tinvite$
softkey.1.use.idle = 1
```

- 4 Reboot the system.

A soft key **ChainAct** displays. Press **ChainAct** to dial the system number 2900.

**To map the Do Not Disturb Enhanced Feature Key sequence to a soft key:**

- 1 Update the configuration file as follows:

```
softkey.1.label = DND
softkey.1.action = $FDoNotDisturb$
softkey.1.use.idle = 1
```

- 2 Reboot the system.

A **DND** soft key is displayed on the system when it is in the idle state. When the **DND** soft key is pressed, the Do Not Disturb icon is displayed.

**To map a Send-to-Voicemail Enhanced Feature Key sequence to a soft key:**

- 1 Update the configuration file as follows:

```
softkey.2.label = ToVMail
softkey.2.action = ^*55$P1N10$Tinvite$
softkey.2.use.alerting = 1
```

- 2 Reboot the system.

When another party calls, the **ToVMail** soft key is displayed. When the user presses the **ToVMail** soft key, the other party is transferred to voicemail.

**Tip: Active Call Transfer Star Codes Depend On Your Call Server**

The exact star code to transfer the active call to Voicemail depends on your call server.

The following example enables a soft key in the system's idle state that navigates to a system's administrator settings. The soft is inserted in soft key position 3, after the default soft keys. Note the macro action string:

```
$FMenu$$FDialpad3$$FDialpad2$$FDialpad4$$FDialpad5$$FDialpad6$$FSoftKey1$
```



## Capture Wireshark Trace using Flash File to USB Flash Drive

The CX5500 unified conference station allows you to capture the Wireshark trace to a USB flash drive. You must connect the USB flash drive to the CX5500 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 CX5500 system.
5. Turn on the CX5500 system.

The CX5500 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 CX5500 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 CX5500 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 CX5500 system.
  4. Turn on the CX5500 system.
  5. From a computer connected to the same network, perform a telnet to the CX5500 unified conference station.
  6. Use the following commands to start capturing:
    - a. `pcapFilterSet` – Sets the capture filter to be used with the USB flash drive
    - b. `pcapStart` – Starts the capture to 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.

## Enable the Power Saving Feature

CX5500 systems support a power-saving feature, which is disabled by default. This feature has a number of options you can configure, as listed in the table [Power Saving](#). You can turn on the system's power-saving feature during non-working hours and working hours. If you want to turn on power-saving during non-working hours, you can configure the power-saving feature around your work schedule. Or, if you want to turn on the power-saving feature while at work, you can configure the sensitivity of the system's motion detection system and an idle time after which the system enters the power-saving mode.

### Power Saving

Central Provisioning Server	template > parameter
Turn the power-saving feature on or off	site.cfg > <a href="#">powerSaving.enable</a>
Specify the amount of time before the system screen goes idle	site.cfg > <a href="#">powerSaving.idleTimeout.*</a>
Set the office hour start time and duration for each day of the week	site.cfg > <a href="#">powerSaving.officeHours.*</a>

### Web Configuration Utility

To turn this feature on or off and configure how it works, navigate to **Settings > Power Saving** and expand the panels to set the general, office hour, idle timeout, and user detection sensitivity settings.

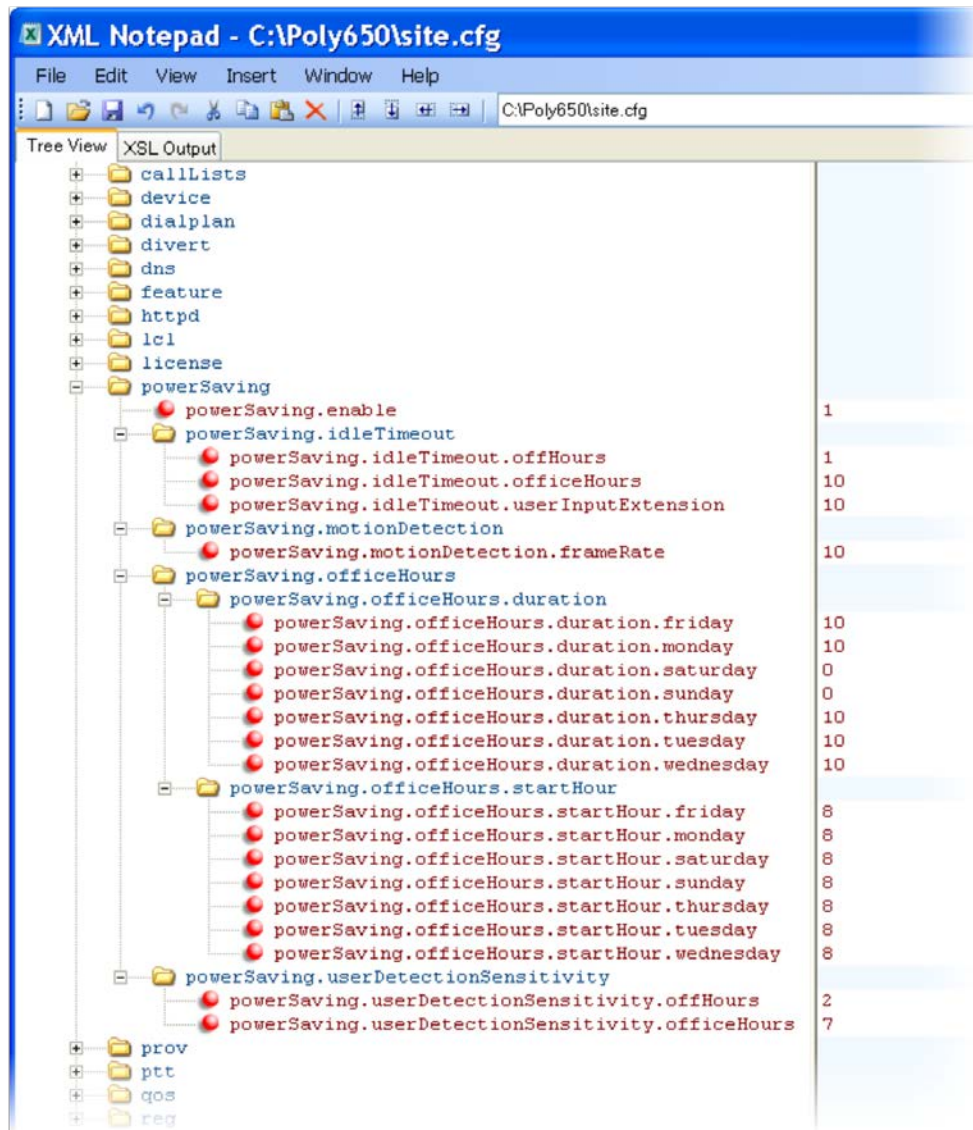
### Local System User Interface

To configure the Power Saving Office Hours, Timeouts, and User Detection, navigate to **Settings > Basic > Power Saving**.



## Example Power-Saving Configuration

The following illustration shows the power-saving default settings, which reflect the hours of a typical work week.



## Configure Group Paging

The Group Paging feature enables you to make pages—one-way audio announcements—to users subscribed to a page group. Administrators must enable Paging before users can subscribe to a page group.

Paging has 25 groups you can subscribe to and announcements play only through the system's speaker system. To configure Group Paging, see the table [Configure Group Paging](#).





### Web Info: Using a Different IP multicast address

The Group Paging feature uses an IP multicast address. If you want to change the default IP multicast address, ensure that the new address does not already have an official purpose as specified in the [IPv4 Multicast Address Space Registry](#).

You specify the same IP multicast address in the parameter `ptt.address` for Paging mode. Paging administrator settings shown in the table [Configure Group Paging](#) are located in the `site.cfg` template file. Page group settings are located in the `features.cfg` template file.

### Configure Group Paging

Central Provisioning Server	template > parameter
Specify the IP multicast address used for the paging feature	<code>site.cfg</code> > <code>ptt.address</code>
Enable Paging mode	<code>site.cfg</code> > <code>ptt.pageMode.enable</code>
Specify the display name	<code>site.cfg</code> > <code>ptt.pageMode.displayName</code>
Specify settings for all Page groups	<code>features.cfg</code> > <code>ptt.pageMode.group.*</code>

### Web Configuration Utility

To specify the IP multicast address and port, and available paging groups for Group Paging, navigate to **Settings > Paging/PTT Configuration** and expand **Settings** and **Group Paging Configuration**.

### Local System User Interface

Specify the IP multicast address and port, and available paging groups for Group Paging from the Paging/PTT Configuration menu, accessible from **Settings > Advanced > Admin Settings**. Users can access basic Group Paging settings from **Settings > Basic > Preferences > Paging/PTT Configuration**.

## Paging Mode Groups

You can subscribe to the following Paging groups. Note that groups one and two are enabled by default, and that groups 24 and 25, the priority and emergency channels respectively, are also enabled by default.

ptt.channel.24.subscribed	1
ptt.channel.25.subscribed	1
ptt.pageMode	
ptt.pageMode.group	
ptt.pageMode.group.1.allowTransmit	1
ptt.pageMode.group.1.available	1
ptt.pageMode.group.1.label	
ptt.pageMode.group.1.subscribed	1
ptt.pageMode.group.2.allowTransmit	1
ptt.pageMode.group.2.available	1
ptt.pageMode.group.2.label	
ptt.pageMode.group.2.subscribed	0
ptt.pageMode.group.3.subscribed	0
ptt.pageMode.group.4.subscribed	0
ptt.pageMode.group.5.subscribed	0
ptt.pageMode.group.6.subscribed	0
ptt.pageMode.group.7.subscribed	0
ptt.pageMode.group.8.subscribed	0
ptt.pageMode.group.9.subscribed	0
ptt.pageMode.group.10.subscribed	0
ptt.pageMode.group.11.subscribed	0
ptt.pageMode.group.12.subscribed	0
ptt.pageMode.group.13.subscribed	0
ptt.pageMode.group.14.subscribed	0
ptt.pageMode.group.15.subscribed	0
ptt.pageMode.group.16.subscribed	0
ptt.pageMode.group.17.subscribed	0
ptt.pageMode.group.18.subscribed	0
ptt.pageMode.group.19.subscribed	0
ptt.pageMode.group.20.subscribed	0
ptt.pageMode.group.21.subscribed	0
ptt.pageMode.group.22.subscribed	0
ptt.pageMode.group.23.subscribed	0
ptt.pageMode.group.24.subscribed	1
ptt.pageMode.group.25.subscribed	1
roaming_buddies	
roaming_privacy	

## Configure Shared Call Appearances

With the shared call appearance feature enabled, an active call displays simultaneously on multiple systems in a group. By default, the answering system has sole access to the incoming call, called line seize. You can enable another system in the group the ability to enter a conversation, called a barge in. If the answering system places the call on hold, that call becomes available to all systems of that group. The parameters you can configure are listed in the table [Configure Shared Call Appearances](#). All call states of a call —active, inactive, on hold—are displayed on all systems of a group.

This feature is dependent on support from a SIP call server. To enable shared call appearances on your system, obtain a shared line address from your SIP service provider. For more details on SIP signaling with shared call appearances, see [Shared Call Appearance Signaling](#).



### Tip: Shared Call and Bridged Line Appearances Are Distinct

Shared call appearances and bridged line appearances are similar signaling methods that enable more than one system to share the same line or registration. The method you use varies with the SIP call server you are using.

## Configure Shared Call Appearances

### Central Provisioning Server

Specify the shared line address

**template** > [parameter](#)

Specify the line type as shared

**reg-basic.cfg** > [reg.x.address](#)

**reg-advanced.cfg** > [reg.x.type](#)

To disable call diversion, expose auto-holds, resume with one touch, or play a tone if line-seize fails

**sip-interop.cfg** > [call.shared.\\*](#)

Specify standard or non-standard behavior for processing a line-seize subscription for mutual exclusion

**sip-interop.cfg** > [volpProt.SIP.specialEvent.lineSeize.nonStandard](#)

Specify barge-in capabilities and line-seize subscription period if using per-registration servers. A shared line will subscribe to a server providing call state information

**reg-advanced.cfg** > [reg.x.\\*](#)

Specify per-registration whether diversion should be disabled on shared lines

**sip-interop.cfg** > [divert.x.sharedDisabled](#)

### Web Configuration Utility

To specify the line seize subscription period for SIP Server 1 or Server 2, navigate to **Settings > SIP**, expand **Server 1** or **Server 2**, and edit the **Line Seize Timeout**.

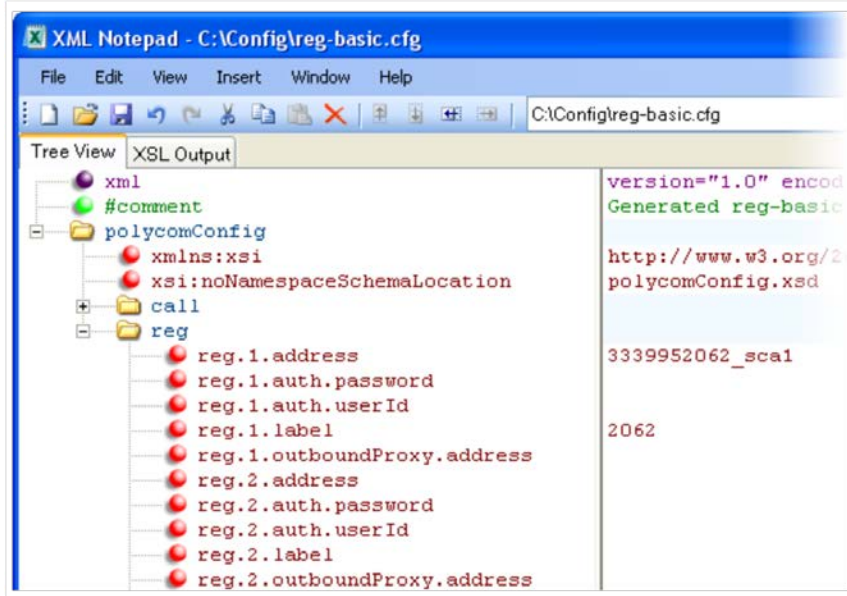
To specify standard or non-standard behavior for processing line-seize subscription for the mutual exclusion feature, navigate to **Settings > SIP**, expand **Local Settings**, and enable or disable **Non Standard Line Seize**. Specify the per-registration line type (shared) and the line-seize subscription behavior if you are using per-registration server, and whether diversion should be disabled on shared lines by navigating to **Settings > Lines**.

### Local System User Interface

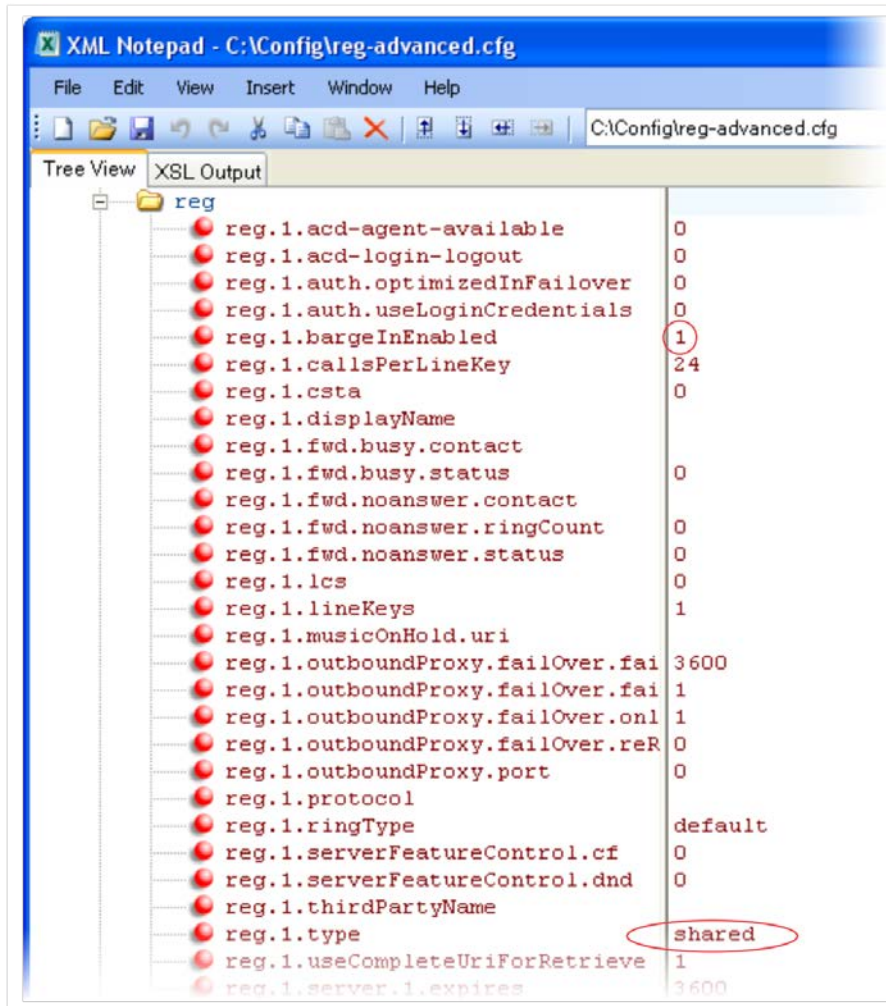
To specify the per-registration line type (shared) and shared line address, navigate to **Settings > Advanced > Admin Settings > Line Configuration > Line X > Line Type**.

## Example Configuration

The following illustration shows the address of a registered system line and the label that displays beside the line key, as specified in the **reg-basic.cfg** template.



If you want to configure this line to be shared, in the **reg-advanced.cfg** template, specify `shared` in `reg.1.type`. All systems that specify `shared` for registration 1 will have shared call appearance enabled for this line. In the following example, the `reg.1.bargeInEnabled` parameter is set to '1' to enable systems of this group to barge in on active calls.



After setting these parameters, activity on line 2062 displays on all systems that configure a shared call appearance for line 2062.

## Enable Bridged Line Appearance

Bridged line appearance connects calls and lines to multiple systems. See the table [Enable Bridged Line Appearance](#) for a list of the parameters you can configure. With bridged line appearance enabled, an active call displays simultaneously on multiple systems in a group. By default, the answering system has sole access to the incoming call—line seize. If the answering system places the call on hold, that call becomes available to all systems of that group. All call states—active, inactive, on hold—are displayed on all systems of a group. For more information, see [Bridged Line Appearance Signaling](#).



### Tip: Bridged Line and Shared Call Appearances are Distinct

Shared call appearances and bridged line appearances are similar signaling methods that enable more than one system to share the same line or registration. The methods you use vary with the SIP call server you are using. In the configuration files, bridged lines are configured by 'shared line' parameters. The barge-in feature is not available with bridged line appearances; it is available with shared call appearances.

## Enable Bridged Line Appearance

Central Provisioning Server	template > parameter
Specify whether call diversion should be disabled by default on all shared lines	<code>sip-interop.cfg</code> > <code>call.shared.disableDivert</code>
Specify the per-registration line type (private or shared)	<code>reg-advanced.cfg</code> > <code>reg.x.type</code>
Specify the shared line third-party name	<code>reg-advanced.cfg</code> > <code>reg.x.thirdPartyName</code>
Specify whether call diversion should be disabled on a specific shared line (overrides default)	<code>reg-advanced.cfg</code> > <code>divert.x.sharedDisabled</code>

## Web Configuration Utility

To specify the line type (private or shared) and the shared line third party name for a specific line, navigate to **Settings > Lines**, choose a line from the left pane, expand **Identification**, and edit **Type** and **Third Party Name**. To specify whether call diversion should be disabled for a specific shared line, navigate to **Settings > Lines**, choose a line from the left pane, expand **Call Diversion**, and set **Disable Forward for Shared Lines**.

## Local System User Interface

Specify the line type for each registration and the shared line third party name by navigating to **Settings > Advanced > Admin Settings > Line Configuration > Line X**. Edit the **Line Type** and the **Third Party Name**.

## Example Bridged Line Appearance Configuration

To begin using bridged line appearance, get a registered address dedicated for use with bridged line appearance from your call server provider. This dedicated address must be assigned to a system line in the `reg.x.address` parameter of the `reg-basic.cfg` template.



Next, in the **reg-advanced.cfg** template, enter the dedicated address in `thirdPartyName` for all systems of the BLA group and set the line type to `shared`. In this example, two or more systems can use the same dedicated address `6044533036` as the BLA address, and the line `type` has been set to `shared` from the default `private`.

<code>reg.1.outboundProxy.port</code>	<code>0</code>
<code>reg.1.protocol</code>	<code>default</code>
<code>reg.1.ringType</code>	<code>0</code>
<code>reg.1.serverFeatureControl.cf</code>	<code>0</code>
<code>reg.1.serverFeatureControl.dnd</code>	<code>0</code>
<code>reg.1.thirdPartyName</code>	<code>6044533036</code>
<code>reg.1.type</code>	<code>shared</code>
<code>reg.1.useCompleteUriForRetrieve</code>	<code>1</code>
<code>reg.1.server.1.expires</code>	<code>3600</code>
<code>reg.1.server.1.expires.lineSeize</code>	<code>30</code>
<code>reg.1.server.1.expires.overlap</code>	<code>60</code>
<code>reg.1.server.1.lcs</code>	<code>0</code>
<code>reg.1.server.1.retryMaxCount</code>	<code>3</code>
<code>reg.1.server.1.retryTimeOut</code>	<code>0</code>
<code>reg.1.server.1.specialInterop</code>	<code>standard</code>
<code>reg.1.server.2.expires</code>	<code>3600</code>
<code>reg.1.server.2.expires.lineSeize</code>	<code>30</code>

For example, two systems `6044533036` and `6044533037` are configured with the 3036 BLA address. There is an incoming call to `6044533036` from `3038` that causes `3036` and `3037` systems to show the incoming call.

## Enable Voicemail Integration

The system is compatible with voicemail servers. You can configure each system or line registration per system to subscribe with a SIP URL to a voicemail server contact. You can also configure the system to access voicemail with a single soft key, for example, the **Messages** icon in the status bar on the CX5500 system. When you access the voicemail server, the system gives a visual and audio alert; you can also configure a message waiting alert to indicate that you have unread voicemail messages. The following table shows you the parameters you can configure.

### Voicemail Integration

Central Provisioning Server	template > parameter
To turn one-touch Voicemail on or off	<code>sip-interop.cfg</code> > <code>up.oneTouchVoiceMail</code>
Specify the URI of the message center server	<code>sip-interop.cfg</code> > <code>msg.mwi.x.subscribe</code>
Set the mode of message retrieval	<code>sip-basic.cfg</code> > <code>msg.mwi.x.callBackMode</code>
Specify a contact number for the system to call to retrieve messages, <code>callBackMode</code> must be set to <code>Contact</code>	<code>sip-interop.cfg</code> > <code>msg.mwi.x.callBack</code>
Specify if message waiting notifications should display or not	<code>site.cfg</code> > <code>up.mwiVisible</code>
Specify if the system screen backlight illuminates when you receive a new voicemail message	<code>site.cfg</code> > <code>mwi.backLight.disable</code>

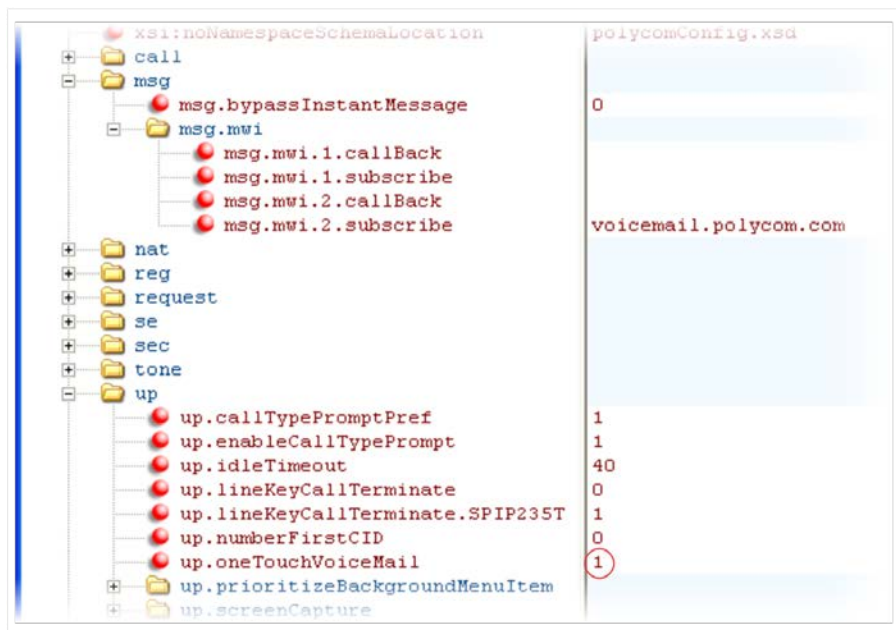
### Web Configuration Utility

To turn One Touch Voicemail on or off, navigate to **Preferences > Additional Preferences**, expand **User Preferences**, and set **One Touch Voicemail**.

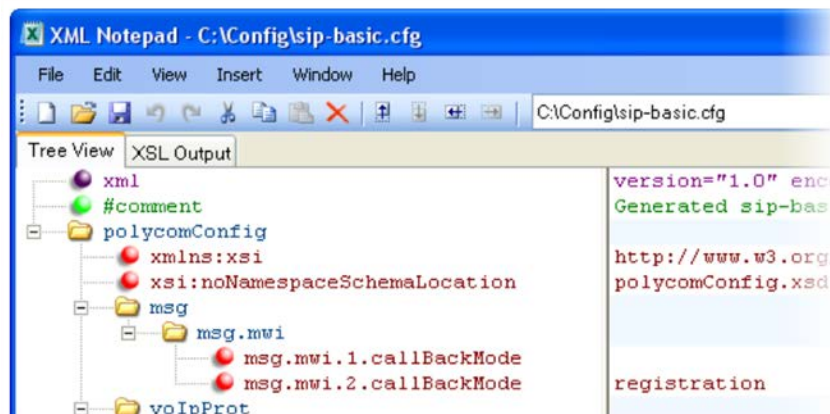
To specify the message center settings for a specific line, navigate to **Settings > Lines**, select a line from the left pane, and expand **Message Center**.

## Example Voicemail Configuration

The following illustration shows you how to enable one-touch access to the voicemail server. In the next illustration, line 2 is configured to subscribe to the voicemail server at *voicemail.polycom.com*.



The following illustration shows that, in the **sip-basic.cfg** template, the default **callBackMode** setting for line 2 is set to **registration**. The system will use the address assigned to line 2 to subscribe to the voicemail server you entered in **msg.mwi.2.subscribe**.





Once this is enabled in the **sip-interop.cfg** template, on the system, press the **Messages** key and select **Message Center** to access your voicemail.

## Enable Multiple Registrations

The CX5500 system can have multiple registrations; each registration requires an address, or system number. CX5500 systems registered with Microsoft Lync Server support one Lync registration. Enable Multiple Registrations explains the registration parameters and options. The CX5500 system supports a maximum of 16 registrations.

Each registration can be mapped to one or more line keys. Note that a line key can be used for only one registration. The user can select which registration to use for outgoing calls or which to use when initiating new instant message dialogs. Note that this feature is one of several features associated with *Flexible Call Appearances*. For definitions of all features associated with Flexible Call Appearances, see the following table.

### Enable Multiple Registrations

---

#### Central Provisioning Server

Specify the local SIP signaling port and several optional SIP servers to register to. For each server specify the registration period and the signaling failure behavior

Specify a display name, a SIP address, an optional display label, an authentication user ID and password, the number of line keys to use, and an optional array of registration servers. The authentication user ID and password are optional and for security reasons can be omitted from the configuration files. The local flash parameters will be used instead. The optional array of servers and their parameters will override the servers specified in <volpProt.server/> if non-Null

**template** > [parameter](#)

**sip-interop.cfg** > [volpProt.SIP.\\*](#) and [volpProt.server.x.\\*](#)

**reg-basic.cfg, reg-advanced.cfg** > [reg.x.\\*](#)

---

#### Web Configuration Utility

Specify the local SIP signaling port and several optional SIP servers to register to.

Specify a display name, a SIP address, an optional display label, an authentication user ID and password, the number of line keys to use, and an optional array of registration servers. The authentication user ID and password are optional and for security reasons can be omitted from the configuration files. The local flash parameters will be used instead. The optional array of servers will override the servers specified in <server/> in non-Null.

Configure multiple registrations by navigating to **Settings > Lines**.

---

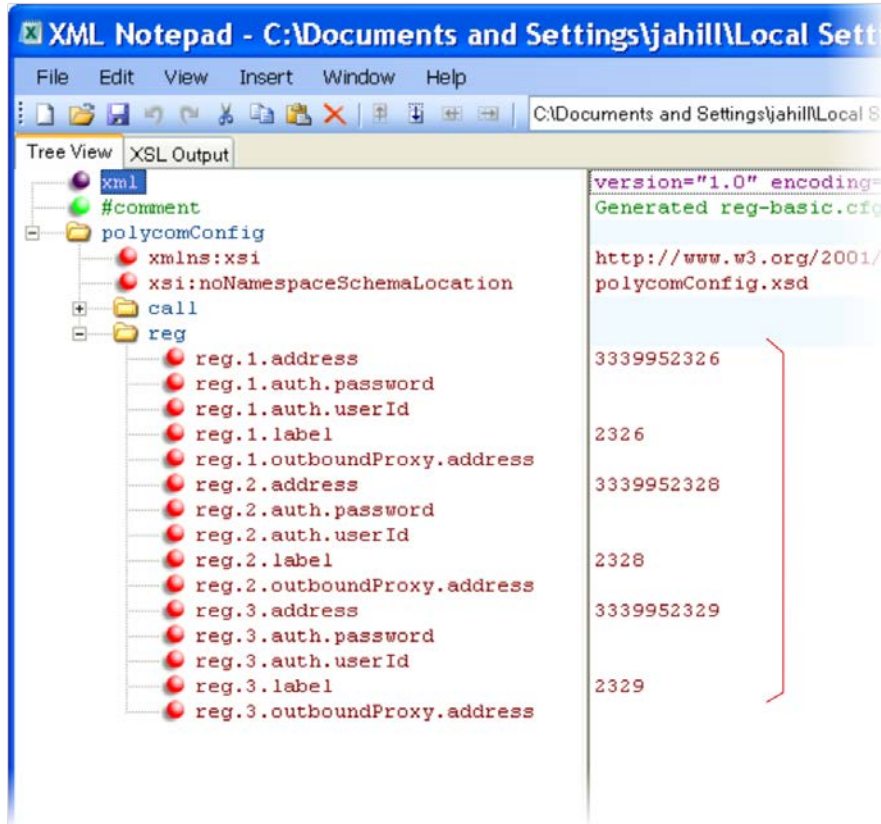
#### Local System User Interface

Use the Call Server Configuration and Line Configuration menu to specify the local SIP signaling port, a default SIP server to register to, and registration information for up to twelve registrations (depending on the system model). These configuration menus contain a sub-set of all the parameters available in the configuration files.

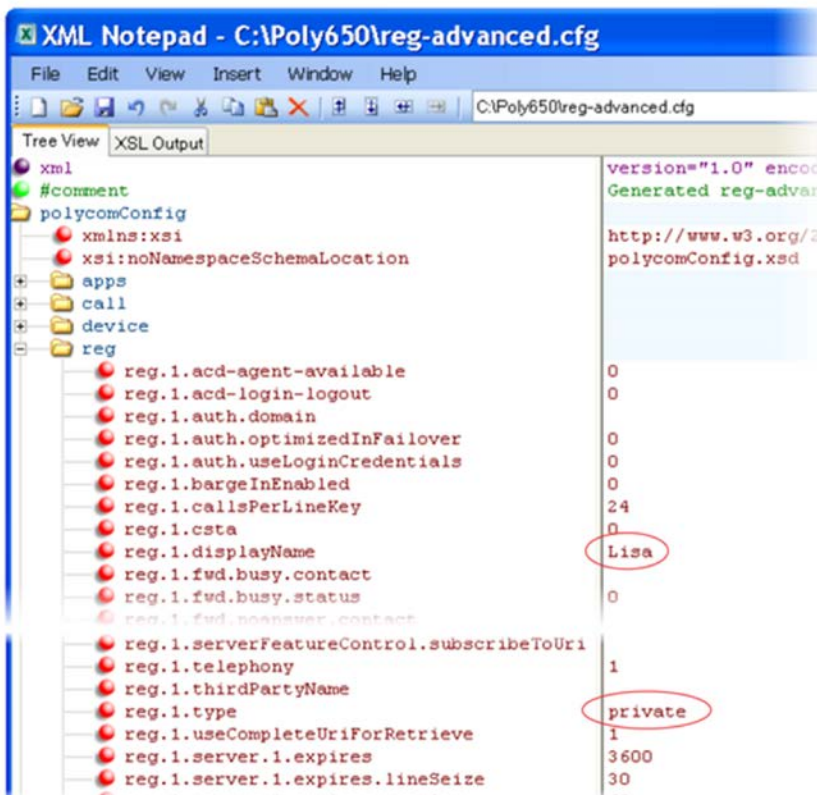
---

## Example Multiple Registration Configuration

In the next illustration, in the **reg-basic.cfg** template, multiple line registrations and a label for each registration has been enabled for lines 1, 2, and 3.



In the **reg-advanced.cfg** template shown next, when you make a call using line 1, the name you enter in `reg.1.displayname` will display as your caller ID, in this case *Lisa*. The parameter `reg.x.type` is left in the default `private`, which indicates that the registration will use standard call signaling.



## Set Up Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of system service if, for example, where the call server needs to be taken offline for maintenance, the server fails, or the connection between the system and the server fails. The table [Set Up Server Redundancy](#) points to several parameters you can configure.

Two types of redundancy are possible:

- **Failover** In this mode, full system functionality is preserved by having a second call server of equivalent capability take over from the server that went down/off-line. Use this mode of operation with DNS mechanisms or 'IP Address Moving' from the primary to the back-up server.
- **Fallback** In this mode, a second call server of lesser capability (router or gateway device) takes over call control to provide basic calling capability without some of the richer features offered by the primary call server (for example, shared lines, presence, and Message Waiting Indicator). The CX5500 system supports configuration of multiple servers per SIP registration for this purpose.

In some cases, a combination of the two may be deployed. Consult your SIP server provider for recommended methods of configuring systems and servers for failover configuration.

**Note: Compatibility with Microsoft® Lync**

The concurrent failover/fallback feature is not compatible with Microsoft Lync.

**Caution: Old Failover Behavior Is Not Supported**

Prior to SIP 2.1, the `reg.x.server.y` parameters in `<reg/>` could be used for failover configuration. The older behavior is no longer supported. Customers that are using the `reg.x.server.y.*` configuration parameters where  $y \geq 2$  should take care to ensure that their current deployments are not adversely affected. For example, the system will only support advanced SIP features such as shared lines, missed calls, and presence with the primary server ( $y=1$ ).

**Set Up Server Redundancy****Central Provisioning Server**`template > parameter`

Specify server redundancy options including fallback mode, fallback timeout, and failover registration behavior

`sip-interop.cfg > volpProt.server.x.failOver.*`

Specify which server to contact if failover occurs

`reg-advanced.cfg > reg.x.auth.optimizedInFailover`

Override the default server redundancy options for a specific registration

`reg-advanced.cfg > reg.x.outboundProxy.failOver.*`**Web Info: Failover Configuration Details**

For more information, see [Technical Bulletin 5844: SIP Server Fallback Enhancements on Polycom Systems](#) and [Engineering Advisory 66546: Using Optional Geographical Server Redundancy Failover Behaviors](#).

## DNS SIP Server Name Resolution

If a DNS name is given for a proxy/registrar address, the IP addresses associated with that name will be discovered as specified in RFC 3263. If a port is given, the only lookup will be an A record. If no port is given, NAPTR and SRV records will be tried, before falling back on A records if NAPTR and SRV records return no results. If no port is given, and none is found through DNS, 5060 will be used. If the registration type is Transport Layer Security (TLS), 5061 will be used as the port number. See [RFC 3263](#) for an example.

**Caution: No DNS Resolution Will Cause Failover**

Failure to resolve a DNS name is treated as signaling failure that will cause a failover.

## Behavior When the Primary Server Connection Fails

For Outgoing Calls (INVITE Fallback)

When the user initiates a call, the system will go through the following steps to connect the call:

- 1 The system will try to call the working server.
- 2 If the working server does not respond correctly to the INVITE, the system will try and make a call using the next server in the list (even if there is no current registration with these servers). This could be the case if the Internet connection has gone down, but the registration to the working server has not yet expired.
- 3 If the second server is also unavailable, the system will try all possible servers (even those not currently registered) until it either succeeds in making a call or exhausts the list at which point the call will fail.

At the start of a call, server availability is determined by SIP signaling failure. SIP signaling failure depends on the SIP protocol being used:

- If TCP is used, then the signaling fails if the connection fails or the Send fails.
  - If UDP is used, then the signaling fails if ICMP is detected or if the signal times out. If the signaling has been attempted through all servers in the list and this is the last server, then the signaling fails after the complete UDP timeout defined in RFC 3261. If it is not the last server in the list, the maximum number of retries using the configurable retry timeout is used. For more information, see [<server/>](#) and [<reg/>](#).



### Caution: Use Long TTLs to Avoid DNS Timeout Delays

If DNS is used to resolve the address for Servers, the DNS server is unavailable, and the TTL for the DNS records has expired, the system will attempt to contact the DNS server to resolve the address of all servers in its list *before* initiating a call. These attempts will timeout, but the timeout mechanism can cause long delays (for example, two minutes) before the system call proceeds using the working server. To prevent this issue, long TTLs should be used. Polycom recommends deploying an on-site DNS server as part of the redundancy solution.

## System Configuration

The systems at the customer site are configured as follows:

- Server 1 (the primary server) will be configured with the address of the service provider call server. The IP address of the server(s) will be provided by the DNS server, for example:  
`reg.1.server.1.address=voipserver.serviceprovider.com .`
- Server 2 (the fallback server) will be configured to the address of the router/gateway that provides the fallback telephony support and is on-site, for example:  
`reg.1.server.2.address=172.23.0.1.`

**Note: Caution When Using Multiple Servers Per Registration**

It is possible to configure the system for more than two servers per registration, but you need to exercise caution when doing this to ensure that the system and network load generated by registration refresh of multiple registrations does not become excessive. This would be of particular concern if a system had multiple registrations with multiple servers per registration and it is expected that some of these servers will be unavailable.

## System Operation for Registration

After the system has booted up, it will register to all the servers that are configured.

Server 1 is the primary server and supports greater SIP functionality than other servers. For example, SUBSCRIBE/NOTIFY services used for features such as shared lines and presence, will be established only with Server 1.

Upon the registration timer expiry of each server registration, the system will attempt to re-register. If this is unsuccessful, normal SIP re-registration behavior (typically at intervals of 30 to 60 seconds) will proceed and continue until the registration is successful (for example, when the Internet link is once again operational). While the primary server registration is unavailable, the next highest priority server in the list will serve as the working server. As soon as the primary server registration succeeds, it will return to being the working server.

**Note: Failover to Servers that are Not Registered**

If `reg.x.server.y.register` is set to 0, the system will not register to that server. However, the INVITE will fail over to that server if all higher priority servers are down.

## Recommended Practices for Fallback Deployments

In situations where server redundancy for fallback purpose is used, the following measures should be taken to optimize the solution:

- Deploy an on-site DNS server to avoid long call initiation delays that can result if the DNS server records expire.
- Do not use OutBoundProxy configurations on the system if the OutBoundProxy could be unreachable when the fallback occurs. If Server 2 is not accessible through the configured proxy, call signaling with Server 2 will fail.
- Avoid using too many servers as part of the redundancy configuration as each registration will generate more traffic.
- Educate users as to the features that will not be available when in fallback operating mode.

**Note: Compatibility with Microsoft® Lync**

The concurrent/registration failover/fallback feature is not compatible with Microsoft® Lync.

## Use the Presence Feature

The presence feature enables you to monitor the status of other remote users and systems. By adding remote users to your Buddy List, you can monitor changes in the status of remote users in real time or you can monitor remote users as speed-dial contacts. You can also manually specify your status in order to override or mask automatic status updates to others and you can receive notifications when the status of your a remote line changes. The table [Use the Presence Feature](#) lists the parameters you can configure. Note that other system users can block you from monitoring their systems.

For more information about the Lync presence feature, see [Feature Profile 84538: Using Polycom® VVX® Business Media Systems with Microsoft® Lync™ Server 2013](#).

For more information about the BroadSoft UC-One presence feature, see [Feature Profile 84393: Using the Polycom® BroadSoft UC-One Application on Polycom® VVX® Business Media Systems](#).

### Use the Presence Feature

---

#### Central Provisioning Server

**template** > [parameter](#)

Specify the line/registration number used to send SUBSCRIBE for presence

**features.cfg** > [pres.reg](#)

Specify if the MyStatus and Buddies soft keys display on the Home screen

**features.cfg** > [pres.idleSoftkeys](#)

Turn the presence feature on or off

**features.cfg** > [feature.presence.enabled](#)

---

#### Local System User Interface

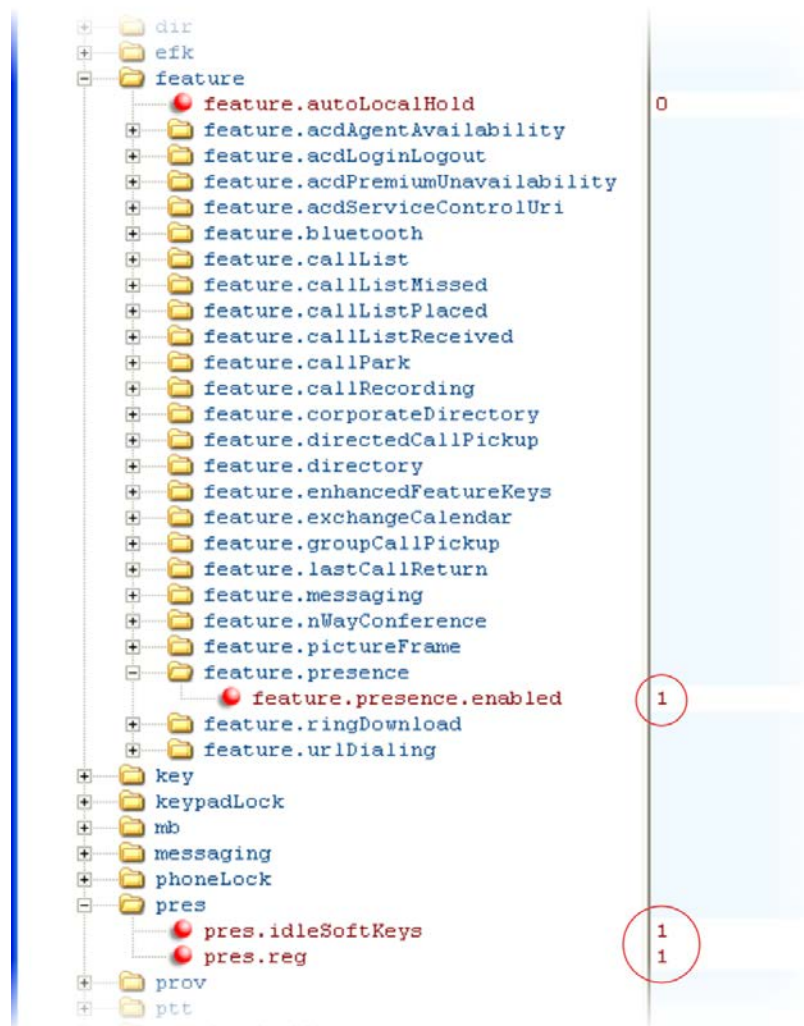
The user can edit the directory contents. The *Buddy Watch* and *Buddy Block* fields control the buddy behavior of contacts.

---



## Example Presence Configuration

In the following illustration, the presence feature has been enabled in `feature.presence.enabled`. The **MyStatus** and **Buddies** soft keys will both display on the system's home screen when you enable the `pres.idleSoftKeys` parameter. The `pres.reg` parameter will use the address of system line 1 for the presence feature.





This configuration enables the presence feature and display the **MyStatus** and **Buddies** soft keys on the system. When you press the **Buddies** soft key, contacts you have entered to your Buddy List display.



Presence Soft Keys

## Configuring the Static DNS Cache

Beginning SIP 2.1.0, failover redundancy can only be used when the configured IP server hostname resolves (through SRV or A record) to multiple IP addresses. Unfortunately, the DNS cache cannot always be configured to take advantage of failover redundancy.

The solution in SIP 3.1 is to enable you to statically configure a set of DNS NAPTR SRV and/or A records into the system. See the table [Configuring the Static DNS Cache](#) for configurable parameters.

When a system is configured with a DNS server, it will behave as follows by default:

- The system will make an initial attempt to resolve a hostname that is within the static DNS cache. For example, a query will be made to the DNS if the system registers with its SIP registrar.
- If the initial DNS query returns no results for the hostname or cannot be contacted, then the values in the static cache are used for their configured time interval.
- After the configured time interval has elapsed, a resolution attempt of the hostname will again result in a query to the DNS.
- If a DNS query for a hostname that is in the static cache returns a result, the values from the DNS are used and the statically cached values are ignored.

When a system is not configured with a DNS server, it will behave as follows:

- When the system attempts to resolve a hostname within the static DNS cache, it will always return the results from the static cache.

Support for negative DNS caching as described in RFC 2308 is also provided to allow faster failover when prior DNS queries have returned no results from the DNS server. For more information, see [RFC 2308](#).

### Configuring the Static DNS Cache

#### Central Provisioning Server

Specify the line registration

`template > parameter`

`sip_interop.cfg > reg.x.address`

Specify the call server used for this registration	<b>sip_interop.cfg</b> > <b>reg.x.server.y.*</b>
Specify the DNS A address, hostname, and cache time interval (ttl)	<b>site.cfg</b> > <b>dns.cache.A.x.*</b>
Specify the DNS NAPTR parameters, including: name, order, preference, regexp, replacement, service, and ttl	<b>site.cfg</b> > <b>dns.cache.NAPTR.x.*</b>
Specify DNS SRV parameters, including: name, port, priority, target, ttl, and weight	<b>site.cfg</b> > <b>dns.cache.SRV.x.*</b>

## Example Static DNS Cache Configuration

The following examples show you how to configure the static DNS cache.

### Example 1

This example shows how to configure static DNS cache using A records IP addresses in SIP server address fields.

When the static DNS cache is not used, the **site.cfg** configuration will look as follows:

```

reg
├── reg.1.address 1001
├── reg.1.server.1.address 172.23.0.140
├── reg.1.server.1.port 5075
├── reg.1.server.1.transport UDPOnly
├── reg.1.server.2.address 172.23.0.150
├── reg.1.server.2.port 5075
└── reg.1.server.2.transport UDPOnly
    
```

When the static DNS cache is used, the **site.cfg** configuration will look as follows:

```

reg
├── reg.1.address 1001
├── reg.1.server.1.address sipserver.example.com
├── reg.1.server.1.port 5075
├── reg.1.server.1.transport UDPOnly
├── reg.1.server.2.address
├── reg.1.server.2.port
├── reg.1.server.2.transport
├── dns.cache.A.1.name sipserver.example.com
├── dns.cache.A.1.ttl 3600
├── dns.cache.A.1.address 172.23.0.140
├── dns.cache.A.2.name sipserver.example.com
├── dns.cache.A.2.ttl 3600
└── dns.cache.A.2.address 172.23.0.150
    
```



**Note: Details of the Preceding Example**

Above addresses are presented to Polycom UC Software in order, for example, `dns.cache.A.1`, `dns.cache.A.2`, and so on.

## Example 2

This example shows how to configure static DNS cache where your DNS provides A records for `reg.x.server.x.address` but not SRV. In this case, the static DNS cache on the system provides SRV records. For more information, see [RFC 3263](#).

When the static DNS cache is not used, the **site.cfg** configuration will look as follows:

```

reg
├── reg.1.address          1002@sipserver.example.com
├── reg.1.server.1.address primary.sipserver.example.com
├── reg.1.server.1.port    5075
├── reg.1.server.1.transport UDPOnly
├── reg.1.server.2.address secondary.sipserver.example.com
├── reg.1.server.2.port    5075
└── reg.1.server.2.transport UDPOnly
    
```

When the static DNS cache is used, the **site.cfg** configuration will look as follows:

```

reg
├── reg.1.address          1002
├── reg.1.server.1.address sipserver.example.com
├── reg.1.server.1.port    UDPOnly
├── reg.1.server.2.address
├── reg.1.server.2.port
├── reg.1.server.2.transport
├── dns.cache.SRV.1.name  _sip._udp.sipserver.example.com
├── dns.cache.SRV.1.ttl   3600
├── dns.cache.SRV.1.priority 1
├── dns.cache.SRV.1.weight 1
├── dns.cache.SRV.1.port   5075
├── dns.cache.SRV.1.target primary.sipserver.example.com
├── dns.cache.SRV.2.name  _sip._udp.sipserver.example.com
├── dns.cache.SRV.2.ttl   3600
├── dns.cache.SRV.2.priority 2
├── dns.cache.SRV.2.weight 1
├── dns.cache.SRV.2.port   5075
└── dns.cache.SRV.2.target secondary.sipserver.example.com
    
```



### Settings: Port Value Settings

The `reg.1.server.1.port` and `reg.1.server.2.port` values in this example are set to null to force SRV lookups.

## Example 3

This example shows how to configure static DNS cache where your DNS provides NAPTR and SRV records for `reg.x.server.x.address`.

When the static DNS cache is used, the **site.cfg** configuration will look as follows:

```
reg
├── reg.1.address 1002@sipserver.example.com
├── reg.1.server.1.address 172.23.0.140
├── reg.1.server.1.port 5075
├── reg.1.server.1.transport UDPOnly
├── reg.1.server.2.address 172.23.0.150
├── reg.1.server.2.port 5075
└── reg.1.server.2.transport UDPOnly
```

```
reg
├── reg.1.address 1002@sipserver.example.com
├── reg.1.server.1.address 172.23.0.140
├── reg.1.server.1.port 5075
├── reg.1.server.1.transport UDPOnly
├── reg.1.server.2.address 172.23.0.150
├── reg.1.server.2.port 5075
└── reg.1.server.2.transport UDPOnly
```

When the static DNS cache is used, the **site.cfg** configuration will look as follows:

```

reg.1.address 1002
reg.1.server.1.address sipserver.example.com
reg.1.server.1.port
reg.1.server.1.transport
reg.1.server.2.address
reg.1.server.2.port
reg.1.server.2.transport
dns.cache.NAPTR.1.name sipserver.example.com
dns.cache.NAPTR.1.ttl 3600
dns.cache.NAPTR.1.order 1
dns.cache.NAPTR.1.preference 1
dns.cache.NAPTR.1.flag s
dns.cache.NAPTR.1.service SIP+D2U
dns.cache.NAPTR.1.regex
dns.cache.NAPTR.1.replacement _sip._udp.sipserver.example.com
dns.cache.SRV.1.name _sip._udp.sipserver.example.com
dns.cache.SRV.1.ttl 3600
dns.cache.SRV.1.priority 1
dns.cache.SRV.1.weight 1
dns.cache.SRV.1.port 5075
dns.cache.SRV.1.target primary.sipserver.example.com
dns.cache.SRV.2.name _sip._udp.sipserver.example.com
dns.cache.SRV.2.ttl 3600
dns.cache.SRV.2.priority 2
dns.cache.SRV.2.weight 1
dns.cache.SRV.2.port 5075
dns.cache.SRV.2.target secondary.sipserver.example.com
dns.cache.A.1.name primary.sipserver.example.com
dns.cache.A.1.ttl 3600
dns.cache.A.1.address 172.23.0.140
dns.cache.A.2.name secondary.sipserver.example.com
dns.cache.A.2.ttl 3600
dns.cache.A.2.address 172.23.0.150
    
```



**Settings: Forcing NAPTR Lookups**

The reg.1.server.1.port, reg.1.server.2.port, reg.1.server.1.transport, and reg.1.server.2.transport values in this example are set to null to force NAPTR lookups.



**Web Info: Using a Static DNS Cache**

For more information about using a static DNS cache, see [Technical Bulletin 36033: Using a Static DNS Cache with SoundPoint IP and SoundStation IP Systems](#).

## Displaying SIP Header Warnings

The warning field from a SIP header may be configured to display a three second pop-up message on the system, for example, that a call transfer failed due to an invalid extension number. For more information, see [Header Support](#).



You can display these pop-up messages in any language supported by the system. The messages will display for three seconds unless overridden by another message or action. To turn the warning display on or off or specify which warnings are displayable, you can configure the parameters in [Displaying SIP Header Warnings](#).

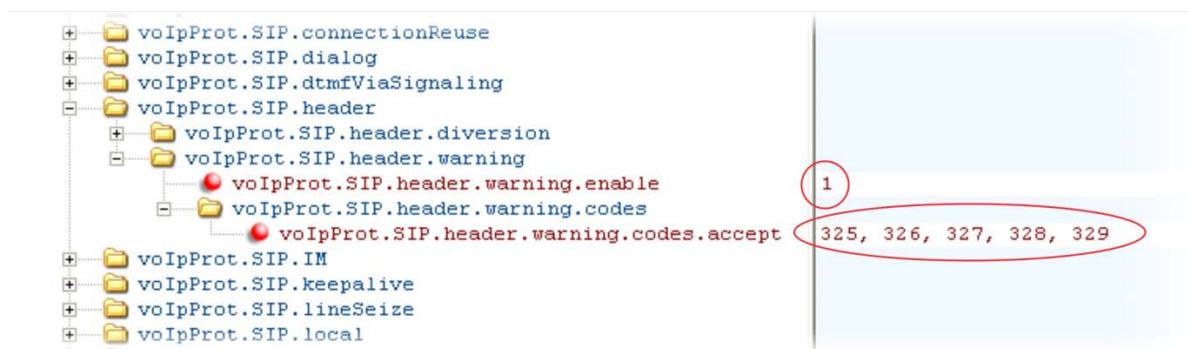
### Displaying SIP Header Warnings

<b>Central Provisioning Server</b>	<code>template &gt; parameter</code>
Turn this feature on or off	<code>sip-interop.cfg &gt; voIpProt.SIP.header.warning.enable</code>
Specify which warnings are displayable	<code>sip-interop.cfg &gt; voIpProt.SIP.header.warning.codes.accept</code>

## Example Display of Warnings from SIP Headers Configuration

To enable the display of warnings from SIP headers, set the `voIpProt.SIP.header.warning.enable` parameter in the `features.cfg` template to 1. Enter the warning codes as a comma-separated string. The strings associated with the values 325 to 329 that display on the system screen, as shown in the next illustration, have been entered automatically by the call server and are not entered by the administrator in the configuration file.

The following illustration shows a sample configuration from the `sip-interop.cfg` template file:



## Quick Setup of the CX5500 System

A Quick Setup feature was added to simplify the process of entering the provisioning (boot) server parameters from the system's user interface. This feature is designed to make it easier for on-site *out of the box* provisioning of the CX5500 system.

When you enable this feature, a **QSetup** soft key will display on the system. When you press the **QSetup** soft key, a new menu will display. The menu enables you to access the provisioning server and quickly configure the system to work. After configuring the Quick Setup, you can disable display of the **QSetup** soft key using a configuration file setting. The table [Quick Setup of the CX5500 System](#) indicates the parameter that enables this feature.

You can enable the Quick Setup feature through the **site.cfg** configuration file or through the system's menu.



#### Web Info: Configuring Quick Setup

For details on how to configure quick setup, see [Technical Bulletin 45460: Using Quick Setup with Polycom Systems](#).

### Quick Setup of the CX5500 System

#### Central Provisioning Server

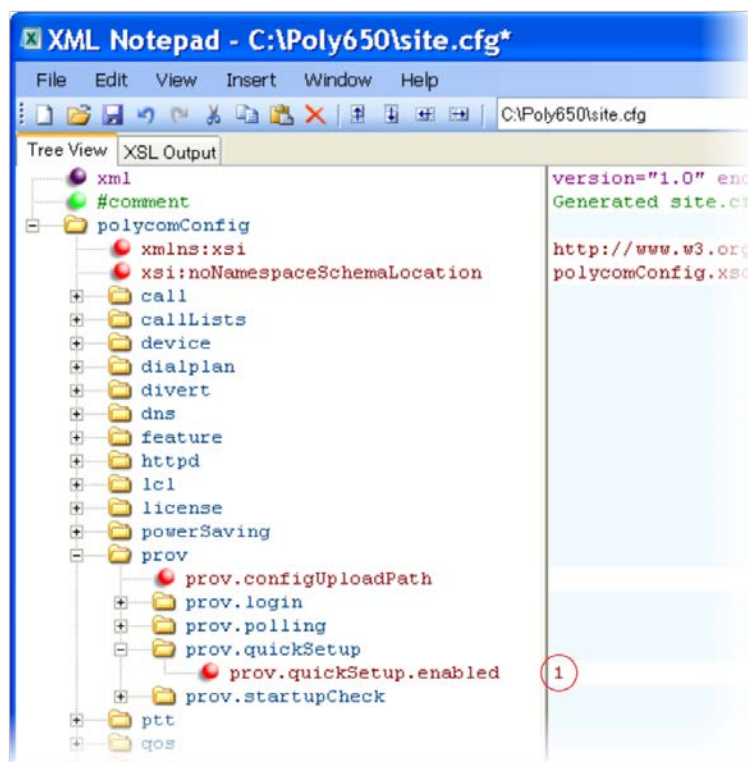
template > parameter

To enable or disable Quick Setup

site.cfg > prov.quickSetup.enabled

## Example Quick Setup Configuration

To enable the Quick Setup feature, enable the `prov.quickSetup.enabled` parameter in the **site.cfg** template file, shown next.



The **QSetup** will display on the system screen. Press the **QSetup** soft key to open the menu and access the quick setup feature.

## Provisional Polling of the CX5500 System

You can configure how your system provisioning automatically by configuring the parameters in the table [Provisional Polling of the CX5500 System](#).

You can set the system's automatic provisioning behavior to be:

- **Absolute** The system polls at the same time every day.
- **Relative** The system polls every x seconds, where x is a number greater than 3600.
- **Random** The system polls randomly based on a time interval you set.
  - If the time period is less than or equal to one day, the first poll is at a random time, x, between the system starting up and the polling period. Afterwards, the system will poll every x seconds.
  - If you set the polling period to be greater than one day with the period rounded up to the nearest day, the system polls on a random day based on the system's MAC address, and within a random time set by the start and end polling time.

For example:

- If `prov.polling.mode` is set to `rel` and `prov.polling.period` is set to `7200`, the system polls every two hours.
- If `prov.polling.mode` is set to `abs` and `prov.polling.timeRandomEnd` is set to `04:00`, the system polls at 4am every day.
- If `prov.polling.mode` is set to `random`, `prov.polling.period` is set to `604800` (7 days), `prov.polling.time` is set to `01:00`, `prov.polling.timeRandomEnd` is set to `05:00`, and you have 25 systems, a random subset of those 25 systems, as determined by the MAC address, will poll randomly between 1am and 5am every day.
- If `prov.polling.mode` is set to `abs` and `prov.polling.period` is set to `2328000`, the system polls every 20 days.

### Provisional Polling of the CX5500 System

---

#### Central Provisioning Server

`template` > [parameter](#)

To enable polling and set the mode, period, time, and time end parameters

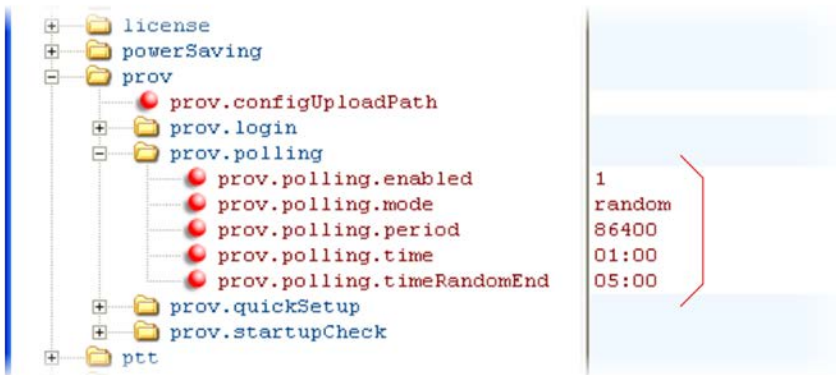
`site.cfg` > [prov.polling.\\*](#)

---



## Example Provisional Polling Configuration

The following illustration shows the default sample random mode configuration for the provisional polling feature in the `site.cfg` template file. In this setup, every system will poll once per day, between 1 and 5 am.



### Tip: Only provision files when polling

If `prov.startupCheck.enabled="0"` then the CX5500 system will not look for the sip.id or the configuration files when they are rebooted, lose power, or restarted. Instead, they will look only when receiving a checksync message, a polling trigger, or a manually started update from the menu or web UI.

Some files such as bitmaps, .wav, the local directory and any custom ringtones will still be downloaded every time as they are stored in RAM and lost with every reboot.

## Set Up Microsoft Lync Server 2010 and 2013

Microsoft® Lync® Server 2010 and 2013 each provide a unified communications (UC) solution that enables customers, colleagues, and business partners to communicate instantly by voice, video, or messaging through a single interface, regardless of their location or network. The following features are available with the CX5500 system registered with Lync Server.

- **Shared Line Appearance** Assign administrative delegates to answer, hold, and transfer calls, set distinct ringtones, and make calls on behalf of Boss lines.
- **Lync Management** Sign in and out of Lync using your login credentials or PIN authentication, set your presence status, manage your Lync contacts, and search for contacts in the Lync directory.
- **Address Book Service (ABS)** Access and search a complete corporate directory.
- **Call Park:** Call park enables you to place a call on a separate line, called a call orbit, where anyone can retrieve the call.

Polycom CX5500 software enables you to register a single system line with Lync Server; you cannot register multiple or shared lines with Lync Server.

The section following, [Registering with Microsoft Lync Server 2010](#), provides an important overview of Polycom provisioning methods and an example configuration to get a system registered with Lync Server.

For details on the user features available on Polycom systems registered with Microsoft Lync Server 2010, see [Feature Profile 72430: Using Polycom® Systems with Microsoft® Lync™ Server 2010](#).

For details on the user features available on Polycom systems registered with Microsoft Lync Server 2010, see [Feature Profile 84538: Using Polycom® VVX® Business Media Systems with Microsoft® Lync™ Server 2013](#).



**Note: You must purchase a license to use Microsoft Lync Server 2010 with the CX5500 System.**

You must purchase a *Lync Feature License* from a Polycom reseller or Polycom sales representative to use Polycom products in a Microsoft Lync environment. You can use the CX5500 system in a Lync environment for trial purposes, without purchasing a license, to a maximum of 30 days.

The concurrent failover/fallback feature explained in [Set Up Server Redundancy](#) is not compatible with Microsoft Lync Server.



**Note: Understanding the Lync Contact List and Your System's Local Contact Directory**

When you are running CX5500 software for use with Lync Server 2010, you have access to two separate contact lists: the default local contact directory on your CX5500 system and a Lync contact list. If you want to disable the local contact directory on your CX5500 system or make it read-only, see [Use the Local Contact Directory](#).

## Register with Microsoft Lync Server 2010

You can register the CX5500 system with Lync Server 2010 in one of three ways:

- Using the Web Configuration Utility
- Using centralized provisioning, which includes a provisioning server and configuration files in XML format.
- From the system user interface



**Note: Registering a System with Lync Server 2010**

For details on using the system user interface and for details on each registration method, including registration instructions, see [Deploying Polycom® UC Software for use with Microsoft® Lync™ Server 2010](#).

## Set the Base Profile to Lync - System User Interface and Web Configuration Utility

You can quickly register systems with the Lync Server by setting the system's Base Profile to *Lync* from the system's user interface or using the Web Configuration Utility. Note that although registering the

system using either of these two methods is simpler than centralized provisioning, each method registers one system at a time. In addition, you cannot enable extensive diagnostic logging that the system writes to the provisioning server, contact directory files, or system user interface language files.

## Centralized Provisioning

You can register multiple systems to Lync Server using a provisioning server and configuration files in XML format. You can provision your systems with Lync Server 2010 using the **lync.cfg** template configuration file included with Polycom CX5500 software. Polycom recommends using this method - also called centralized provisioning - when deploying multiple systems, about twenty or more. A provisioning server enables you to store configuration files in a single location on a server, which simplifies maintenance of feature settings and updates for multiple systems. In addition, use of a provisioning server allows the systems to send diagnostic and other information to files stored on the server, including log files, a contact directory, individual call lists, and multiple languages on the system user interface.

## Ensure Security

The CX5500 systems are computing devices that you must configure for security as you do other computing devices. Polycom strongly recommends that you change the default user name and password on each Polycom device on first deployment. To maximize security, do not leave username and password fields blank. Create user names and passwords of a reasonably long length, and change user names and passwords periodically.

Polycom provides the following ways for you to change the administrative password of a device:

- [Configuration File](#)
- [Web Configuration Utility](#)
- [System User Interface](#)
- [CX5100/CX5500 Control Panel](#)

### Configuration File

Polycom provides configuration files in XML format that you can use to change user names and passwords. You can modify the attached sample configuration file and add it to your file directory, or you can add the parameters and values directly to your existing configuration files. However you use the files or parameters, ensure that you add them to your boot server directory. After you have updated your configuration files, you need to update your device configuration from the device user interface by going to **Settings > Basic > Update Configuration**.



#### Settings: Use a Secure Protocol

Use a secure provisioning protocol such as FTPS or HTTPS to maximize security of user names and passwords.

## Web Configuration Utility

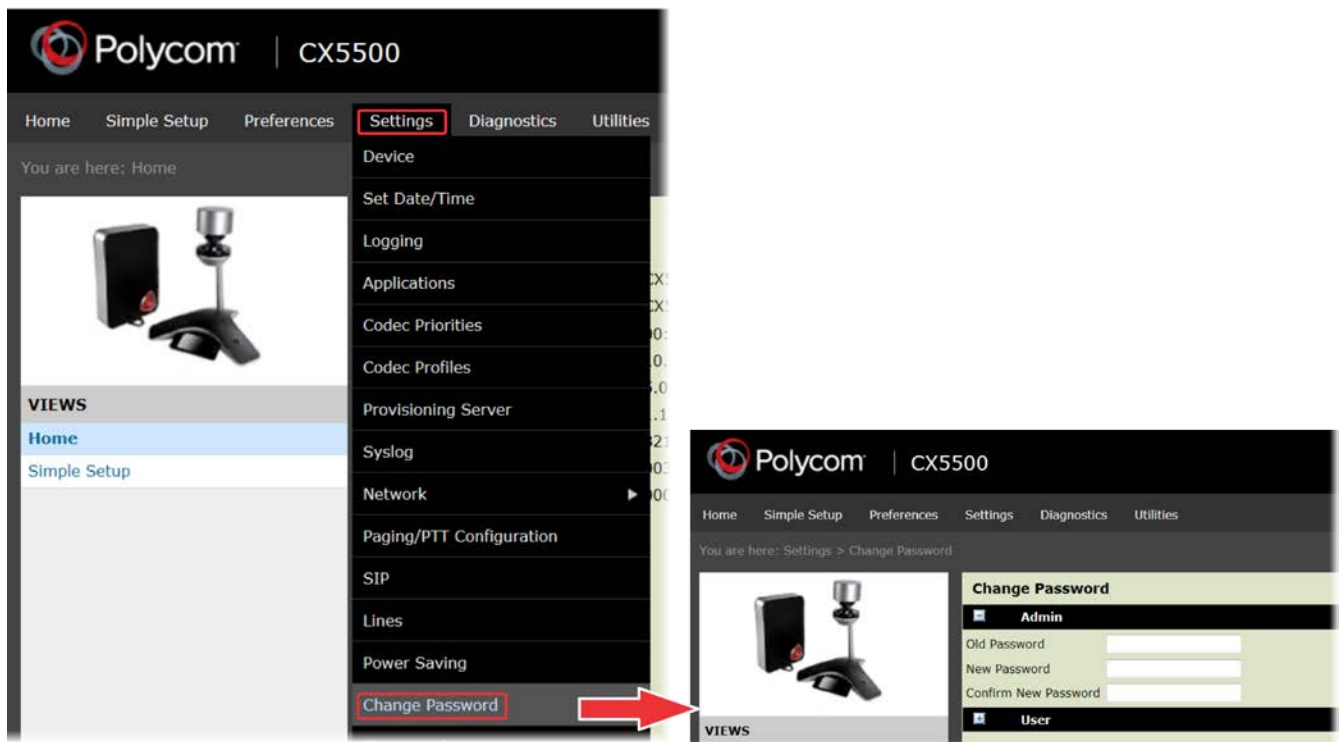
The Web Configuration Utility enables you to configure settings and features on a per-system basis. To access the Web Configuration, enter the IP address of the device to the address bar of your browser. Log in as Admin and enter the default password 456.



### Settings: Use HTTPS

Polycom recommends using the Web Configuration Utility with HTTPS to maximize security.

In the Web Utility, go to **Settings > Change Password** to access settings that change the user name and password, as shown next.



## System User Interface

On your system, select **Settings > Advanced**, enter the default password **456**, and tap **Administration Settings > Change Admin Password**.

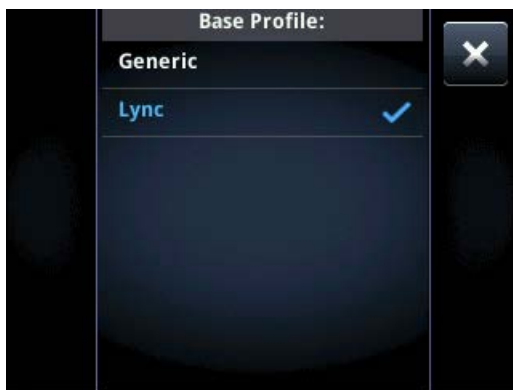
## Example Configuration: Setting the Base Profile to Lync

This example configuration shows you how to set the system's Base Profile to *Lync* using the system's interface. For instructions on all methods you can use to provision CX5500 systems with Lync Server, including tips on how to quickly provision multiple systems to save time, see the Polycom Lync Provisioning Guide.

When you set the system Base Profile to Lync you are provisioning the system with the minimum number of parameters required to register a CX5500 system with Lync Sever 2010. However, if your organization's security procedures don't allow you to enter user IDs and passwords in clear text to configuration files set `reg.x.auth.useLoginCredentials` to 1 and instruct each user to enter their credentials through the system's user interface—the Login Credential screen.

#### To set the Base Profile to Lync:

- 1 Tap **Settings > Advanced**.
- 2 Enter the password (default 456) and press **Enter**.
- 3 Tap **Administration Settings > Network Configuration** and scroll to **Base Profile**.
- 4 In the **Base Profile** menu, select **Lync**, as shown.



The system automatically restarts and displays the Lync Server *Sign In* screen.



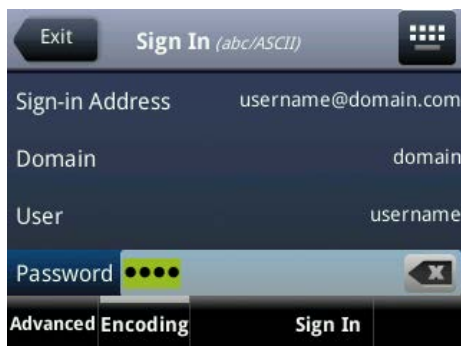
#### Troubleshooting: Rebooting the System

If the system does not restart, you can manually restart by powering off/on the system. You can also manually reboot the system: Tap **Settings > Advanced**, enter the password (default **456**), and choose **Reboot System**. When the system completes the reboot cycle, the Lync Server Sign In screen displays.

#### To sign in and register a line with Lync Server:

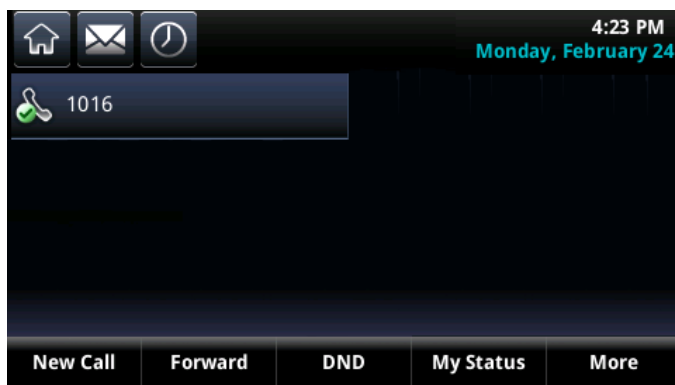
- 1 Enter your sign in credentials in the following formats:
  - **Sign In Address** This is your Lync SIP URI address, not the user name for the Active Directory account. For example, `username@domain.com`.
  - **Domain** By default, use the NetBIOS *domain* name. If that does not work, try the DNS domain name (for example, `domain.com`).
  - **User** username

➤ **Password** password



**2** Select **Sign In**.

The system registers with Lync Server and you can begin using Lync features directly from the system. The following illustration shows a line 1, extension 1016 on the CX5500 system successfully registered to Lync Server.



There are two ways to sign in/out of Lync:

- Tap **Settings > Features > Microsoft Lync > Sign In/Sign Out**.
- Press the **More** soft key and select the **Sign In/Sign Out** soft key.



**Admin Tip: Workaround for Systems using G.722 and Retrieving Microsoft Lync Voicemail**

If your CX5500 systems are configured with G.722 and users find that they do not hear audio when retrieving voicemail from the Microsoft Lync Server, you need to make the following changes to parameters in the site.cfg template file:

Change `voice.codecPref.G7221.24kbps` from 0 to 5.

Change `voice.codecPref.G7221.32kbps` from 5 to 0.

Add `voice.audioProfile.G7221.24kbps.payloadType` and set it to 112.

## Enable Microsoft Exchange Calendar Integration

The CX5500 system can display the Microsoft Exchange 2007 and 2010 calendar. The calendar gives you quick access to meeting information and you can dial in to conference calls. To integrate the Microsoft Exchange Calendar features with your system, configure the parameters in the table [Enable Microsoft Exchange Calendar Integration](#).

You can launch the feature from a calendar icon that displays in Home view or in the Features menu.

You need a valid Microsoft Windows credentials to access the Microsoft Exchange Calendar information on the system. You can manage these credentials through the Login Credentials, which are available through **Settings > Basic > Login Credentials**.

You can view the calendar information in day or month format. The meeting details also display beside the calendar view.

All possible system numbers that you can dial to place a call to the meeting display in the meeting details. You can automatically place a call by pressing a soft key.

A reminder pop-up is displayed 15 minutes before a scheduled meeting. You can dismiss the reminder, select snooze to have the reminder pop up again, open the meeting details view. A tone will be played along with the reminder pop-up.



### Web Info: Using Microsoft Exchange Calendar Integration

For user instructions on how to use calendar integration, refer to the [Polycom CX5500 Unified Conference Station User Guide](#).

### Enable Microsoft Exchange Calendar Integration

Central Provisioning Server	template > parameter
Turn Microsoft Exchange Calendar Integration on or off	features.cfg > feature.exchangeCalendar.enabled
Specify the Microsoft Exchange Server address	applications.cfg > exchange.server.url
Specify the pattern to use to identify system numbers in meeting descriptions	applications.cfg > exchange.meeting.systemPattern
Turn the meeting reminder on or off	applications.cfg > exchange.meeting.reminderEnabled

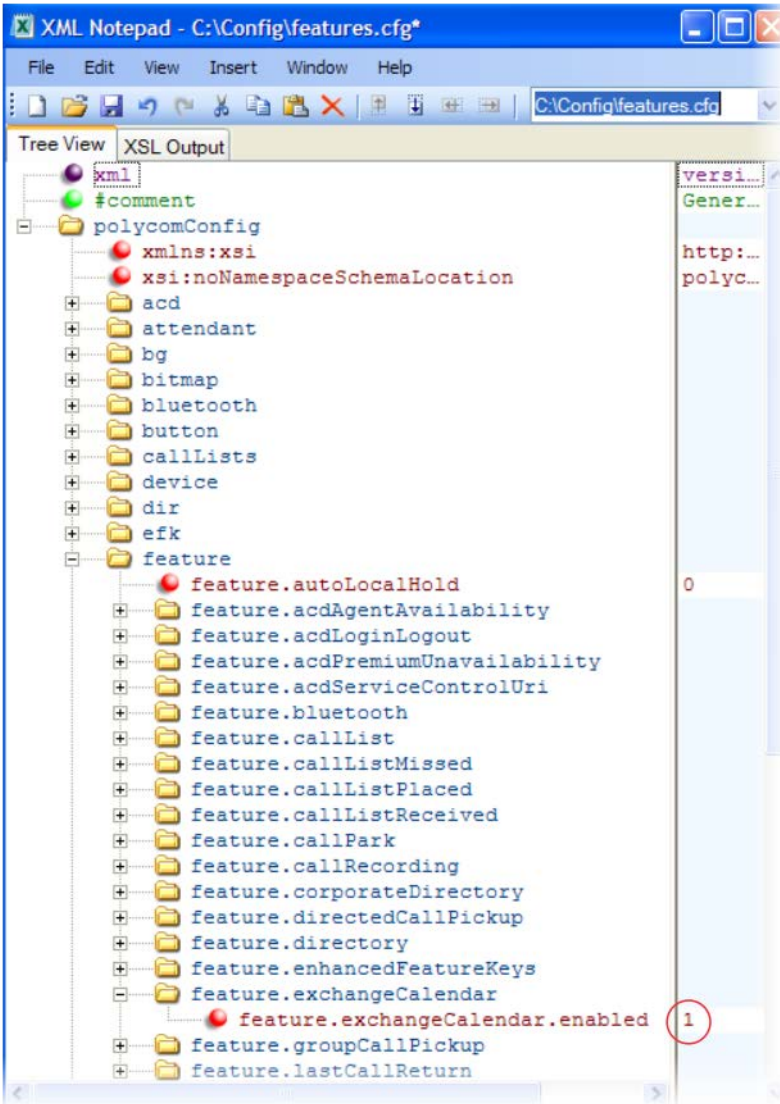
### Web Configuration Utility

To enable Microsoft Exchange Calendar Integration and configure the settings, navigate to **Settings > Applications** and expand **Exchange Applications**.

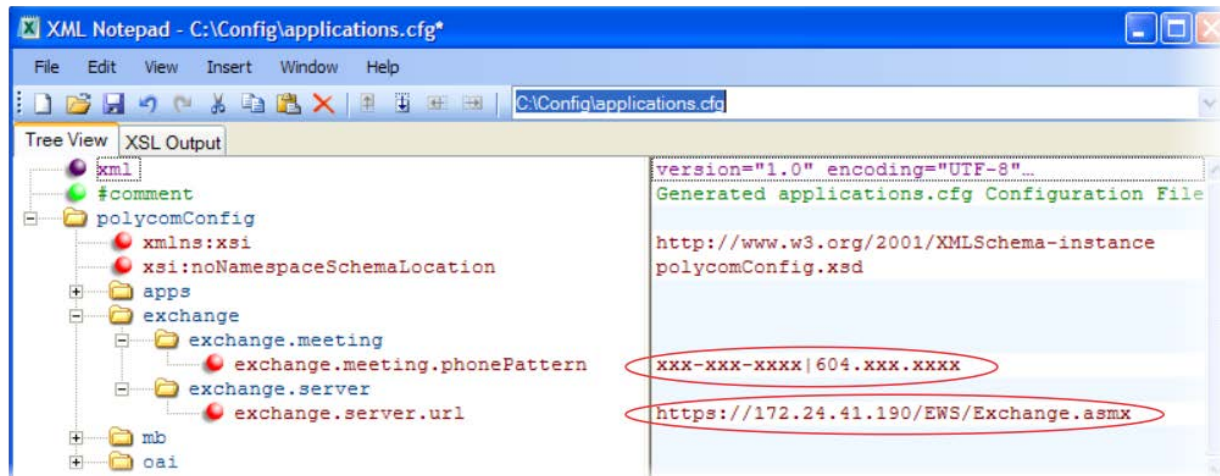


## Example Exchange Calendar Configuration

The following example shows the Calendar feature enabled in **features.cfg**.



After you enable the feature, specify the Microsoft Exchange Server address in **applications.cfg**, as shown next. In this example, a pattern has been specified for meeting numbers. When you specify a pattern, any number in your meeting invitation that matches the pattern will display on a meeting participants' systems as a soft key. Then, participants can press the soft key to dial in to the meeting. You can specify multiple patterns, separated by a bar. In the following example, two patterns are specified.



## Configure Mac OS Support

The CX5500 unified conference station is supported on Microsoft Windows and Mac OS computers. By default, the CX5500 automatically detects the operating system of a connected computer and integrates with the Lync or Skype for Business client. For Mac OS computers connected to CX5500 unified conference station, the active speaker detection overlaid by the panoramic view is supported.



Note: The panoramic view is supported only when the UVC output resolution is 1080p or 720p.

Users can connect a CX5500 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. You can also disable Mac OS support using the parameter `device.local.enableMacSupport`.

**Note: CX5100-CX5500 Control Panel Supports**

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**.

# Set Up System Audio Features

---

After you set up your Polycom® systems on the network, system users can send and receive calls using the default configuration. However, you might consider modifications that optimize the audio quality of your network.

Frequency bandwidth is one of the most critical elements affecting the intelligibility of speech in telephony. The frequency range that the human ear is most sensitive to is far beyond the capabilities of the plain old telephony system (POTS). In fact 80 percent of the frequencies in which speech occurs are not even used by public telephone networks because they only operate from 300Hz to 3.5 kHz.

Complicating the intelligibility of telephony speech in today's world is background noise, variations in environmental reverberation, and communication among persons speaking a variety of native languages. While VoIP technology can broaden the frequency bandwidth and improve sound quality and intelligibility, it can also increase the network load and create a demand for lower raw bit rates. As Audio Codec Specifications shows, Polycom offers systems with a range of codecs, including codecs with high frequency bandwidth and low raw bit rates.

This section describes the audio sound quality features and options you can configure for your CX5500 system. Use these features and options to optimize the conditions of your organization's system network system.

This section shows you how to update your configuration for the following audio-related features:

- [Customize Audio Sound Effects](#) Enables you to customize sound effects associated with incoming calls and other events.
- [Voice Activity Detection](#) Conserves network bandwidth by detecting periods of relative 'silence' in the transmit data path and replacing that silence with special packets that indicate silence is occurring.
- [Generate Dual Tone Multi-Frequency \(DTMF\) Tones](#) Generates dual tone multi-frequency (DTMF) tones in response to user dialing on the dial pad.
- [DTMF Event RTP Payload](#) Conforms to RFC 2833, which describes a standard RTP-compatible technique for conveying DTMF dialing and other telephony events over an RTP media stream.
- [Acoustic Echo Cancellation](#) Employs advanced acoustic echo cancellation for hands-free operation.
- [Audio Codecs](#) Enables access to a wide range of industry standard audio codecs.
- [IP Type-of-Service](#) Enables the setting packet priority.
- [IEEE 802.1p/Q](#) The system may tag all Ethernet packets it transmits with an 802.1Q VLAN header.
- [Voice Quality Monitoring \(VQMon\)](#) Generates various quality metrics including MOS and R-factor for listening and conversational quality. This feature is part of the Productivity Suite

This section also outlines the following built-in audio processing features, which do not require any configuration changes to work:

- [Automatic Gain Control](#) Designed for hands-free operation, this feature boosts the transmit gain of the local user in certain circumstances.
- [Background Noise Suppression](#) Designed primarily for hands-free operation, this feature reduces background noise to enhance communication in noisy environments.

- **Comfort Noise Fill** Provides a consistent noise level to the remote user of a hands-free call.
- **Dynamic Noise Reduction** Provides maximum microphone sensitivity, while automatically reducing background noise. The CX5500 system automatically supports this non-adjustable feature. This feature is also known as Noise Suppression.
- **Jitter Buffer and Packet Error Concealment** Employs a high-performance jitter buffer and packet error concealment system designed to mitigate packet inter-arrival jitter, and out-of-order, lost, or delayed packets.
- **Low-Delay Audio Packet Transmission** Minimizes latency for audio packet transmission.

## Customize Audio Sound Effects

You can customize the audio sound effects that are used for incoming calls and other alerts using synthesized tones or sampled audio files. You can replace the default sampled audio files with your own custom **.wav** audio file format. The system supports the following **.wav** audio file formats:

- mono G.711 (13-bit dynamic range, 8-khz sample rate)
- mono L16/16000 (16-bit dynamic range, 16-kHz sample rate)
- mono L16/32000 (16-bit dynamic range, 32-kHz sample rate)
- mono L16/44100 (16-bit dynamic range, 44.1 kHz sample rate)
- mono L16/48000 (16-bit dynamic range, 48-kHz sample rate)



### Note: Supported Audio Formats

The L16/32000 and L16/48000 wav formats are supported only on the CX5500 system.

Your custom sampled audio files must be available at the path or URL specified by `saf.x` in the table [Customize Audio Sound Effects](#) so the system can download them. Include the name of the file and the **.wav** extension in the path.

### Customize Audio Sound Effects

#### Central Provisioning Server

**template** > [parameter](#)

Specify a path or URL for the system to download a custom audio file

**site.cfg** > [saf.x](#)

Specify the name, type, and value for a custom sound effect

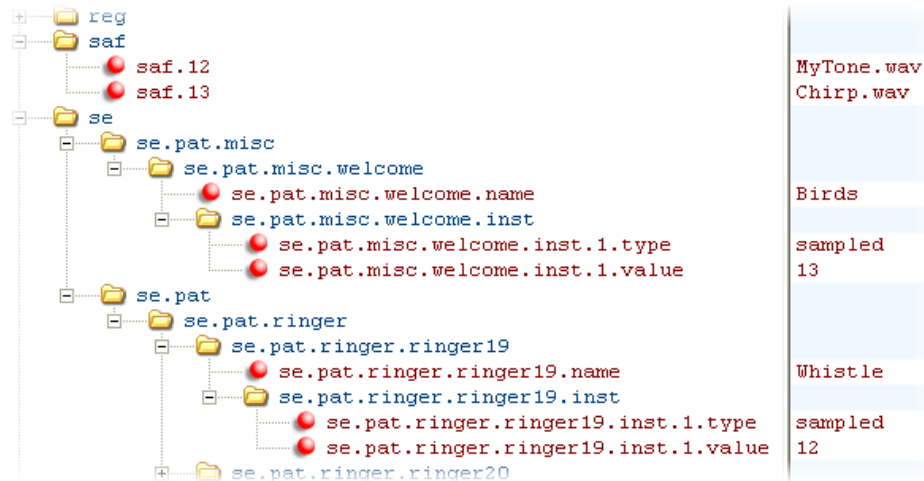
**region.cfg** > [se.pat.\\*](#)

#### Web Configuration Utility

To add, play, or delete a custom audio file, navigate to **Settings > Basic > Preferences > Ringtones** and expand the **Custom Audio Files** menu.

## Example Configuration

The following example configuration illustrates how to add a custom sound effect from a sampled audio file. In the example, the custom audio files `MyTone.wav` and `Chirp.wav` have been added as sound effects 12 and 13. The `welcome` sound has been customized to use the sampled audio file 13 (`Chirp.wav`) with the label `Birds`. Ringtone 19 is named `Whistle` and is configured to use sampled audio file 12 (`MyTone.wav`).



## Voice Activity Detection

The purpose of voice activity detection is to detect periods of silence in the transmit data path so the system doesn't have to transmit unnecessary data packets for outgoing audio. This process conserves network bandwidth. The VAD parameters in the table [Voice Activity Detection \(VAD\)](#) will help you set up this feature. For compression algorithms without an inherent VAD function, such as G.711, the system uses the codec-independent comfort noise transmission processing specified in RFC 3389. The RFC 3389 algorithm is derived from G.711 Appendix II, which defines a comfort noise (CN) payload format (or bit-stream) for G.711 use in packet-based, multimedia communication systems. The system generates CN packets—also known as Silence Insertion Descriptor (SID) frames—and also decodes CN packets, to efficiently regenerate a facsimile of the background noise at the remote end.

### Voice Activity Detection (VAD)

Central Provisioning Server	template > parameter
Specify if G.729 Annex B should be signaled	site.cfg > <a href="#">voice.vad.signalAnnexB</a>
Enable or disable voice activity detection	site.cfg > <a href="#">voice.vadEnable</a>
Specify the threshold between active voices and background voices	site.cfg > <a href="#">voice.vadThresh</a>

## Generate Dual Tone Multi-Frequency (DTMF) Tones

The system generates dual tone multi-frequency (DTMF) tones in response to user dialing on the dial pad. Use the parameters in the table [Dual Tone Multi-Frequency \(DTMF\) Tone Generation](#) to set up this feature. These tones, commonly referred to as *touch tones*, are transmitted in the real-time transport protocol (RTP) streams of connected calls. The system can encode the DTMF tones using the active voice codec or using RFC 2833-compatible encoding. The coding format decision is based on the capabilities of the remote endpoint.

### Dual Tone Multi-Frequency (DTMF) Tone Generation

Central Provisioning Server	template > parameter
Specify if DTMF tones should be played through the speaker system	sip-interop.cfg > <a href="#">tone.dtmf.chassis.masking</a>
Specify the frequency level of DTMF digits	sip-interop.cfg > <a href="#">tone.dtmf.level</a>
Specify how long the system should wait between DTMF digits	sip-interop.cfg > <a href="#">tone.dtmf.onTime</a>
Specify how long the system should play each DTMF tone for	sip-interop.cfg > <a href="#">tone.dtmf.onTime</a>
Enable or disable DTMF encoding in an RTP stream	sip-interop.cfg > <a href="#">tone.dtmf.viaRtp</a>

## DTMF Event RTP Payload

The system is compatible with *RFC 2833—RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals*. RFC 2833 describes a standard RTP-compatible technique for conveying DTMF dialing and other telephony events over an RTP media stream. The system generates RFC 2833 (DTMF only) events but does not regenerate—or otherwise use—DTMF events received from the remote end of the call. Use the parameters in the table [DTMF Event RTP Payload](#) to set up this feature.

### DTMF Event RTP Payload

Central Provisioning Server	template > parameter
Specify if the system will use RFC 2833 to encode DTMF	sip-interop.cfg > <a href="#">tone.dtmf.rfc2833Control</a>
Specify the system-event payload encoding in the dynamic range to be used in SDP offers	sip-interop.cfg > <a href="#">tone.dtmf.rfc2833Payload</a>

## Acoustic Echo Cancellation

Your CX5500 system uses advanced acoustic echo cancellation (AEC). See the table [Audio Codecs Supported on the CX5500 System](#) for a list of audio codecs available for the CX5500 system and their priority. The system uses both linear and non-linear techniques to aggressively reduce echo while permitting natural, full-duplex communication patterns.



**Caution: Contact Polycom Support Before Modifying Acoustic Echo Cancellation Parameters**

Consult [Polycom Support](#) before you make changes to any acoustic echo cancellation parameters.

## Audio Codecs

The following table lists the audio codecs supported on the CX500 system.

### Audio Codecs Supported on the CX5500 System

<i>Codec</i>	<i>Priority</i>
G.722.1C.48kbps	2
G.722.1C.32kbps	0
G.722.1C.24kbps	0
Siren14.48kbps	3
Siren14.32kbps	0
Siren14.24kbps	0
G.722.1.32kbps	5
G.722.1.24kbps	0
G.722.1.16kbps	0
G.719.64kbps	0
G.719.48kbps	0
G.719.32kbps	0
G.722	4
G.711Mu	6
G.711A	7
G.729AB	8
Lin16.48ksps	0
Lin16.44.1ksps	0
Lin16.32ksps	0

<i>Codec</i>	<i>Priority</i>
Lin16.16ksps	0
Lin16.8ksps	0

The following table summarizes the audio codecs supported on the CX5500 system:

#### Audio Codec Specifications

<i>Algorithm</i>	<i>Reference</i>	<i>Raw Bit Rate</i>	<i>IP Bit Rate</i>	<i>Sample Rate</i>	<i>Default Payload Size</i>	<i>Effective Audio Bandwidth</i>
G.719	RFC 5404	32 Kbps 48 Kbps 64 Kbps	48 Kbps 64 Kbps 80 Kbps	48 Ksps	20 ms	20 KHz
G.711	RFC 1890	64 Kbps	80 Kbps	16 Ksps	20 ms	7 KHz
G.722.1	RFC 3047	16 Kbps 24 Kbps 32 Kbps	32 Kbps 40 Kbps 48 Kbps	16 Ksps	20 ms	7 KHz
G.722.1C	G7221C	224 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 Ksps	20 ms	14 KHz
G.729AB	RFC 1890	8 Kbps	24 Kbps	8 Ksps	20 ms	3.5 KHz
Lin16	RFC 1890	128 Kbps 256 Kbps 512 Kbps 705.6 Kbps 768 Kbps	132 Kbps 260 Kbps 516 Kbps 709.6 Kbps 772 Kbps	8 Ksps 16 Ksps 32 Ksps 44.1 Ksps 48 Ksps	10 ms	3.5 KHz 7 KHz 14 KHz 20 KHz 22 KHz
Siren14	SIREN14	24 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 Ksps	20 ms	14 KHz



#### Note: Network Bandwidth Requirements for Encoded Voice

The network bandwidth necessary to send the encoded voice is typically 5–10% higher than the encoded bit rate due to packetization overhead. For example, a G.722.1C call at 48 kbps for both the receive and transmit signals consumes about 100 kbps of network bandwidth (two-way audio).

Use parameters in the following table to specify the priority for audio codecs.

### Audio Codec Priorities

#### Central Provisioning Server

**template** > [parameter](#)

To specify the priority for a codec

**site.cfg** > [voice.codecPref.<nameOfCodec>](#)

#### Web Configuration Utility

To enable or disable codecs and specify codec priority, navigate to **Settings > Codec Profiles** and expand the **Audio Priority** menu.

## IP Type-of-Service

The *type-of-service* field in an IP packet header consists of four type-of-service (TOS) bits and a 3-bit precedence field. See the following table for available parameters. Each TOS bit can be set to either 0 or 1. The precedence field can be set to a value from 0 through 7. The type of service can be configured specifically for RTP packets and call control packets, such as SIP signaling packets.

### IP Type-of-Service (ToS)

#### Central Provisioning Server

**template** > [parameter](#)

Set the IP header bits for call control

**site.cfg** > [qos.ip.callControl.\\*](#)

Set the IP header bits for RTP

**site.cfg** > [qos.ip.rtp.\\*](#)

Set the IP header bits for RTP video

**site.cfg** > [qos.ip.rtp.video.\\*](#)

#### Web Configuration Utility

Set the QoS IP settings by navigating to **Settings > Network > QoS**.

## IEEE 802.1p/Q

The system will tag all Ethernet packets it transmits with an 802.1Q VLAN header when:

- A valid VLAN ID specified in the system's network configuration.
- The system is instructed to tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch.
- A VLAN ID is obtained from DHCP or LLDP (see DHCP Menu).

Use the following table to set values. The 802.1p/Q *user\_priority* field can be set to a value from 0 to 7. The *user\_priority* can be configured specifically for RTP packets and call control packets, such as SIP signaling packets, with default settings configurable for all other packets.

---

**IEEE 802.1p/Q**

---

**Central Provisioning Server****template** > [parameter](#)

Set the user priority for packets without a per-packet protocol setting (including 802.1p/Q)

**site.cfg** > [qos.ethernet.other.user\\_priority](#)

---

**Web Configuration Utility**To set the user priority for 802.1p/Q packets, navigate to **Settings > Network > QoS** and expand the **Other Protocols** menu.

---

## Voice Quality Monitoring (VQMon)

You can configure the systems to generate various quality metrics you can use to monitor sound and listening quality. These metrics can be sent between the systems in RTCP XR packets, which are compliant with [RFC 3611—RTP Control Extended Reports \(RTCP XR\)](#). The packets are sent to a report collector as specified in draft RFC [draft-ietf\\_sipping\\_rtcp-summary-02](#). The metrics can also be sent as SIP PUBLISH messages to a central voice quality report collector.

A license key is required to activate the VQMon feature on all systems. For more information on VQMon, contact your Certified Polycom Reseller.

You can enable three types of voice quality reports:

- **Alert** Generated when the call quality degrades below a configurable threshold.
- **Periodic** Generated during a call at a configurable period.
- **Session** Generated at the end of a call.

You can generate a wide range of performance metrics, the parameters for which are shown in the following table. Some are based on current values, such as jitter buffer nominal delay and round trip delay, while others cover the time period from the beginning of the call until the report is sent, such as network packet loss. Some metrics are computed using other metrics as input, such as listening Mean Opinion Score (MOS), conversational MOS, listening R-factor, and conversational R-factor.

**Voice Quality Monitoring (VQM)**

---

**Central Provisioning Server****template** > [parameter](#)

Specify the warning threshold for alerts

**features.cfg** > [voice.qualityMonitoring.collector.alert.\\*](#)

Enable the generation of quality reports

**features.cfg** > [voice.qualityMonitoring.collector.enable.\\*](#)

Specify the server address and port

**features.cfg** > [voice.qualityMonitoring.collector.server.x.\\*](#)

Enable the generation of RTCP-XR packets

**features.cfg** > [voice.qualityMonitoring.rtcpxr.enable](#)

---

---

## **Built-In Audio Processing Features**

Your CX5500 system has the following built-in audio processing features: automatic gain control, background noise suppression, comfort noise fill, dynamic noise reduction, jitter buffer and packet error concealment, and low delay audio packet transmission. These features work automatically, without configuration changes.

### ***Automatic Gain Control***

Automatic Gain Control (AGC) is applicable to hands-free operation and is used to boost the transmit gain of the local talker in certain circumstances. This increases the effective user-system radius and helps with the intelligibility of soft-talkers.

### ***Background Noise Suppression***

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

### ***Comfort Noise Fill***

Comfort noise fill is designed to help provide a consistent noise level to the remote user of a hands-free call. Fluctuations in perceived background noise levels are an undesirable side effect of the non-linear component of most AEC systems. This feature uses noise synthesis techniques to smooth out the noise level in the direction toward the remote user, providing a more natural call experience.

### ***Dynamic Noise Reduction***

Dynamic noise reduction (DNR) provides maximum microphone sensitivity, while automatically reducing background noise— from fans, projectors, heating and air conditioning—for clearer sound and more efficient conferencing.

### ***Jitter Buffer and Packet Error Concealment***

The system employs a high-performance jitter buffer and packet error concealment system designed to mitigate packet inter-arrival jitter and out-of-order, or lost or delayed (by the network) packets. The jitter buffer is adaptive and configurable for different network environments. When packets are lost, a concealment algorithm minimizes the resulting negative audio consequences.

### ***Low-Delay Audio Packet Transmission***

The system is designed to minimize latency for audio packet transmission.

# Set Up User and System Security Features

---

After you set up your CX5500 system on your network with the default configuration, users can place and answer calls. Polycom's Open SIP UC software enables you to make custom configurations to optimize security settings.

This section shows you how to update your configuration for the following security features:

- [Local User and Administrator Passwords](#) Several local settings menus are protected with two privilege levels—user and administrator—each with its own password.
- [Incoming Signaling Validation](#) Levels of security are provided for validating incoming network signaling.
- [Configuration File Encryption](#) Confidential information stored in configuration files can be protected (encrypted). The system can recognize encrypted files, which it downloads from the provisioning server, and it can encrypt files before uploading them to the provisioning server.
- [Digital Certificates](#) The CX5500 system supports digital certificates and associated private keys.
- [Generate a Certificate Signing Request](#) Create a request to obtain a device certificate.
- [TLS Profiles](#) Configure your system with a profile that specifies trusted digital certificates. You can also install and specify custom certificates.
- [Support Mutual TLS Authentication](#) Support system authentication of the server and server authentication of the system.
- [Configurable TLS Cipher Suites](#) Control which of cipher suites will be offered/accepted during TLS session negotiation.
- [Secure Real-Time Transport Protocol](#) Encrypting audio streams to avoid interception and eavesdropping. Encrypting audio streams to avoid interception and eavesdropping.
- [Lock the System](#) Prevent access to the system menu and to key presses.
- [Support 802.1X Authentication](#) Authenticate devices connecting to a local area network (LAN) or a wireless local area network (WLAN).
- [Set User Profiles](#) Access your personal system settings from any system in your organization's network.

## Local User and Administrator Passwords

Several local settings menus are protected with user and administrator passwords. The system will prompt you for a user or administrator password before you can access certain menu options. If the system requires the administrator password, you may be able to use the user password, but you will be presented with limited menu options. If the system prompts you for the user password, you may use the administrator password (you will see the same menus as the user). The Web Configuration Utility is protected by the user and administrator password and displays different features and options depending on which password you use. The default user password is **123** and the default administrator password is **456**. You should change the administrator password from the default value. You may want to change the user password for security reasons, see the following table for all parameters.

---

## Local User and Administrator Password Settings

### Central Provisioning Server

	<a href="#">template</a> > <a href="#">parameter</a>
Set the minimum length for the administrator password	<a href="#">site.cfg</a> > <a href="#">sec.pwd.length.admin</a>
Set the minimum length for the user password	<a href="#">site.cfg</a> > <a href="#">sec.pwd.length.user</a>
Set the system's local administrator password	<a href="#">device.cfg</a> > <a href="#">device.auth.localAdminPassword</a>
Set the system's local user password	<a href="#">device.cfg</a> > <a href="#">device.auth.localUserPassword</a>

### Web Configuration Utility

To change the user or administrator password, navigate to **Settings > Change Password**. To change the administrator password, you must log in to the Web configuration utility as an administrator.

### Local System User Interface

To change the administrator password, navigate to **Settings > Advanced**, enter the current administrator password, and select **Admin Settings > Change Admin Password**.  
To change the User Password, navigate to **Settings > Advanced**, enter the current user or administrator password, and select **Change User Password**.

---

## Incoming Signaling Validation

You can choose from three optional levels of security for validating incoming network signaling:

- Source IP address validation
- Digest authentication
- Source IP address validation and digest authentication

See the following table for the parameters that specify the validation type, method, and the events you want to validate.

### Incoming Signal Validation Parameters

#### Central Provisioning Server

	<a href="#">template</a> > <a href="#">parameter</a>
Specify what type of validation to perform	<a href="#">sip-interop.cfg</a> > <a href="#">volp.SIP.requestValidation.x.method</a>
Set the name of the method for which validation will be applied	<a href="#">sip-interop.cfg</a> > <a href="#">volp.SIP.requestValidation.x.request</a>
Determine which events within the Event header should be validated	<a href="#">sip-interop.cfg</a> > <a href="#">volp.SIP.requestValidation.x.request.y.event</a>

---



## Configuration File Encryption

You can encrypt configuration files, contact directories, and configuration override files can all be encrypted. Note that you cannot encrypt the master configuration file.

You can determine whether encrypted files are the same as unencrypted files and use the SDK to facilitate key generation. Use the following table to configure the parameters used to encrypt files. For more information about encrypting configuration files, see [Encrypting Configuration Files](#).

### Configuration File Encryption Parameters

Central Provisioning Server	template > parameter
Specify if configuration files uploaded from the system to the provisioning server should be encrypted	site.cfg > <a href="#">sec.encryption.upload.config</a>
Specify if the contact directory is encrypted when it is uploaded from the system to the provisioning server	site.cfg > <a href="#">sec.encryption.upload.dir</a>
Specify if the configuration overrides file should be encrypted when it is uploaded from the system to the server	site.cfg > <a href="#">sec.encryption.upload.overrides</a>
Specify an encryption key so the system can download encrypted files from the provisioning server	device.cfg > <a href="#">device.sec.configEncryption.key</a>

## Digital Certificates

You can download the Polycom Root CA from <http://pki.polycom.com/>. The certificate is set to expire on March 9, 2044.



### Web Info: Digital Certificates on Polycom Systems

For details on installing digital credentials on all systems, see [Feature Profile 37148: Device Certificates on Polycom SoundPoint IP, SoundStation IP, and VVX Systems](#).

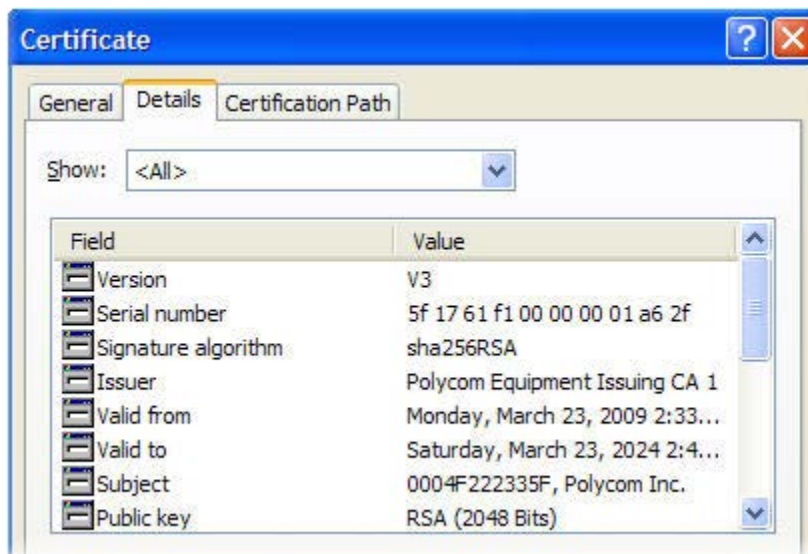
Polycom uses the X.509 standard, which defines what information can go into a certificate. An X.509 digital certificate is a digitally signed statement. All X.509 certificates have the following fields, in addition to the signature:

- **Version** This identifies which version of the X.509 standard applies to this certificate, which in turn affects what information can be specified in the certificate.
- **Serial Number** The entity that created the certificate is responsible for assigning it a serial number to distinguish it from other certificates it issues.
- **Signature Algorithm Identifier** This identifies the algorithm used by the Certificate Authority (CA) to sign the certificate.
- **Issuer Name** The X.500 name of the entity that signed the certificate. This is normally a CA. Using this certificate means trusting the entity that signed this certificate.

- **Validity Period** Each certificate is valid for a limited amount of time. This period is described by a start date and time and an end date and time, and can be as short as a few seconds or almost as long as a century.
- **Subject Name** The name of the entity whose public key the certificate identifies. This name uses the X.500 standard, so it is intended to be unique across the Internet.
- **Subject Public Key Information** This is the public key of the entity being named, together with an algorithm identifier that specifies to which public key cryptographic system this key belongs and any associated key parameters.

Polycom supports the use of Subject Alternative Names (SAN) with TLS security certificates. Polycom does not support the use of the asterisk (\*) or wildcard characters in the Common Name field of a Certificate Authority's public certificate. If you want to enter multiple hostnames or IP addresses on the same certificate, use the SAN field.

The following is an example of a Polycom device certificate when viewed in a browser.



The device certificate and associated private key are stored on the system in its non-volatile memory as part of the manufacturing process. For more information on digital certificates, see [Public Key Infrastructure \(X.509\)](#) and [RFC 2459: Internet X.509 Public Key Infrastructure](#).



#### Web Info: Using Custom Device Certificates With Polycom Systems

As of UC Software 4.0.0, you can install custom device certificates on your Polycom systems. These certificates are installed in the same way custom CA certificates are installed. See [Technical Bulletin 17877: Using Custom Certificates With Polycom Systems](#).

**To determine if there is a device certificate on a CX5500 system:**

- 1 Tap **Settings > Advanced > Admin Settings > TLS Security > Custom Device Certificates**.  
You can view the Polycom device certificate on the system at **Settings > Status > Platform > System**.

## 2 Tap the **Info** soft key to view the certificate.

One of the following messages will be displayed:

- **Device Certificate: Installed** or **Device Certificate: Factory Installed** is displayed if the certificate is available in flash memory, all the certificate fields are valid (listed above), and the certificate has not expired.
- **Device Certificate: Not Installed** is displayed if the certificate is not available in flash memory (or the flash memory location where the device certificate is to be stored is blank).
- **Device Certificate: Invalid** is displayed if the certificate is not valid.



### **Note: Device Certificate Shown as Self-Signed**

Some Polycom systems manufactured after December, 2011 report the device certificate as 'self-signed' and not as 'Factory Installed'. The difference indicates that different issuing CAs were used to generate the certificates. As long as the authenticating server trusts the Polycom Root CA that issued these certificates, the systems will operate correctly.

## Generate a Certificate Signing Request

You may need a certificate to perform a number of tasks, for example, multiple TLS authentication. To obtain a certificate you need to:

- Request a certificate from a Certificate Authority (CA) by creating a certificate signing request (CSR).
- Forward the CSR to a CA to create a certificate. If your organization doesn't have its own CA, you will need to forward the CSR to a company like Symantec. If successful, the CA will send back a certificate that has been digitally signed with their private key.

After you receive the certificate, you can download it to the system:

- Using a configuration file
- Through the system's user interface
- Through the Web Configurable Utility

**To generate a certificate signing request on a CX5500 system:**

- 1 Navigate to **Settings > Advanced > Admin Settings > Generate CSR**.
- 1 When prompted, enter the administrative password and press the **Enter** soft key. The default administrative password is **456**.
- 2 From the **Generate CSR Screen**, fill in the **Common Name** field - the Organization, Email Address, Country, and State fields are optional.

The following figure shows the Generate CSR screen.



The screenshot shows a mobile application interface for generating a Certificate Signing Request (CSR). The title bar at the top reads "Generate CSR (Abc/ASCII)" and includes a "Back" button on the left and a menu icon on the right. The form contains the following fields:

- Common Name:** user.polycom.com
- Organization:** Polycom
- Email Address:** john@polycom.com
- Country:** US

At the bottom of the screen, there are two buttons: "Encode" and "Generate".

### 3 Press **Generate**.

A message *CSR generation completed* displays on the system's screen. The MAC.csr (certificate request) and MAC-private.pem (private key) are uploaded to the system's provisioning server.

## Configure TLS Profiles

The Transport Layer Security (TLS) profiles describe a collection of custom CA and device certificates installed on the CX5500 systems and the features where these certificates are used for authentication.

Your system can trust certificates issued by widely recognized certificate authorities when trying to establish a connection to a provisioning server for application provisioning. There are a number of parameters you can use to configure TLS Profiles listed in [TLS Platform Profile and TLS Application Profile Parameters](#). For the complete list of trusted Certificate Authorities, see [Trusted Certificate Authority List](#).

Custom CA and device certificates can be added to the system and set up to be used by different features. For example, the system's factory-installed or custom device certificate could be used for authentication when system provisioning is performed by an HTTPS server. A custom CA certificate could also be used when accessing content through the microbrowser or browser.

Once you install certificates on the system, you can determine which TLS Platform Profiles or TLS Application Profiles will use these certificates. By default, TLS Platform Profile 1 uses every CA certificate and the default device certificate. Also, each TLS Application uses TLS Platform Profile 1 as the default profile. You can quickly apply a CA certificate to all TLS Applications by installing it on the system and keeping the default TLS Profile and default TLS Application values.

Lastly you must choose which TLS platform profile or application profile will be used for each TLS Application. The profiles can be used for system provisioning, with the applications running on the microbrowser and browser, and for 802.1X, LDAP, and SIP authentication. Some applications, such as Syslog, can only use a TLS Platform Profile, not a TLS Application Profile. See [<TLS/>](#) for the list of applications.

For more information on device (or digital) certificates installed on the systems at the factory, see [Digital Certificates](#).



### Web Info: Using Custom CA Certificates

For more information on using custom certificates, see [Technical Bulletin 17877: Using Custom Certificates With Polycom Systems](#).

The following table shows parameters for TLS Platform Profile 1. To configure TLS Platform Profile 2, use a 2 at the end of the parameter instead of a 1. For example, set `device.sec.TLS.profile.caCertList2` instead of `.caCertList1`.

### TLS Platform Profile and TLS Application Profile Parameters

#### Central Provisioning Server

**template** > [parameter](#)

**TLS Platform Profile Parameters** (use 2 at the end of each parameter (instead of 1) to set up platform profile 2)

Specify which CA certificates to use

**device.cfg** >  
[device.sec.TLS.profile.caCertList1](#)

Specify the cipher suite

**device.cfg** >  
[device.sec.TLS.profile.cipherSuite1](#)

Select the default cipher suite or a custom cipher suite

**device.cfg** >  
[device.sec.TLS.profile.cipherSuiteDefault1](#)

Specify a custom certificate

**device.cfg** >  
[device.sec.TLS.customCaCert1](#)

Specify which device certificates to use

**device.cfg** >  
[device.sec.TLS.profile.deviceCert1](#)

#### TLS Application Profile Parameters

Specify which CA certificates to use

**site.cfg** > [sec.TLS.profile.x.caCert.\\*](#)

Specify the cipher suite

**site.cfg** > [sec.TLS.profile.x.cipherSuite](#)

Select the default cipher suite or a custom cipher suite

**site.cfg**  
> [sec.TLS.profile.x.cipherSuiteDefault](#)

Specify a custom certificate

**site.cfg** > [sec.TLS.customCaCert.x](#)

Specify which device certificates to use

**site.cfg** > [sec.TLS.profile.x.deviceCert](#)

Specify the custom device key

**site.cfg** > [sec.TLS.customDeviceKey.x](#)

#### Web Configuration Utility

To install CA or device certificates and configure TLS profiles, navigate to **Settings > Network > TLS** and expand the **Certificate Configuration** and **TLS Profiles** menus.

#### Local System User Interface

To install a CA or device certificate, navigate to **Settings > Advanced > Admin Settings > TLS Security** and select **Custom CA Certificates** or **Custom Device Credentials** and enter the URL of a custom certificate or PEM-encoded certificate.

Once you have configured the certificates, configure a TLS profile. To configure TLS profiles, navigate to **Settings > Advanced > Admin Settings > TLS Security > Configure TLS Profiles**. Select the profile that you would like to configure, and configure the cipher suite, choose which CA certificates to use, and choose which device

---

certificates to use. The menu options are: Configure Cipher Suite, CA Certificates, and Device Certificates.

---

This section provides detailed information on:

- [Download Certificates to a CX5500 System](#)
- [Set TLS Profiles](#)

## Download Certificates to a CX5500 System

You can download certificates to a CX5500 system by specifying a URL where the certificate is currently stored. You can install up to eight CA certificates and eight device certificates on the system. You can refresh certificates when they expire or are revoked. You can delete any CA certificate or device certificate that you install.



### Note: Maximum Size for Certificates

The maximum certificate size on Platform CA1 is 1536KB and 4KB for Platform CA2.

### To download a certificate to a CX5500 system:

- 1 Navigate to **Settings > Advanced > Administrative Settings > TLS Security** and select **Custom CA Certificates** or **Custom Device Certificates**.

When prompted, enter the administrative password and tap the **Enter** soft key. The default administrative password is **456**.

- 2 Select the **Install** soft key.
- 3 Enter the URL where the certificate is stored.

For example, *http://bootserver1.vancouver.polycom.com/ca.crt*

- 4 Select the **Enter** soft key.

The certificate is downloaded. The certificate's MD5 fingerprint displays to verify that the correct certificate is to be installed.

- 5 Select the **Accept** soft key.

The certificate is installed successfully.

The appropriate certificate menu displays the certificate's common name.

## Set TLS Profiles

By default, all Polycom-installed profiles are associated with the default cipher suite and use trusted and widely recognized CA certificates for authentication. Use the following table to set parameters. You can change the cipher suite, CA certificates, and device certificates for the two platform profiles and the six application profiles. You can then map profiles directly to the features that use certificates.

---

## Set a TLS Profile for each TLS Application

---

### Central Provisioning Server

**template** > [parameter](#)

Specify the TLS profile to use for each application (802.1X and Provisioning)

**device.cfg** > [device.sec.TLS.profileSelection.\\*](#)

Specify the TLS profile to use for each application (other applications)

**device.cfg** > [sec.TLS.profileSelection.\\*](#)

---

### Web Configuration Utility

To specify the TLS profile to use for a specific application, navigate to **Settings > Network > TLS**, and expand the **TLS Applications** menu.

---

### Local System User Interface

To specify the TLS profile to use for a specific application, navigate to **Settings > Advanced > Admin Settings > TLS Security > TLS Applications**, select the **TLS application**, and choose a **TLS Profile** to use.

---

## Support Mutual TLS Authentication

Mutual Transport Layer Security (TLS) authentication is a process in which both entities in a communications link authenticate each other. In a network environment, the system authenticates the server and vice-versa. In this way, system users can be assured that they are doing business exclusively with legitimate entities and servers can be certain that all would-be users are attempting to gain access for legitimate purposes.

This feature requires that the system being used has a Polycom factory-installed device certificate or a custom device certificate installed on it. See the section, Digital Certificates.

Prior to SIP 3.2, and in cases where the systems do not have device certificates, the system will authenticate to the server as part of the TLS authentication, but the server cannot cryptographically authenticate the system. This is sometimes referred to as Server Authentication or single-sided Authentication.

Mutual TLS authentication is optional and is initiated by the server. When the system acts as a TLS client and the server is configured to require mutual TLS, the server will request and then validate the client certificate during the handshake. If the server is configured to require mutual TLS, a device certificate and an associated private key must be loaded on the system.

The device certificate, stored on the system, is used by:

- HTTPS device configuration, if the server is configured for Mutual Authentication
- SIP signaling, when the selected transport protocol is TLS and the server is configured for Mutual Authentication
- Syslog, when the selected transport protocol is TLS and the server is configured for Mutual Authentication
- Corporate Directory, when the selected transport protocol is TLS and the server is configured for Mutual Authentication
- 802.1X Authentication, if the server is configured for Mutual Authentication (optional for EAP-TLS)





**Note: You Cannot Modify the Factory-Installed Certificate or Private Key**

Users cannot modify or update the digital certificate or the associated private key installed on the system during manufacturing. Users can install a custom device certificate to be used instead of, or in addition to, the factory-installed certificate.

The Polycom Root CA can be downloaded from <http://pki.polycom.com>. The location of the Certificate Revocation List (CRL)—a list of all expired certificates signed by the Polycom Root CA—is part of the Polycom Root CA digital certificate. If Mutual TLS is enabled, the Polycom Root CA or your organization's CA must be downloaded onto the HTTPS server.

The following operating system/Web server combinations have been tested and verified:

- Microsoft Internet Information Services 6.0 on Microsoft Windows Server 2003
- Apache v1.3 on Microsoft Windows XP



**Web Info: Provisioning Using Microsoft Internet Information Services**

For more information on using Mutual TLS with Microsoft® Internet Information Services (IIS) 6.0, see [Engineering Advisory 52609: Mutual Transport Layer Security Provisioning Using Microsoft Internet Information Services 6.0](#).

## Configurable TLS Cipher Suites

The system administrator can control which cipher suites will be offered/accepted during TLS session negotiation. The system supports the cipher suites listed in the following table and you can use the parameters listed in [Configurable TLS Cipher Suites](#) to configure TLS Cipher Suites. The 'Null Cipher' listed in the following table is a special case option which will not encrypt the signaling traffic, and is useful for troubleshooting purposes.

### TLS Cipher Suites

<i>Cipher</i>	<i>Cipher Suite</i>
ADH	ADH-RC4-MD5, ADH-DES-CBC-SHA, ADH-DES-CBC3-SHA, ADH-AES128-SHA, ADH-AES256-SHA
AES128	AES128-SHA
AES256	AES256-SHA
DES	DES-CBC-SHA, DES-CBC3-SHA
DHE	DHE-DSS-AES128-SHA, DHE-DSS-AES256-SHA, DHE-RSA-AES128-SHA, DHE-RSA-AES256-SHA
EXP	EXP-RC4-MD5, EXP-DES-CBC-SH, EXP-EDH-DSS-DES-CBC-SHA, EXP-DES-CBC-SHA, EXP-ADH-RC4-MD5, EXP-ADH-DES-CBC-SHA, EXP-EDH-RSA-DES-CBC-SHA



<i>Cipher</i>	<i>Cipher Suite</i>
EDH	EDH-RSA-DES-CBC-SHA, EDH-DSS-DES-CBC3-SHA, EDH-DSS-CBC-SHA
NULL	NULL-MD5, NULL-SHA
RC4	RC4-MD5, RC4-SHA



#### Tip: Changes to the Default TLS Cipher Suites in UC Software 4.0.0

Changes have been made to the default TLS cipher suites in UC Software 4.0.0. If you created customized TLS cipher suites in a previous release of the UC Software, your changes will be lost unless you back up the configuration files.

### Configurable TLS Cipher Suites

#### Central Provisioning Server

**template** > [parameter](#)

Specify the global cipher list

**site.cfg** > [sec.TLS.cipherList](#)

Specify the cipher list for a specific TLS Platform Profile or TLS Application Profile

**site.cfg** > [sec.TLS.<application>.cipherList](#)

#### Web Configuration Utility

To specify the cipher list for a specific TLS Platform Profile or TLS Application Profile, navigate to **Settings** > **Network** > **TLS** and expand the **TLS Profiles** menu.

#### Local System User Interface

To specify the cipher list for a specific TLS Platform Profile or TLS Application Profile, navigate to **Settings** > **Advanced** > **Admin Settings** > **TLS Profiles** > **Configure TLS Profiles**, select a profile, and choose **Configure Cipher Suite**.

## Secure Real-Time Transport Protocol

Secure Real-Time Transport Protocol (SRTP) provides a way of encrypting audio stream(s) to avoid interception and eavesdropping on system calls. As described in RFC 3711, both RTP and RTCP signaling may be encrypted using an AES (advanced encryption standard) algorithm. The parameters used to configure SRTP are shown in [Secure Real Time Transport Protocol Parameters](#). When this feature is enabled, systems negotiate with the other end-point the type of encryption and authentication to use for the session. This negotiation process is compliant with RFC4568—Session Description Protocol (SDP) Security Descriptions for Media Streams.




#### Web Info: SRTP RFC Resources

For more information on SRTP, see [RFC 3711](#). For the procedure describing how two systems set up SRTP for a call, see [RFC 4568](#).

Authentication proves to the system receiving the RTP/RTCP stream that the packets are from the expected source and have not been tampered with. Encryption modifies the data in the RTP/RTCP streams so that, if the data is captured or intercepted, it sounds like noise and cannot be understood. Only the receiver knows the key to restore the data.

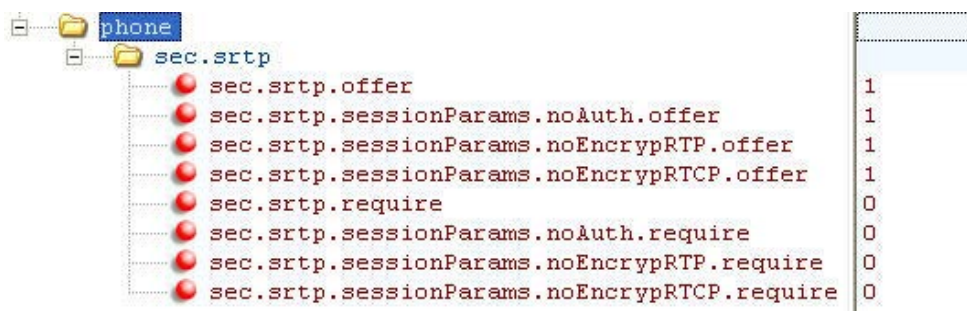
A number of session parameters have been added to enable you to turn off authentication and encryption for RTP and RTCP streams. This is done mainly to reduce the system's processor usage.

If the call is completely secure (RTP authentication and encryption and RTCP authentication and RTCP encryption are enabled), then the user sees a padlock symbol  appearing in the last frame of the connected context animation (two arrows moving towards each other)

### Secure Real Time Transport Protocol Parameters

Central Provisioning Server	template > parameter
Enable SRTP	sip-interop.cfg > sec.srtp.enable
Include secure media in SDP of SIP INVITE	sip-interop.cfg > sec.srtp.offer
Include crypto in offered SDP	sip-interop.cfg > sec.srtp.offer.*
Secure media stream required in all SIP INVITES	sip-interop.cfg > sec.srtp.require
Check tag in crypto parameter in SDP	sip-interop.cfg > sec.srtp.requireMatchingTag
Specify if the system offers and/or requires: RTP encryption, RTP authentication, and RTCP encryption	sip-interop.cfg > sec.srtp.sessionParams.*

In the following example, the **srtp\_1.cfg** configuration file is shown below:



This would result in an offer (SIP INVITE with SDP) with 8 crypto attributes with the following session parameters:

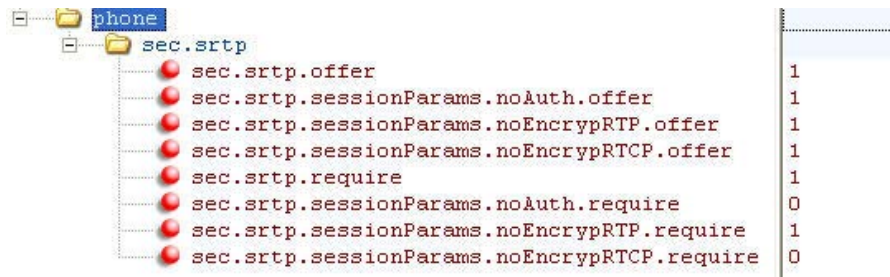
```

<no session parameters> UNENCRYPTED_SRTCP UNENCRYPTED_S RTP
UNAUTHENTICATED_S RTP
UNAUTHENTICATED_S RTP, UNENCRYPTED_S RTCP UNENCRYPTED_S RTP, UNENCRYPTED_S RTCP
UNAUTHENTICATED_S RTP, UNENCRYPTED_S RTP
UNAUTHENTICATED_S RTP, UNENCRYPTED_S RTP, UNENCRYPTED_S RTCP

```

In the above example, the crypto attributes are ordered “most secure” to “least secure” (more security turned off). The system receiving this call should chose the most secure crypto it can support based on the SRTP *require* settings in **sip.cfg** and reply with it in the SDP of a 200 OK SIP message.

In this example, the **srtp\_2.cfg** configuration file is shown below:



This results in an offer (SIP INVITE with SDP) with 4 crypto attributes with the following session parameters:

```
UNENCRYPTED_SRTP UNENCRYPTED_SRTP,UNENCRYPTED_SRTCP
UNAUTHENTICATED_SRTP,UNENCRYPTED_SRTP
UNAUTHENTICATED_SRTP,UNENCRYPTED_SRTP,UNENCRYPTED_SRTCP
```

In the above example, every crypto includes the UNENCRYPTED\_SRTP session parameter because it is required.

If nothing compatible is offered based on the receiving system’s STRP “require” settings, then the call is rejected or dropped.

## Lock the System

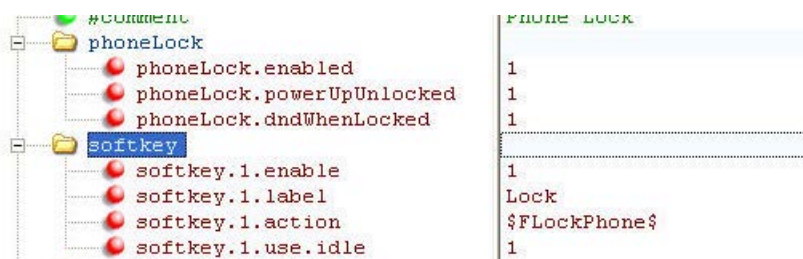
As of Polycom UC Software 3.3.0, users can lock their systems, and prevent access to the menu or key presses, by tapping the **Lock** soft key or through the system menu.



### Note: Displaying the Lock Soft Key On Your System

You need to enable the enhanced feature key (EFK) feature if you want your system to display a Lock soft key. See [feature.enhancedFeatureKeys.enabled](#).

The following configuration file snippet shows how to display the **Lock** soft key.



Once the system is locked, all user features and access to menus are disabled. The messages “The system is locked.” and “Authorized calls only.” display on the screen. Incoming calls to the system may receive a Do Not Disturb message. You can specify the authorized numbers to which users can place calls.

Using the **New Call** soft key, users can place calls using up to five authorized numbers including the emergency number. If the user places a call —using the keypad— to a number that matches an authorized number, the call will proceed. This is to ensure that certain numbers such as emergency numbers can be placed from the system.

To unlock the system, the user presses the **Unlock** soft key and enters their password; if it is entered correctly, the system returns to its normal idle state.

In case the user forgets their password, the system administrator can unlock their system either by entering the administrator password or by disabling (and re-enabling) the system lock feature. The latter method facilitates remote unlocking and avoids disclosing the administrator password to the user. See the following table for the parameters that configure the system lock feature.



#### Note: Shared Lines on Locked Systems

If a locked system has a registered shared line, calls to the shared line will be displayed on the locked system and the system’s user can answer the call.

### System Lock Parameters

#### Central Provisioning Server

	<a href="#">template</a> > <a href="#">parameter</a>
Enable enhanced feature keys	<a href="#">features.cfg</a> > <a href="#">feature.enhancedFeatureKeys.enabled</a>
Enable or disable system lock	<a href="#">features.cfg</a> > <a href="#">systemLock.enabled</a>
Specify an authorized contact (description and value) who can be called while the system is locked	<a href="#">features.cfg</a> > <a href="#">systemLock.authorized.*</a>
Specify the scenarios when system lock should be enabled	<a href="#">features.cfg</a> > <a href="#">systemLock.*</a>

#### Web Configuration Utility

To enable and configure system lock, navigate to **Settings > System Lock**.

#### Local System User Interface

To lock the system, press the Lock soft key (if available) or navigate to **Settings > Basic > Preferences > Lock System**. To unlock the system, press the **Unlock** soft key and enter the user or administrator password.

## Support 802.1X Authentication

IEEE 802.1X is a port-based Network Access Control (PNAC). It provides an authentication mechanism to devices trying to attach to a local area network (LAN) or a wireless local area network (WLAN). IEEE

802.1X is based on the Extensible Authentication Protocol (EAP). The following figure shows a typical 802.1X network configuration with wired and wireless CX5500 systems.

#### A Typical 802.1X Network Configuration



The CX5500 system supports the following EAP authentication methods:

- EAP-TLS (requires Device and CA certificates)
- EAP-PEAPv0/MSCHAPv2 (requires CA certificates)
- EAP-PEAPv0/GTC (requires CA certificates)
- EAP-TTLS/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/GTC (requires CA certificates)
- EAP-FAST (optional Protected Access Credential (PAC) file, if not using in-band provisioning)
- EAP-MD5

To set up an EAP method that requires a Device or CA certificate, you need to configure TLS Platform Profile 1 or TLS Platform Profile 2 to use with 802.1X. You can use the parameters in the following table to configure 802.1X Authentication. For more information see [TLS Profiles](#).



#### Web Info: EAP Authentication Protocol

For more information, see [RFC 3748: Extensible Authentication Protocol](#).

#### Set 802.1X Authentication Parameters

##### Central Provisioning Server

Enable or disable the 802.1X feature

`template > parameter`

`device.cfg > device.net.dot1x.enabled`

---

Specify the identity (username) for authentication	<b>device.cfg</b> > <a href="#">device.net.dot1x.identity</a>
Specify the 802.1X EAP method	<b>device.cfg</b> > <a href="#">device.net.dot1x.method</a>
Specify the password for authentication	<b>device.cfg</b> > <a href="#">device.net.dot1x.password</a>
To enable EAP In-Band Provisioning for EAP-FAST	<b>device.cfg</b> > <a href="#">device.net.dot1x.eapFastInBandProv</a>
Specify a PAC file for EAP-FAST (optional)	<b>device.cfg</b> > <a href="#">device.pacfile.data</a>
Specify the optional password for the EAP-FAST PAC file	<b>device.cfg</b> > <a href="#">device.pacfile.password</a>

---

### Web Configuration Utility

To enable and configure the 802.1X feature, navigate to **Settings > Network > Ethernet** and expand the **Ethernet 802.1X** menu.

---

### Local System User Interface

To enable 802.1X authentication, navigate to the Ethernet Menu (**Settings > Advanced > Admin Settings > Network Configuration > Ethernet Menu**) and select **802.1X Auth**.

To configure the 802.1X feature, navigate to the **Ethernet Menu** and select **802.1X Menu** (802.1X Auth must be set to enable first).

---

## Set User Profiles

There are a number of parameters shown in the table [User Profile Parameters](#) that enable users to access their personal system settings from any system in the organization. This means that users can access their contact directory and speed dials, as well as other system settings, even if they temporarily change work areas. This feature is particularly useful for remote and mobile workers who do not have a dedicated work space and conduct their business in more than one location. The User Profile feature is also beneficial if an office has a common conference system. In this case, multiple users could use the system and access their own settings.

If a user changes any settings while logged in to a system, the settings will be saved and displayed the next time the user logs in to a system. When a user logs out, the user's personal system settings are no longer displayed.

If you set up the User Profile feature, a user can log in to a system by entering their user ID and password. The default password is **123**.



#### Tip: Calling Authorized Numbers while Logged Out

You can configure the systems so that anyone can call authorized and emergency numbers when not logged in to a system. For more information, see [dialplan.routing.emergency.outboundIdentity](#).

If the User Profile feature is set up on your company's systems, users can:

- Log in to a system to access their personal system settings.
- Log out of a system after they finish using it.

- Place a call to an authorized number from a system that is in the logged out state.
- Change their user password.

When you set up the User Profile feature, you will have to decide whether you want to require users to always log in to a system. If the User Profile feature is enabled, but not required, users can choose to use the system as is (that is, without access to their personal settings), or they can log in to display their personal settings. You can specify if a user is logged out of the system when the system restarts or reboots, or if they remain logged in.

You can also choose to define default credentials for the system (see the section [Create a System Configuration File](#)). If you specify a default user ID and password, the system automatically logs itself in each time an actual user logs out or the system restarts or reboots. When the system logs itself in using the default login credentials, a default system profile is displayed (as defined in the system's master configuration file on the provisioning server). In this scenario, users will still have the option to log in and view their personal settings.

To set up the User Profile feature, perform the following procedures on the provisioning server:

- Create a system configuration file, or update an existing file, to enable the feature's settings.
- Create a user configuration file—called **<user>.cfg**—that specifies the user's password and registration, and other user-specific settings that you want to define.



**Tip: Resetting a User's Password**

You can reset a user's password by removing the password parameter from the override file. This will cause the system to use the default password in the **<user>.cfg** file.

After you complete these procedures, update the system's configuration to affect your changes. The User Profile feature will be ready to use.

### User Profile Parameters

Central Provisioning Server	template > parameter
Enable or disable the user profile feature	site.cfg > prov.login.enabled
Specify the amount of time before a non-default user is logged out	site.cfg > prov.login.automaticLogout
Specify the default password for the default user	site.cfg > prov.login.defaultPassword
Specify if the system can have users other than the default user	site.cfg > prov.login.defaultOnly
Specify the name of the default user	site.cfg > prov.login.defaultUser
Specify the password used to validate the user login	site.cfg > prov.login.localPassword
Specify if a user should remain logged in after the handset reboots	site.cfg > prov.login.persistent
Specify if a user must log in while the feature is enabled	site.cfg > prov.login.required



## Create a System Configuration File

Create a system configuration file for the User Login feature, and then add and set the attributes for the feature. Or, if you already have a system configuration file, update the file to include the User Login parameters you want to change. Polycom recommends that you create a single default user password for all users.

### To define the feature's settings:

- 1 Create a **site.cfg** file for the system and place it on the provisioning server.  
You can base this file on the sample configuration template that is in your software package. To find the file, navigate to **<provisioning server location>/Config/site.cfg**.
- 2 In **site.cfg**, open the `<prov.login/>` attribute, and then add and set values for the user login attributes.

The following example is an example **site.cfg** file. Your file will contain different values, depending on how you want the feature to work.

Attribute	Value
<code>prov.login.automaticLogout</code>	0
<code>prov.login.defaultDomain</code>	
<code>prov.login.defaultOnly</code>	0
<code>prov.login.defaultPassword</code>	
<code>prov.login.defaultUser</code>	
<code>prov.login.enabled</code>	0
<code>prov.login.localPassword</code>	123
<code>prov.login.persistent</code>	0
<code>prov.login.required</code>	0

## Create a User Configuration File

Create a configuration file for each user that you want to be able to log in to the system. The name of the file will specify the user's login ID. In the file, specify any user-specific settings that you want to define for the user.



### Tip: Converting a System-Based Deployment to a User-Based Deployment

To convert a system-based deployment to a user-based deployment, copy the `<MACaddress>-system.cfg` file to `<user>-system.cfg` and copy `systemConfig<MACaddress>.cfg` to `<user>.cfg`.

### To create a user configuration file:

- 1 On the provisioning server, create a user configuration file for each user that will be able to log in to the system. The name of the file will be the user's ID to log in to the system. For example, if the user's login ID is **user100**, the name of the user's configuration file is **user100.cfg**.
- 2 In each `<user>.cfg` file, you can add and set values for the user's login password (optional).
- 3 Add and set values for any user-specific parameters, such as:
  - Registration details (for example, the number of lines the profile will display and line labels).
  - Feature settings (for example, microbrowser settings).





### Caution: Adding User-Specific Parameters

If you add optional user-specific parameters to <user>.cfg, add only those parameters that will not cause the system to restart or reboot when the parameter is updated. For information on which parameters cause the system to restart or reboot, see the [Configuration Parameters](#).

The following is a sample user configuration file.

The screenshot shows a configuration file editor with a tree view on the left and XML code on the right. The tree view shows a folder named 'polycomConfig' containing several elements: 'xmlns:xsi', 'xsi:noNamespaceSchemaLocation', '#comment', 'prov.login', 'prov.login.localPassword', 'prov.login.localPassword', 'prov.login.localPassword.hash', '#comment', 'reg', '#comment', 'saf', '#comment', and 'feature'. The XML code on the right shows the corresponding XML structure:

```

http://www.w3.org/2001/XMLSchema-instance
polycomConfigPrivate.xsd
User Profile
123
0
Registration definition
Sampled audio definition
Feature definition

```

If a user updates their password or other user-specific settings using the Main Menu on the system, the updates will be stored in **<user>-system.cfg**, not **<MACaddress>-system.cfg**.

If a user updates their Contact Directory while logged in to a system, the updates will be stored in **<user>-directory.xml**. Directory updates will be displayed each time the user logs in to a system. For certain systems, an up-to-date call lists history will be defined in **<user>-calls.xml**. This list will be retained each time the user logs in to their system. Configuration parameter precedence (from first to last) for a system that has the User Profile feature enabled is:

- **<user>-system.cfg**
- Web Configuration Utility (through a browser)
- Polycom CMA system
- Configuration files listed in the master configuration file (including **<user>.cfg**)
- Default values

# Use the CX5100/5500 Control Panel

The Polycom CX5100/CX5500 Control Panel enables you to change a limited group of settings for an individual system when connected to a computer and used as a video conference device. If you are not using the telephony features of the CX5500 system, you can use the Control Panel to configure your system. Note that you cannot configure telephony settings and features in the Control Panel.

You can download and install the Control Panel from the [Polycom CX5500 Support](#) site. The following figure shows the System Information tab in the Control Panel.



The screenshot displays the Polycom CX5100/CX5500 Control Panel interface. The top navigation bar includes 'Profile Editor', 'System', 'Diagnostics', and 'Support'. The 'System' tab is active, showing system information for a CX5500 device. A left sidebar lists navigation options: 'System Information', 'Password', 'Date/Time', 'Software Update', and 'Additional Information'. The main content area lists various system details:

Product Name:	Polycom CX5500 Unified Conference Station
Product Serial Number:	8213194000430A
Tabletop Hardware Version:	000.00
Power Data Box Hardware Version:	003.4
Device Software Version:	1.1.0.10110
Microcontroller Information:	Hardware Rev :4 , uC major: 0x27 , mini: 0x27 , boot: 0x27
Camera Information:	ISP HW v:0x5231a6be ISP SW v:0x77da Wdy
Time Settings:	Thursday, April 3, 2014 04:18PM
USB Connectivity Type:	2
IP Address:	10.146.204.224

A 'Refresh' button is located at the bottom right of the interface.

The Control Panel provides a user-friendly, intuitive method to configure settings for using the CX5500 as a connected device.

After you install the Control Panel, you can connect your system to your computer and create a profile for CX5500 system, view your system's information, change system settings, and view diagnostics and retrieve logs.

## Find Your Default System Password

To make changes to your Polycom CX5500 system using the Control Panel, enter the system password. By default, the password is the 14-digit system serial number. 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 system's password in the System tab in the Control Panel.

### To change the system default 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 system in the **New Password** field and retype the new password in the **Confirm New Password** field.
- 4 Click **Change Password**.

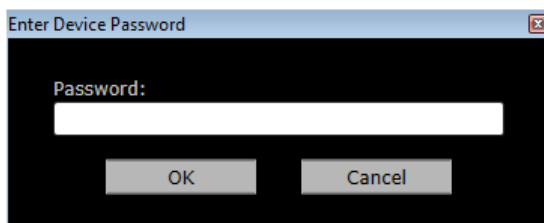
Your new password is saved.

## Create or Load a System Profile

The Profile Editor in the Control Panel enables you to change device settings and update software. You can also save profiles onto your computer and load a profile to your CX5500 system.

### To create a profile:

- 1 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.
- 2 In the **Control Panel**, click **Profile Editor**.  
The Enter Device Password dialog displays.



- 3 Enter the **Device Password** and click **OK**.

Note that the default device password is the system's serial number (see figure [Location of the Serial Number Label on the Power Data Box](#) for the location of the system's serial number).

- 4 On the **Software Update** tab, enter the name of the **Update Server** and select values for the **Update Frequency** and **Update Time** fields.
- 5 On the **Advanced** tab, select options for the following settings:
  - a 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.
  - b Select the **Power Frequency** for your system.
  - c Choose the **USB Connectivity Reset Interval** and the **USB Connectivity Reset Time**.
- 6 Do one of the following:
  - Click **Apply to Device** to save the profile on your CX5500 system.
  - Click **Save to File (PC)** to save the profile to your computer. Specify the name of the file and the location of where to save the profile and click **Save**.

You can also load a profile from the device, a saved profile from your computer, or a default system profile onto your CX5500 systems.

#### To load a profile:

- 1 In the **Profile Editor** tab, click **Load Profile**.
- 2 Select one of the following options:
  - **Load from Device** Uploads the profile saved on the system.
  - **Load from File (PC)** Uploads a profile saved on your computer on to the system.
  - **Load Default Profile** Uploads the factory default profile for the system.
- 3 After you make your selection, click **Apply to Device**.

The profile is saved onto the CX5500 system.

## *Update the CX5500 System's Software Automatically*

You can configure your system to check for available updates automatically, or you can update the software for your CX5500 system manually in the Control Panel or upload new software to the system using a USB flash drive.

#### To update the software automatically:

- 1 In the **Profile Editor** tab, select **Software Update**.
- 2 Enter the name of the **Update Server**.
- 3 Select how often your system updates for **Update Frequency**.
- 4 Select what time your system updates for **Update Time**.

Your CX5500 system retrieves software updates from the server on the chosen date and time, if available.

## Update the CX5500 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 system uploads the software update from the server, if available.

# Troubleshoot Your CX5500 System

---

This section shows you some tools and techniques for troubleshooting the CX5500 system running Polycom® UC Software. The system can provide feedback in the form of on-screen error messages, status indicators, and log files for troubleshooting issues.

This section includes information on:

- [Understand Error Message Types](#)
- [Status Menu](#)
- [Log Files](#)
- [Manage the System's Memory Resources](#)
- [Test System Hardware](#)
- [Upload a System's Configuration](#)
- [Network Diagnostics](#)
- [Ports Used on the CX5500 System](#)

This section also addresses system issues, likely causes, and corrective actions. Issues are grouped as follows:

- [Power and Startup Issues](#)
- [Dial Pad Issues](#)
- [Screen and System Access Issues](#)
- [Calling Issues](#)
- [Display Issues](#)
- [Audio Issues](#)
- [Licensed Feature Issues](#)
- [Upgrading Issues](#)
- [SoundStation Duo Failover Issues](#)

Review the latest *UC Software Release Notes* on the [Polycom UC Software Support Center](#) for known problems and possible workarounds. If a problem is not listed in this section or in the latest *Release Notes*, contact your Certified Polycom Reseller for support.

## Understand Error Message Types

Several types of errors can occur while the system is booting. If an error occurs, the system will inform you by displaying an error message. Errors can affect how the system boots up. If the error is fatal, the system will not be able to boot until the error is resolved. If the error is recoverable, the system will continue to boot but the system's configuration may change.

### ***Error Messages***

Most of the following errors will be logged to the system's boot log. However, if you are having trouble connecting to the provisioning server, the system will likely not be able to upload the boot log.

### **Failed to get boot parameters via DHCP**

The system does not have an IP address and therefore cannot boot. Check that all cables are connected, the DHCP server is running, and that the system has not been set to a VLAN that is different from the DHCP server. Check the DHCP configuration.

### **Could not contact boot server using existing configuration**


The system could not contact the provisioning server, but the causes may be numerous. It may be a cabling issue, it may be related to DHCP configuration, or it could be a problem with the provisioning server itself. The system can recover from this error so long as it previously downloaded a valid application BootROM image and all of the necessary configuration files.

### **Error, application is not present!**

This message indicates that the system has no application stored in device settings, that the system could not download an application, and that the system cannot boot. To resolve this issue, you must download compatible Polycom UC Software to the system using one of the supported provisioning protocols. You need to resolve the issue of connecting the system to the provisioning server and provide a compatible software image on the provisioning server. This error is fatal, but recoverable.

## ***Polycom UC Software Error Messages***

The warning notification feature provides users a visual indication that one or more error conditions exist. When the warning notification displays, users will see:

- An informative message when the warning is first detected
- A warning icon  displays in the status bar
- A persistent list of current warnings, which can be viewed from **Status > Diagnostics > Warnings**

**Config file error: Files contain invalid params: <filename1>, <filename2>,...**

**Config file error: <filename> contains invalid params.**

**The following contain pre-3.3.0 params: <filename>**

These messages display if any of the following parameters are found in the configuration files:

- tone.chord.ringer.x.freq.x
- se.pat.callProg.x.name
- ind.anim.IP\_500.x.frame.x.duration
- ind.pattern.x.step.x.state
- feature.2.name
- feature.9.name

This message also appears if any configuration file contains:

- More than 100 unknown parameters, or
- More than 100 out-of-range values, or
- More than 100 invalid values.

To update the configuration files to use the correct parameters, see [Change Configuration Parameter Values](#) for details.



**Line: Unregistered**

This message displays if a line fails to register with the call server.

**Login credentials have failed. Please update them if information is incorrect.**

This message displays when the user enters incorrect login credentials (**Status > Basic > Login Credentials**).

**Missing files, config. reverted**

This message displays when errors in the configuration and a failure to download the configuration files force the system to revert to its previous (known) condition with a complete set of configuration files. This will also display if the files listed in the **<MAC Address>.cfg** file are not present on the provisioning server.

**Network Authentication Failure**

This message displays if 802.1X authentication with the CX5500 system fails. The error codes shown in the table [Event Codes and Descriptions](#) display on the system's screen—if the **Details** soft key is selected—and in the log files:

**Event Codes and Descriptions**

<i>Event Code</i>	<i>Description</i>	<i>Comments</i>
1	Unknown events	This includes any event listed in this table.
2	Mismatch in EAP Method type Authenticating server's list of EAP methods does not match with clients'.	
30xxx	TLS Certificate failure The TLS certificate-related failures. "xxx" when having a non-zero value, is the standard TLS alert message code. For example, if a bad/invalid certificate (on the basis of its signature and/or content) is presented by the system, "xxx" will be 042. If the exact reason for the certificate being invalid is not known, then the generic certificate error code will be xxx=000.	See section 7.2 of <a href="#">RFC 2246</a> for further TLS alert codes and error codes.
31xxx	Server Certificate failure Certificate presented by the server is considered invalid. "xxx" can take the following values: <ul style="list-style-type: none"> <li>• 009 - Certificate not yet Valid</li> <li>• 010 - Certificate Expired</li> <li>• 011 - Certificate Revocation List (CRL) not yet Valid</li> <li>• 012 - CRL Expired</li> </ul>	

<i>Event Code</i>	<i>Description</i>	<i>Comments</i>
4xxx	Other TLS failures This is due to TLS failure other than certification related errors. The reason code (the TLS alert message code) is represented by "xxx". For example, if the protocol version presented by the server is not supported by the system, then xxx will be 70, and the EAP error code will be 4070.	See section 7.2 of <a href="#">RFC 2246</a> for further TLS alert codes and error codes.

## Network link is down

Link failures are indicated with the message 'Network link is down'. This message displays on the screen whenever the system is not in the menu system and persists until the link problem is resolved. Call related functions and the soft keys and line keys are disabled when the network is down; however the menu works.

## Status Menu

Debugging of a single system may be possible by examining the system's status menu. Tap **Settings > Status** to view the Status menu. Tap one of the Status menu items to view that item. Each of the menu items is explained next.

Under the **Platform** menu, you can get details on the system's serial number or MAC address, the current IP address, the application version, the name of the configuration files in use, and the address of the provisioning server.

In the **Network** menu, you can find information about the TCP/IP Setting, Ethernet port speed, connectivity status of the PC port (if it exists), and statistics on packets sent and received since last boot. You can also find out the last time the system rebooted. The **Call Statistics** screen shows packets sent and received on the last call.

The **Lines** menu shows you details about the status of each line that has been configured on the system.

The **Diagnostics** menu offers a series of hardware tests to verify correct operation of the microphone, speaker, and touchscreen. In addition to the hardware tests, the Diagnostics menu has a series of real-time graphs for CPU, network, and memory use that can be helpful for diagnosing performance issues.

## Log Files

The CX5500 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.

There is one log file for the UC Software. When a system uploads its log files, the files are saved on the provisioning server with the MAC address of the system prepended to the file name. For example, **0004f200360b-app.log** is the file associated with MAC address 00f4f200360b. The application log file is uploaded periodically or when the local copy reaches a predetermined size. For more information on log file contents, see the reference section [<log/>](#).

The amount of logging that the system performs can be tuned for the application to provide more or less detail on specific components of the system's software. For example, if you are troubleshooting a SIP signaling issue, you are not likely interested in DSP events. Logging levels are adjusted in the configuration files or via the Web Configuration Utility. You should not modify the default logging levels unless directed to by Polycom Customer Support. Inappropriate logging levels can cause performance issues on the system.

In addition to logging events, the system can be configured to automatically execute command-line instructions at specified intervals that output run-time information such as memory utilization, task status, or network buffer contents to the log file. These techniques should only be used in consultation with Polycom Customer Support.

## ***Logging Options***

Each of the components of the Polycom UC software is capable of logging events of different severity. This allows 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 CX5500 system:

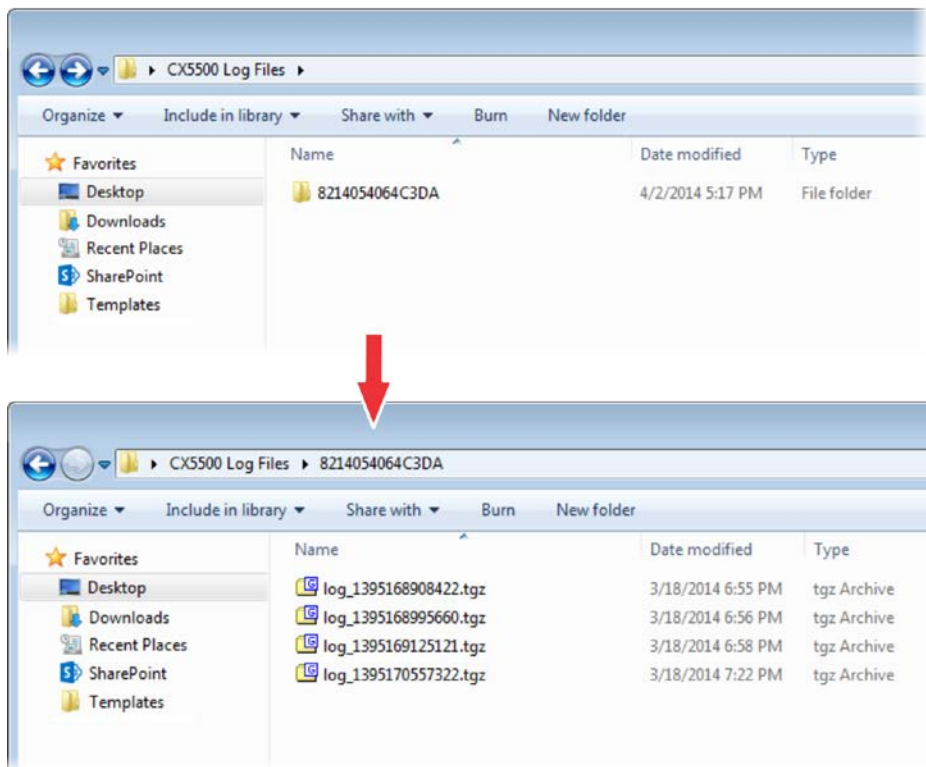
- USB drive
- CX5100-CX5500 Control Panel
- Web Configuration Utility
- Provisioning server
- Log level parameters

## **Retrieve Logs using 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.

The following figure shows an example device folder with log files.

### Device Folder and Log Files for the CX5500 System



#### To retrieve system log files using a USB drive:

- » Connect a USB flash drive to the USB port on the tabletop unit or on the power data box. Make sure there is no software update package on the flash drive.

The logs are transferred automatically. Note that it takes approximately one minute to complete the transfer.



#### Note: Export configuration file to USB flash drive

Similarly, you can also export the configuration file to a USB flash drive.

## 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 log files 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 the 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.

### To upload logs to the provisioning server:

- 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).
- `log.render.file.upload.append.sizeLimit`—Controls the maximum size of UC Software log files on the provisioning server (default=512 kb). This does not apply to system log files for the CX5500 system.
- `log.render.file.upload.append.limitMode`—Controls whether to stop or delete UC Software log files when the server log reaches its maximum size (default=delete). This does not apply to system log files for the CX5500 system.

## 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.

See the following figure for an example of a configuration file and the resulting log file.

### Scheduled Logging Log File

Parameter	Value
<code>log.sched.1.name</code>	<code>showCpuLoad</code>
<code>log.sched.1.level</code>	<code>4</code>
<code>log.sched.1.period</code>	<code>15</code>
<code>log.sched.1.startMode</code>	<code>rel</code>
<code>log.sched.1.startTime</code>	<code>0</code>
<code>log.sched.1.startDay</code>	<code>0</code>
<code>log.sched.2.name</code>	<code>memShow</code>
<code>log.sched.2.level</code>	<code>4</code>
<code>log.sched.2.period</code>	<code>15</code>
<code>log.sched.2.startMode</code>	<code>rel</code>
<code>log.sched.2.startTime</code>	<code>0</code>
<code>log.sched.2.startDay</code>	<code>0</code>



The following figure shows a number of boot failure messages:

### Boot Failure Messages

```
0522183251|copy|3|00|Beginning to provision phone
0522183251|copy|3|00|'ftp://plcmisp:***@172.23.2.92/2345-12450-001.bootrom.ld' from
0522183251|copy|4|00|Download of '2345-12450-001.bootrom.ld' FAILED on attempt 1 (addr
0522183251|copy|4|00|Server '172.23.2.92' said '2345-12450-001.bootrom.ld' is not pres
0522183251|cfg|4|00|Could not get all 512 bytes of the header
0522183251|copy|3|00|'ftp://plcmisp:***@172.23.2.92/bootrom.ld' from '172.23.2.92'
0522183251|copy|4|00|Download of 'bootrom.ld' FAILED on attempt 1 (addr 1 of 1)
0522183251|copy|4|00|Server '172.23.2.92' said 'bootrom.ld' is not present
0522183251|cfg|4|00|Could not get all 512 bytes of the header
0522183251|cfg|3|00|bootROM file not present on boot server
0522183251|copy|3|00|'ftp://plcmisp:***@172.23.2.92/0004f21db094.cfg' from '172.23.2
0522183251|copy|4|00|Download of '0004f21db094.cfg' FAILED on attempt 1 (addr 1 of 1)
0522183251|copy|4|00|Server '172.23.2.92' said '0004f21db094.cfg' is not present
0522183251|copy|3|00|Update of '/ffs0/init.mac' failed, leaving local copy intact
0522183251|copy|3|00|'ftp://plcmisp:***@172.23.2.92/000000000000.cfg' from '172.23.2
0522183251|copy|3|00|Download of '000000000000.cfg' succeeded on attempt 1 (addr 1 of
```

## Reading an Application Log File

The following figure shows portions of an application log file:

### Application Log File

```
0522184554|log  *|01|Initial log entry. Current logging level 4
0522184554|so  *|01|Initial log entry. Current logging level 3
0522184554|so  *|01|----- Initial log entry -----
0522184554|so  *|01|Platform: Model=SoundPoint IP 450, Assembly=2345-12450-001 Rev=
0522184554|so  *|01|Platform: MAC=0004f21db094, IP=172.23.61.141, Subnet Mask=255.2
0522184554|so  *|01|Platform: BootBlock=2.8.1 (12450_001) 04-Jun-08 17:04
0522184554|so  *|01|Platform: Bootrom=4.1.2.0009 20-Jul-08 21:57
0522184554|so  *|01|Application, main: Label=SIP, Version=3.1.3.0439 26-Apr-09 23:5
0522184554|so  *|01|Application, main: P/N=3150-11530-313
0522184554|wdog *|01|Initial log entry. Current logging level 4
0522184554|ethf *|01|Initial log entry. Current logging level 4
0522184554|so  5|01|utilCertificateInit failed.
0522184554|hw  *|01|Initial log entry. Current logging level 4
0522184554|ares *|01|Initial log entry. Current logging level 4
0522184554|dns  *|01|Initial log entry. Current logging level 3
0522184554|cfg  *|01|Initial log entry. Current logging level 3

0522114602|so  *|01|System Info Reports:
0522114602|so  *|01| CPU is TNETV1055/C55x, rev 2 running at 150MHz with memory at 3
0522114602|so  *|01| Board is identified as PolycomSoundPointIP-SPIP_450.
0522114602|so  *|01| DRAM_LO: 0x94000000. DRAM_SIZE: 32 MB
0522114602|so  *|01| Clocks are VBUSP: 125MHz, VBUS: 75MHz, USB: 25MHz, LCD: 20MHz,
0522114602|key  *|01|Initial log entry. Current logging level 4
0522114602|ht  *|01|Initial log entry. Current logging level 4
0522114602|httpd *|01|Initial log entry. Current logging level 4
0522114602|ssps *|01|Application, comp. 1: Label=PolyDSP Titan Mem1 FS5 (G.729), Vers

0522185324|cfg  3|01|Prm|Check of configuration files succeeded
0522185324|cfg  3|01|Prm|Phone successfully provisioned
0522185324|cfg  *|01|Prm|Configuration file "001-phone1.cfg" is from template phone1
0522185324|cfg  *|01|Prm|Configuration file "001-phone1.cfg" SHA1 digest: B712DCC39
0522185324|cfg  *|01|Prm|Configuration file "001-sip.cfg" is from template sip.cfg,
0522185324|cfg  *|01|Prm|Configuration file "001-sip.cfg" SHA1 digest: B4E4534529797
0522185324|so  13|01|Success provisioning.
```



```

0522120608|ldap |*|01|Initial log entry. Current logging level 4
0522120608|ldap |4|01|ldap: Not Enabled
0522120608|ldap |4|01|cDynamicData::cDynamicData:cDynamicData:Failed
0522120608|efk |*|01|Initial log entry. Current logging level 4
0522120608|so |*|01|[SoNcasC]: App-Ctx (6045551234) [0-6045551234]
0522120608|sip |4|01|NAPTR query for host 'as-test' returned no results
0522120608|app1 |*|01|[InitializeBacklightIntensity] m_nDefaultMin = 0, m_nDefaultLow
0522120608|sip |4|01|Registration failed User: 6045551234, Error Code:404 Not Found
0522120608|cfg |4|01|Edit|Error 0x380003 attempting stat of /ffs0/local/0004f21db094-

```

## Reading a Syslog File

The figure [Syslog File](#) shows a portion of a syslog log file. Note that the messages look identical to the normal log except for the addition of a timestamp and IP address:

### Syslog File

```

Jan  0 00:00:00 172.23.7.249 0100000000|so |4|00|----- Initial log entry -----
Jan  0 00:00:00 172.23.7.249 0100000000|so |4|00|+++ Note that bootrom log times are in GMT +++
Jan  0 00:00:00 172.23.7.249 0100000000|cfg |4|00|Initial log entry
Jan  0 00:00:00 172.23.7.249 0100000000|copy |3|00|Initial log entry
Jan  0 00:00:00 172.23.7.249 0100000000|hw |4|00|Initial log entry.
Jan  0 00:00:00 172.23.7.249 0100000000|ethf |4|00|Initial log entry.
Feb 13 01:12:39 172.23.7.249 0213011239|wdog |4|00|Initial log entry
Feb 13 01:12:39 172.23.7.249 0213011239|cdp |3|00|CDP is DISABLED.
Feb 13 01:12:39 172.23.7.249 0213011239|so |3|00|Platform: Model=SoundPoint IP 650, Assembly=2345-126
Feb 13 01:12:39 172.23.7.249 0213011239|so |3|00|Platform: Board=2345-12600-001 1
Feb 13 01:12:39 172.23.7.249 0213011239|so |3|00|Platform: MAC=0004f2111511, IP=Resolving, Subnet Mas
Feb 13 01:12:39 172.23.7.249 0213011239|so |3|00|Platform: BootBlock=2.7.0 (12600_001) 30-May-06 15:8
Feb 13 01:12:39 172.23.7.249 0213011239|so |3|00|Application, main: Label=BOOT, Version=4.1.0.0219 10
Feb 13 01:12:39 172.23.7.249 0213011239|so |3|00|Application, main: P/N=3150-11069-410
Feb 13 01:12:39 172.23.7.249 0213011239|app1 |4|00|Initial log entry.
Feb 13 01:12:40 172.23.7.249 0213011240|so |3|00|Link status is Net down, PC down.
Feb 13 01:12:41 172.23.7.249 0213011241|so |3|00|Link status is Net up Speed 100 half Duplex, PC down
Feb 13 01:12:41 172.23.7.249 0213011241|cdp |3|00|CDP is disabled.
Feb 13 01:12:45 172.23.7.249 0213011245|app1 |3|00|DNS resolver servers are '172.23.0.200' '172.23.0.20
Feb 13 01:12:45 172.23.7.249 0213011245|app1 |3|00|DNS resolver search domain is 'vancouver.polycom.com
Feb 13 01:12:45 172.23.7.249 0213011245|app1 |3|00|Bootline: esw(3,0)bootHost:flash e=172.23.7.249:ffff
Apr 15 22:32:22 172.23.7.249 0415223222|app1 |3|00|Time has been set from 172.23.0.200 (172.23.0.200).
Apr 15 22:32:22 172.23.7.249 0415223222|app1 |3|00|DHCP returned result 0x3E7 from server 172.23.0.232.
Apr 15 22:32:22 172.23.7.249 0415223222|app1 |3|00| Phone IP address is 172.23.7.249.
Apr 15 22:32:22 172.23.7.249 0415223222|app1 |3|00| Subnet mask is 255.255.0.0.
Apr 15 22:32:22 172.23.7.249 0415223222|app1 |3|00| Gateway address is 172.23.2.240.
Apr 15 22:32:22 172.23.7.249 0415223222|app1 |3|00| Time server is 172.23.0.200.
Apr 15 22:32:22 172.23.7.249 0415223222|app1 |3|00| GMT offset is -28800 seconds.

```



#### Web Info: Using Syslog on Polycom Systems

For more information about syslog, see [Feature Profile 17124: Using Syslog on Polycom Systems](#).

## Manage the CX5500 System's Memory Resources

The CX5500 system is designed to operate optimally in a variety of deployments and real-world environments. Each new software release adds new features and capabilities that require varying degrees of the system's memory resources. To ensure your systems and their configured features operate smoothly, you need to check that the systems have adequate available memory resources. If you are using a range of system features—especially customized or advanced features—you may need to

manage system memory resources. To help you optimize your CX5500 system's features and memory resources, Polycom provides several tools and troubleshooting tips.

## Identify Symptoms

When the system memory resources start to run low, you may notice one or more of the following symptoms:

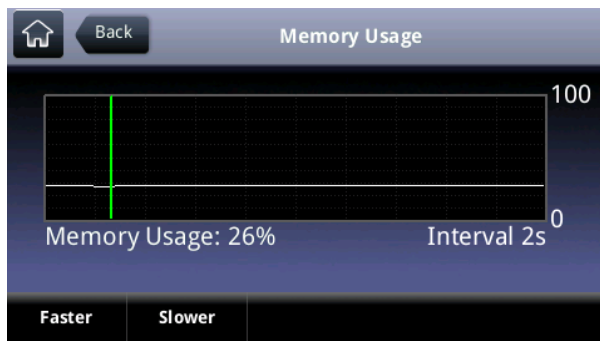
- The systems reboot or freeze up.
- The systems do not download all ringtones, directory entries, backgrounds, or XML dictionary files.
- Applications running in the microbrowser or browser stop or do not run at all.

The next sections show you how to check your system's available memory and manage the system features to make system memory available.

## Check the System's Available Memory

You can use two methods to quickly check whether you need to manage your system's memory. Before you begin checking, load and configure the features and files you want to make available on the system.

Using the first method, on your system's keypad or touch pad interface, choose **Status > Diagnostics > Graphs > Memory Usage** as shown next.



Use the *Memory Usage* chart to check what the current Memory Usage amount is. Typically, you want to ensure that the system is running at less than 95 percent of its available memory.

If the system is using more than 95 percent of its available memory, you may need to take steps to reduce this amount. **Error! Reference source not found.**

The second method you can use to confirm whether you need to manage your system's memory is to check the app log files. The app log file is enabled by default and is saved to your provisioning server directory with the MAC address of the system prepended to the app log file. For example, if the MAC address of your system is **0004f2203b0**, the app log file name will be **0004f2203b0-app.log**.

Open the app log. If you see the message shown next in the following figure, you need to manage your system's memory resources.

## Application Log Error Message

```

000014.458|dnš|*|00|DNS resolver servers are '172.23.0.200' '172.23.0.239'
000014.458|dnš|*|00|DNS resolver search domain is 'vancouver.polycom.com'
000014.460|cfg|*|00|RT|Primary IP changed to 172.23.70.29 subnet mask 255.255.0.0
000016.412|fb|*|00|Initial log entry. Current logging level 4
000016.414|so|*|00|Network initialized. Starting network tasks.
000016.428|cfg|5|00|Prm|Parameter lcl.ml.lang requested type 2 but is of type 4
000016.428|cfg|5|00|Prm|Type 2 4 0 for parameter lcl.ml.lang is not valid
000016.658|sip|*|00|Fast Boot Measurement Point: Ready for Call, uptime: 16.658 sec.
000016.982|tr69|*|00|Initial log entry. Current logging level 4
000016.984|cfg|*|00|Prov|Starting to update 2345-12670-001.sip.ld
000016.994|app1|*|00|Ctx [1] Registered [true]
000017.004|res|4|00|[ResFinderC]: Minimum free memory reached. 0xaf150.
000017.012|cfg|*|00|Prov|Finished updating configuration.

```

## Test System Hardware

You can view diagnostic information from the **Diagnostics** menu on your system (**Settings > Status > Diagnostics**).

If you select **Diagnostics > Test Hardware**, you can select one of the following menu items to perform a hardware diagnostic test:

- **Audio Diagnostics** Test the speaker and microphones.
- **Display Diagnostics** Test the LCD for faulty pixels.
- **Touch Screen Diagnostics** Test the touch screen response.

## Upload a System's Configuration

As of Polycom UC Software 3.3.0, you can upload the files representing a system's current configuration. A number of files can be uploaded to the provisioning server, one for every active source as well as the current non-default configuration set.

As of Polycom UC Software 4.0.0, you can upload the system's configuration through the Web Configuration Utility.

This is primarily a diagnostics tool to help find configuration errors.

### To upload the system's current configuration:

- 1 Navigate to the Upload Configuration menu on the system (**Settings > Advanced > Admin Settings > Upload Configuration**).
- 2 Choose to upload the configuration from one of **All Sources**, **Configuration Files**, **Local**, or **Web**. You can select **Device Settings** if you perform this task using the Web Configuration Utility.
- 3 Press the **Upload** soft key.  
The system uploads the configuration file to the location that you specify in [prov.configUploadPath](#). For example, if you select **All Sources**, a file **<MACaddress>-update-all.cfg** is uploaded.

## Network Diagnostics

In Polycom UC Software 4.0.0, ping and traceroute are added to the system's diagnostics tools. These diagnostics can be used for troubleshooting network connectivity problems in the wired and wireless worlds.

Both tools are accessible by tapping **Settings** and selecting **Status > Diagnostics > Network**.

Enter a URL address (for example, <http://www.google.com>) or any IP address (for example, the system IP address or any other system's IP address), and tap the **Enter** soft key.

## Restore the Default Settings

You can reset the CX5500 to its default settings, which clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to 456.

The restore can take up to 40 minutes to complete. During this time, the system reboots several times, and the indicator lights flash red and green in several patterns. Do not power the system off during the restore process. Wait at least 40 minutes to make sure the update has completed.

**To restore default settings stored in the system factory partition:**

- 1 Remove any USB storage devices from the system. USB devices could be connected to the table console or to the power data box.
- 2 Power off the system.
- 3 Use the end of a paper clip or similar object to press and hold the Restore button on the back of the power data box.



- 4 While holding the Restore button, power on the system.
- 5 Continue holding the Restore button for 20 seconds before releasing.  
The indicator lights flash red and green in several patterns to indicate that the restore process has started.

## Restore Default Settings using a USB Flash Drive

By default, when you perform a factory restore, the CX5500 reverts to its default factory settings. You can use a USB flash drive to restore the CX5500 to a software version later than the default factory software. When using a flash drive to restore settings, make sure the flash drive is formatted as FAT32.

**To restore default settings using a USB flash drive:**

- 1 Using a 2.0 flash drive formatted as FAT32, copy the software package to the root of the USB device. The software package has a .tar extension.
- 2 Remove any previous versions of software updates from the USB drive.
- 3 Remove any USB storage devices from the connected to the table console or to the power data box.
- 4 Power off the system.

- 5 Connect the USB device with the software package to the system.
- 6 Use the end of a straightened paper clip or similar object to press and hold the Restore button on the back of the power data box.
- 7 While holding the Restore button, power on the system.
- 8 Continue holding the Restore button for 10 seconds before releasing.  
The indicator lights flash red and green in several patterns to indicate that the restore process has started.

## ***Restore to Default using the Local Interface***

There are five ways to reset or clear features and settings to the default values using the local interface on the system.

### **To reset the system to the default values:**

- 1 On the system, go to **Settings > Advanced > Administration Settings > Reset to Defaults**.
- 2 Choose one of the following options:
  - **Reset Local Configuration** Clears the override file generated by changes using the system user interface
  - **Reset Web Configuration** Clears the override file generated by changes using the Web Configuration Utility.
  - **Reset Device Settings** Resets the system's flash file system settings that are not stored in an override file. These are your network and provisioning server settings and include custom certificates and encryption keys. Local, web, and other configuration files remain intact.
  - **Format File System** Formats the system's flash file system and deletes the UC software application, log files, configuration, and override files. Note that if the override file is stored on the provisioning server, the system will re-download the override file when you provision the system again. Formatting the system's file system does not delete those device settings affecting network and provisioning, and any certificates and encryption keys remain on the system.
  - **Reset to Factory** Removes the web and local override files, any stored configuration files in the flash file system, as well as any custom certificates and encryption keys. All network and provisioning settings are reset but the UC software application and updater remain intact.

## **Ports Used on the CX5500 System**

See the table [Ports Used by the CX5500 System](#) for a list of the ports currently used by the Polycom UC Software.

### **Ports used by the CX5500 system**

<i>Port Number</i>	<i>Protocol</i>	<i>Outgoing</i>	<i>Incoming</i>	<i>UDP or TCP</i>
21	FTP	Provisioning, Logs		TCP

<i>Port Number</i>	<i>Protocol</i>	<i>Outgoing</i>	<i>Incoming</i>	<i>UDP or TCP</i>
22	SSH	Admin	Admin	TCP
53	DNS			UDP
67	DHCP	Server		UDP
68	DHCP	Client		UDP
69	TFTP	Provisioning, Logs		UDP
80	HTTP	Provisioning, Logs, Pull Web interface, Poll		TCP
123	NTP	Time Server		UDP
389	LDAP			
443	HTTPS	Provisioning, Logs	HTTP Pull Web interface, HTTP Push	TCP
514	Syslog	Logs		
636	LDAP			
1023	Telnet	Admin		TCP
2222	RTP <sup>2</sup>	Media Packets	Media Packets	
2223	RTCP <sup>2</sup>	Media Packet Statistics	Media Packet Statistics	
5060	SIP	SIP signaling	SIP signaling	
5061	SIP over TLS	Secure signaling	Secure signaling	

<sup>1</sup> Telnet is disabled by default.

<sup>2</sup> RTP and RTCP can use any even port between 2222 and 2269, but this is configurable by setting `tcpIpApp.port.rtp.mediaPortRangeStart`.

## Power and Startup Issues

The following table describes possible solutions to several power and startup issues.

---

## Troubleshooting Power and Startup Issues

---

### The system has power issues or the system has no power.

Determine if the problem is caused by the system, the AC outlet, or the PoE switch. Do one of the following:

- Verify that no lights appear on the unit when it is powered up.
  - Check if the system is properly plugged into a functional AC outlet.
  - Make sure that the system isn't plugged into an outlet controlled by a light switch that is off.
  - If plugged into a power strip, try plugging directly into a wall outlet instead.
- 

### The system will not boot.

If your system will not boot, there may be a corrupt or invalid firmware image or configuration on the system:

- Ensure that the provisioning server is accessible on the network and a valid software load and valid configuration files are available.
  - Ensure that the system is pointing to the provisioning server on the network.
  - Reboot the system.
- 

## Touch Screen Issues

The LCD touch screen menu includes a panel in which you can test the sensitivity of the touch screen. Navigate to **Settings > Status > Diagnostics > Test Hardware > Touch Screen Diagnostics** to test the touch screen.

## Screen and System Access Issues

The following table describes possible solutions to screen and system access issues.

### Troubleshooting Screen and System Access Issues

---

#### There is no response from feature key presses.

If your system is not in the active state, do one of the following:

- Press the keys more slowly.
  - Check to see whether or not the key has been mapped to a different function or disabled.
  - Make a call to the system to check for inbound call display and ringing. If successful, try to press feature keys while a call is active to access a Directory or Buddy Status, for example.
  - Navigate to **Settings > Status > Lines** to confirm the line is actively registered to the call server.
  - Reboot the system to attempt re-registration to the call server (navigate to **Settings > Advanced > Reboot System**)
-

---

**The display shows the message *Network Link is Down*.**

If you see this message, the LAN cable is not properly connected. Do one of the following:

- Check termination at the switch or hub (furthest end of the cable from the system).
  - Check that the switch or hub is operational (flashing link/status lights).
  - Press **Settings > Status > Network**. Scroll down to verify that the LAN is active.
  - Ping the system from another machine.
  - Reboot the system to attempt re-registration to the call server (navigate to **Settings > Advanced > Reboot System**).
- 

## Calling Issues

The following table provides possible solutions to a number of generic calling issues.

### Troubleshooting Calling Issues

---

**There is no dial tone.**

If there is no dial tone, power may not be correctly supplied to the system, try one of the following:

- Check that the display is illuminated.
  - Make sure the LAN cable is inserted properly at the rear of the system (try unplugging and re-inserting the cable).
  - If using in-line powering, have your system administrator check that the switch is supplying power to the system.
- 

**The system does not ring.**

If there is a no ring tone, but the system displays a visual indication when it receives an incoming call, do the following:

- Adjust the ring level from the front panel using the volume up/down keys.
- 

**The line icon shows an unregistered line icon.**

If you see one of the following icons the system line is unregistered. Register the line and try to place a call.

**Unregistered Line Icon:** 

**Registered Line Icon:** 

---



---

## Display Issues

The following table provides tips for resolving display screen issues.

### Troubleshooting Display Issues

---

#### **There is no display or the display is incorrect.**

If there is no display, power may not be correctly supplied to the system. Do one of the following:

- Check that the display is illuminated.
- Make sure the power is inserted properly in the power data box.
- If using Power over Ethernet (PoE) powering, check that the PoE switch is supplying power to the system.

Use the screen capture feature to determine if the display on the system is incorrect (see [Capture the System's Current Screen](#)).

---

#### **The display is too dark or too light.**

The system contrast may be set incorrectly. To adjust the contrast, do one of the following:

- Adjust the contrast (Refer the system's user guide).
  - Reboot the system to obtain the default level of contrast.
  - Use the screen capture feature to see if the screen displays properly in the capture (see [Capture the System's Current Screen](#)).
- 

#### **The display is flickering.**

Certain types of older fluorescent lighting cause the display to flicker. If your system is in an environment lit with fluorescent lighting, do one of the following:

- Move the CX5500 system away from the lights.
  - Replace the lights.
- 

## Audio Issues

The following table describes possible solutions to audio issues.

### Troubleshooting Audio Issues

---

#### **There are audio or echo issues**

If you experience echo issues, see [Technical Bulletin 16249: Troubleshooting Audio and Echo Issues on SoundPoint IP Systems](#).

---

## Licensed Feature Issues

You need a license for XT9 support. You can check your licenses on the device by navigating to **Settings > Status > Licenses**.

---

## Upgrading Issues

The following table describes several possible solutions to issues that may occur during or after a software upgrade.

### Troubleshooting Software Upgrading Issues

---

#### **Certain settings or features are not working as expected on the system**

The system's configuration may be incorrect or incompatible. Check for errors on the system by navigating to **Settings > Status > Platform > Configuration**. If there are *Errors Found*, *Unknown Params*, or *Invalid values*, correct your configuration files and restart the system.

---

#### **The system displays a *Config file error* message for 5-seconds after it boots up (see the following figure)**

Pre-UC Software 3.3.0 configuration files are being used with UC Software 3.3.0. Specifically, the following parameters are in the configuration files:

- one.chord.ringer.x.freq.1
- se.pat.callProg.x.name
- ind.anim.IP\_500.x.frame.x. duration
- ind.pattern.1.step.x.state
- feature.2.name
- feature.9.name

Also the configuration files contain:

- more than 100 "unknown" parameters
- more than 100 "out-of-range" parameters
- more than 100 "invalid" parameters

Correct the configuration files, remove the invalid parameters, and restart the system.

---

#### **When you are upgrading system software using the Web Configuration Utility, the system is unable to connect to the Polycom Hosted Server.**

Occasionally, the system is unable to connect to the Polycom Hosted Server because:

- The Polycom Hosted Server is temporarily unavailable.
- There isn't any software upgrade information for the system to receive.
- The network configuration is preventing the system from connecting to the Polycom Hosted Server.

*Note: UC Software 4.0.0 does not support internet access for software upgrades through a Web proxy.*

To troubleshoot the issue:

- Try upgrading your system later.
- Verify that new software is available for your system. To check, see the [Polycom UC Software/Polycom SIP Software Release Matrix](#).
- Verify that your network's configuration will allow the system to connect to <http://downloads.polycom.com>.

If the issue persists, try manually upgrading your system's software. To upgrade system software using this method, see [Set Up the Provisioning Server](#).

---

# Maintenance Tasks

---

This section shows you how to maintain the Polycom® UC Software and includes the following topics:

- [Trusted Certificate Authority List](#)
- [Encrypt Configuration Files](#)
- [Internal Key Functions](#)
- [Assign a VLAN ID Using DHCP](#)
- [Parse Vendor ID Information](#)
- [Product, Model, and Part Number Mapping](#)
- [Capture the System's Current Screen](#)
- [LLDP and Supported TLVs](#)

## 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
- Verisign 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



#### **Troubleshooting: My Certificate Authority is Not Listed**

Polycom endeavors to maintain a built-in list of the most commonly used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you may 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. Refer to [Technical Bulletin 17877: Using Custom Certificates on Polycom Systems](#).

# 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 or use Polycom's Software Development Kit (SDK) to generate a key and to encrypt and decrypt configuration files on a UNIX or Linux server. The SDK is distributed as source code that runs under the UNIX operating system.



## Web Info: Using the SDK to Encrypt Configuration Files

To request the SDK and quickly install the generated key, see [Quick Tip 67442: When Encrypting Polycom UC Software Configuration Files](#).

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.



## Troubleshooting: My System Keeps Displaying an Error Message for My Encrypted File

If a system downloads an encrypted file that it cannot decrypt, the action is logged, and an error message displays. The system will continue to do this until the provisioning server provides an encrypted file that can be read, an unencrypted file, or the file is removed from the master configuration file list.

### 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 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.

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 Provisioning the system again so that it will download the new key. The system will automatically reboot 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 will replace them when it successfully boots.

## Internal Key Functions

A complete list of internal key functions for enhanced feature keys and hard key mappings is shown in the following table.

The following guidelines should be noted:

- The **Function** value is case sensitive.
- Some functions are dependent on call state. Generally, if the soft key displays on a call screen, the soft key function is executable.
- CallPickup refers to the soft key function that provides the menu with separate soft keys for parked pickup, directed pickup, and group pickup.
- Some functions depend on the feature being enabled. For example, BuddyStatus and MyStatus require the presence feature to be enabled.
- The table below shows only Line1 to Line6 functions.

### Key Labels and Internal Functions

<i>Function</i>	<i>Description</i>	<i>Notes</i>
ACDAvailable	ACD available from idle	
ACDLogin	Login to ACD	
ACDLogout	Log out of ACD	
ACDUnavailable	ACD unavailable from idle	
Answer	Answer	Call screen only

<i>Function</i>	<i>Description</i>	<i>Notes</i>
Applications	Main Browser	
BuddyStatus	Buddy Status	
CallList	Call Lists	
Conference	Begin a conference call	Call screen only
Delete	Delete	
Dialpad0	Dialpad 0	
Dialpad1	Dialpad 1	
Dialpad2	Dialpad 2	
Dialpad3	Dialpad 3	
Dialpad4	Dialpad 4	
Dialpad5	Dialpad 5	
Dialpad6	Dialpad 6	
Dialpad7	Dialpad 7	
Dialpad8	Dialpad 8	
Dialpad9	Dialpad 9	
DialpadPound	Dialpad pound sign	
DialpadStar	Dialpad star sign	
DialpadURL	Dial name	Call screen only
Directories	Directories	
DoNotDisturb	Do Not Disturb menu	
EnterRecord	Enter a call record	Call screen only
Exit	Exit existing menu	Menu only
Hold	Toggle hold	
Join	Join	Call screen only
Line1	Line Key 1	
Line2	Line Key 2	
Line3	Line Key 3	
Line4	Line Key 4	



<i>Function</i>	<i>Description</i>	<i>Notes</i>
Line5	Line Key 5	
Line6	Line Key 6	
LockSystem	Lock the system	
Messages	Messages menu	
MicMute	Mute the microphone	
MyStatus	View my status	
NewCall	New call	Call screen only
Null	Do nothing	
Offline	Offline for presence	
Page	Group Paging	
QuickSetup	Quick Setup feature	Call screen only
Redial	Redial	Call screen only
Select	Select	
ServerACDAgentAvailable	serverACDAgentAvailable	
ServerACDAgentUnavailable	serverACDAgentUnavailable	
ServerACDSignIn	serverACDSignIn	
ServerACDSignOut	serverACDSignOut	
Setup	Settings menu	
Silence	RingerSilence	Call screen only
SoftKey1	SoftKey 1	
SoftKey2	SoftKey 2	
SoftKey3	SoftKey 3	
SoftKey4	SoftKey 4	
SpeedDial	SpeedDial	
Split	Split	Call screen only
Talk	Push-to-Talk	
Transfer	Transfer	Call screen only
VolDown	Set volume down	

<i>Function</i>	<i>Description</i>	<i>Notes</i>
VolUp	Set volume up	

## Assign a VLAN ID Using DHCP

In deployments where it is not possible or desirable to assign a VLAN statically in the system's network configuration menu or use CDP (Cisco Discovery Protocol) or LLDP (Link-Layer Discovery Protocol) 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.

### To assign a VLAN ID to a system using DHCP:

- » In the DHCP menu of the Main setup menu, set **VLAN Discovery** to **Fixed** or **Custom**.
  - When set to Fixed, the system will examine DHCP options 128,144, 157 and 191 (in that order) for a valid DVD string.
  - When set to Custom, a value set in the **VLAN ID Option** will be examined for a valid DVD string.
    - ◆ 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 ";" will be ignored
      - There must be no white space before the semi colon ";"
      - VLAN IDs may be decimal, hex, or octal
        - ◆ The following DVD strings will result in the system using VLAN 10:

VLAN-A=10;

VLAN-A=0x0a;

VLAN-A=012;



#### **Note: VLAN Tags Assigned by CDP or LLDP**

If a VLAN tag is assigned by CDP or LLDP, DHCP VLAN tags will be 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).

For example, the following is a sample decode of a packet:

```

3c 74
    > Option 60, length of Option data (part of the DHCP spec.)
00 00 36 3d
    > Polycom signature (always 4 octets)
6f
    > Length of Polycom data
01 07 50 6f 6c 79 63 6f 6d
    > sub-option 1 (company), length, "Polycom"
02 15 53 6f 75 6e 64 50 6f 69 6e 74 49 50 2d 53 50 49 50 5f 36 30 31
    > sub-option 2 (part), length, "CX5500"
03 10 32 33 34 35 2d 31 31 36 30 35 2d 30 30 31 2c 32
    > sub-option 3 (part number), length, "2345-11605-001,2"
04 1c 53 49 50 2f 54 69 70 2e 58 58 58 58 2f 30 38 2d 4a 75 6e 2d 30 37 20 31
30 3a 34 34
    > sub-option 4 (Application version), length, "SIP/Tip.XXXX/08-Jun-07 10:44"
05 1d 42 52 2f 33 2e 31 2e 30 2e 58 58 58 58 2f 32 38 2d 41 70 72 2d 30 35 20
31 33 3a 33 30
    > sub-option 5 (BootROM version), length, "BR/3.1.0.XXXX/28-Apr-05

```

13:30"

ff

➤ end of sub-options

For the Updater, sub-option 4 and sub-option 5 will contain the same string. The string is formatted as follows:

```
<apptype>/<buildid>/<date+time>
```

where:

<apptype> can be 'BR' (BootROM) or 'SIP' (SIP Application)

## 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_CX5500="system1_CX5500.cfg, sip_CX5500.cfg"`, which will override `CONFIG_FILES="system1.cfg, sip.cfg"` for the CX5500.

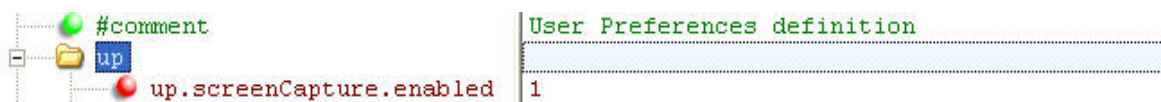
You can also add variables to the master configuration file that are replaced when the system reboots. The variables include `SYSTEM_MODEL`, `SYSTEM_PART_NUMBER`, and `SYSTEM_MAC_ADDRESS`.

## Capture the System's Current Screen

You can capture your system's current screen using a Web browser.

**To capture the system's current screen:**

- 1 Modify your configuration file to enable the screen capture feature.
- 2 Open your configuration file in an XML editor and add the following line:



- 3 Save the configuration file and update your system's configuration.
- 4 On the system, turn on the screen capture feature from the **Screen Capture** menu (**Settings > Basic > Preferences > Screen Capture**).  
Turn the screen capture on again (repeat this step) each time the system restarts or reboots.
- 5 In a Web browser, enter `http://<systemIPAddress>/captureScreen` as the browser address.  
To find your system's IP address, navigate to **Settings > Status > Platform > System**.  
The Web browser displays an image showing the system's current screen. The image can be saved as a BMP or JPEG file.

## 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: Using the LLDP Protocol

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.



### Settings: Enabling VLAN Using Multiple Method

There are four 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); 4. Static (the VLAN ID is entered through the system's user interface).

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 'Telephone' 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 will be recognized as LLDP only if it contains mandatory TLVs. Polycom systems running the UC Software will 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 will 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.

For more information on device configuration parameters, refer to the section [<device/>](#).

## 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	<b>Chassis-Id<sup>1</sup></b>	1	6	<b>0x0206</b>	-	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	<b>Port-Id<sup>1</sup></b>	2	7	<b>0x0407</b>	-	3
	MAC address of system (6 bytes)					
3	<b>TTL</b>	3	2	<b>0x0602</b>	-	-
	TTL value is 120/0 sec					
4	<b>Port description</b>	4	1	<b>0x0801</b>	-	-
	Port description 1					

No	Name	Type(7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Sub Type
5	<b>System name</b>	5	min len > 0, max len <= 255	-	-	-
6	<b>System description</b>	6	min len > 0, max len <= 255	-	-	-
<p>Manufacturer's name - "Polycom"; Refer to <b>Error! Reference source not found.</b>; Hardware version; Application version; BootROM version</p>						
7	<b>Capabilities</b>	7	4	0x0e04	-	-
<p>System Capabilities: Telephone and Bridge if the system has PC port support and it is not disabled. Enabled Capabilities: Telephone and Bridge if system has PC port support, it is not disabled and PC port is connected to PC.</p>						
8	<b>Management Address</b>	8	12	0x100c	-	-
<p>Address String Len - 5, IPV4 subtype, IP address, Interface subtype - "Unknown", Interface number - "0", ODI string Len - "0"</p>						
9	<b>IEEE 802.3 MAC/PHY config/status<sup>1</sup></b>	127	9	0xfe09	0x00120f	1
<p>Auto Negotiation Supported - "1", enabled/disabled, Refer to MD Advertise and Operational MAU.</p>						
10	<b>LLDP-MED capabilities</b>	127	7	0xfe07	0x0012bb	1
<p>Capabilities - 0x33 (LLDP-Med capabilities, Network policy, Extended Power Via MDI-PD, Inventory) Class Type III Note: Once 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</p>						
11	<b>LLDP-MED network policy<sup>2</sup></b>	127	8	0xfe08	0x0012bb	2
<p>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</p>						
12	<b>LLDP-MED network policy<sup>2</sup></b>	127	8	0xfe08	0x0012bb	2
<p>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.</p>						

No	Name	Type(7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Sub Type
13	<b>LLDP-MED network policy<sup>2</sup></b>	127	8	0xfe08	0x0012bb	2
<p>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.</p> <p>Note: Video Conferencing TLV is sent only from Video capable systems.</p>						
14	<b>LLDP-MED location identification<sup>3</sup></b>	127	min len > 0, max len <= 511	-	0x0012bb	3
<p>ELIN data format: 10 digit emergency number configured on the switch. Civic Address: physical address data such as city, street number, and building information.</p>						
15	<b>Extended power via MDI</b>	127	7	0xfe07	0x0012bb	4
<p>PowerType -PD device PowerSource-PSE&amp;local Power Priority -Unknown PowerValue.</p>						
16	<b>LLDP-MED inventory hardware revision</b>	127	min len > 0, max len <= 32	-	0x0012bb	5
<p>Hardware part number and revision</p>						
17	<b>LLDP-MED inventory firmware revision</b>	127	min len > 0, max len <= 32	-	0x0012bb	6
<p>BootROM revision</p>						
18	<b>LLDP-MED inventory software revision</b>	127	min len > 0, max len <= 32	-	0x0012bb	7
<p>Application (SIP) revision</p>						
19	<b>LLDP-MED inventory serial number</b>	127	min len > 0, max len <= 32	-	0x0012bb	8
<p>MAC Address (ASCII string)</p>						
20	<b>LLDP-MED inventory manufacturer name</b>	127	11	0xfe0b	0x0012bb	9
<p>Polycom</p>						
21	<b>LLDP-MED inventory model name</b>	127	min len > 0, max len <= 32	-	0x0012bb	10
22	<b>LLDP-MED inventory asset ID</b>	127	4	0xfe08	0x0012bb	11
<p>Empty (Zero length string)</p>						



No	Name	Type(7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Sub Type
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.

## MD Advertise and Operational MAU

The following table lists values for the PMD Advertise and Operational MAU.

### PMD Advertise and Operation 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: Default PMD Advertise Capability Values**

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 UC Software configuration parameters used to configure all system features and functions. This section is useful if you want to read a detailed description of a particular configuration parameter or you would like to see the default or permitted values for that parameter. If you want to configure a specific feature, see the following sections:

- [Set Up Basic System Features](#)
- [Set Up Advanced System Features](#)
- [Set Up System Audio Features](#)
- [Set Up User and System Security Features](#)

## <apps/>

The following table lists <apps/> parameters you can use to control system notification events, state polling events, and push server controls. For more information, see the [Polycom Web Application Developer's Guide](#).

### Application Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>apps.statePolling.password</b>	<b>string</b>	<b>null</b>
Enter the password that the system requires to authenticate system state polling.		
<b>apps.statePolling.URL</b>	<b>URL</b>	<b>null</b>
The URL to which the system sends call processing state/device/network information. The protocol used can be either HTTP or HTTPS. Note: To enable state polling, the parameters <code>apps.statePolling.URL</code> , <code>apps.statePolling.username</code> , and <code>apps.statePolling.password</code> must be set to non-null values.		
<b>apps.statePoling.responseMode</b>	<b>0 or 1</b>	<b>1</b>
The mode of sending requested polled data. If 1, requested polled data is sent to a configured URL. If 0, the data is sent in the HTTP response.		
<b>apps.statePolling.username</b>	<b>string</b>	<b>null</b>
Enter the user name that the system requires to authenticate system state polling.		
<b>apps.telNotification.callStateChangeEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, call state change notification is disabled. If 1, notification is enabled.		
<b>apps.telNotification.incomingEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, incoming call notification is disabled. If 1, notification is enabled.		
<b>apps.telNotification.lineRegistrationEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, line registration notification is disabled. If 1, notification is enabled.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>apps.telNotification.networkUpEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, network up notification is disabled. If 1, notification is enabled.		
<b>apps.telNotification.offhookEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, off-hook notification is disabled. If 1, notification is enabled.		
<b>apps.telNotification.onhookEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, on-hook notification is disabled. If 1, notification is enabled.		
<b>apps.telNotification.outgoingEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, outgoing call notification is disabled. If 1, notification is enabled.		
<b>apps.telNotification.uiInitializationEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, user interface initialization notification is disabled. If 1, notification is enabled.		
<b>apps.telNotification.URL</b>	<b>URL</b>	<b>null</b>
The URL to which the system sends notifications of specified events. Can be either HTTP or HTTPS.		
<b>apps.telNotification.x.URL</b>	<b>URL</b>	<b>null</b>
The URL to which the system sends notifications of specified events, where x 1 to 9. Can be either HTTP or HTTPS.		
<b>apps.telNotification.userLogInOutEvent</b>	<b>0 or 1</b>	<b>0</b>
If 0, user login/logout notification is disabled. If 1, notification is enabled.		
<b>apps.ucdesktop.adminEnabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the Polycom Desktop Connector is disabled on the administrative level. If 1, it is enabled on the administrative level.		
<b>apps.ucdesktop.desktopUserName</b>	<b>string</b>	<b>null</b>
The user's name, supplied from the user's computer. For example, bsmith.		
<b>apps.ucdesktop.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the Polycom Desktop Connector is disabled for users. If 1, it is enabled for users.		
<b>apps.ucdesktop.ServerAddress</b>	<b>string</b>	<b>null</b>
The user's computer as a fully qualified domain name (FQDN). For example, computer@yourcompany.com.		
<b>apps.ucdesktop.ServerPort</b>	<b>1 to 65535</b>	<b>24800</b>
The port number. Note: This value should be the same as the one that is used on the user's computer, otherwise the connection is not established.		

<sup>1</sup> Change causes system to restart or reboot.

## <bg/>

The parameters listed in the following table define the backgrounds you can display on the CX5500 system.

### Background Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>bg.color.selection</b>	<b>w,x</b>	<b>1,1</b>
<p>Set the background. Specify which type of background (w) and index (x) for that type is selected on reboot. The default selection is 2,1 the first solid background.</p> <p>Use w=1 and x=1 (1,1) to select the built-in image.</p> <p>Use w=2 and x= 1 to 6 to select one of the six background <i>bm</i> images.</p>		
<b>bg.color.bm.x.name</b>	<b>URL or file path of a BMP or PNG image</b>	
<b>System screen background image file</b>		
<p>The name of the image file (including extension). The six (x: 1 to 6) default screen background images are:</p> <p>x=1: Leaf.png  x=2: Sailboat.png  x=3: Beach.png  x=4: Palm.png  x=5: Jellyfish.png  x=6: Mountain.png</p> <p>Note: If the file is missing or unavailable, the built-in default solid pattern is displayed.</p>		

## <button/>

You can configure the color of line keys and soft keys using the <button/> parameter using the parameters in the following table.

### Soft Key Button Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>button.color.selection.x.y.modify</b>	<b>any string</b>	
<p>The label color for soft keys and line key labels associated with the defined colored backgrounds. These values can be modified locally by the user.</p> <p>The format is: rgbHILo, &lt;parameter list&gt;. For example: rgbHiLo, 51, 255, 68, 255, 0, 119 is the default button color associated with the built-in background.</p>		
<b>button.gray.selection.x.y.modify</b>	<b>any string</b>	
<p>The label color for soft keys and line key labels associated with the defined gray backgrounds. These values can be modified locally by the user.</p> <p>The format is: rgbHILo, &lt;parameter list&gt;. By default, all defaults are set to none.</p>		

## <call/>

The system supports an optional per-registration feature that enables automatic call placement when the system is off-hook.

The system supports a per-registration configuration that determines which events will cause the missed-calls counter to increment.

You can enable/disable missed call tracking on a per-line basis.

The following table defines per-site and per-system configuration parameters. In the following table, x is the registration number. For the CX5500 system, x=1-16.

### Call Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>call.advancedMissedCalls.addToReceivedList</b>	<b>0 or 1</b>	<b>0</b>
Applies to calls on that are answered remotely. If 0, calls answered from the remote system are not added to the local receive call list. If 1, calls answered from the remote system are added to the local receive call list.		
<b>call.advancedMissedCalls.enabled</b>	<b>0 or 1</b>	<b>1</b>
If 1, improved missed call handling for shared lines is enabled (shared lines can correctly count missed calls). If 0, the old missed call handling is used for shared lines (shared lines may not correctly count missed calls).		
<b>call.advancedMissedCalls.reasonCodes</b>	<b>comma-separated list of indexes</b>	<b>200</b>
A comma separated list of reason code indexes that are interpreted to mean that a call should not be considered as a missed call.		
<b>call.autoAnswer.micMute</b>	<b>0 or 1</b>	<b>1</b>
If 0, the microphone is active immediately after a call is auto-answered. If 1, the microphone is initially muted after a call is auto-answered.		
<b>call.autoAnswer.ringClass</b>	<b>see the list of ring classes in &lt;rt/&gt;</b>	<b>ringAutoAnswer</b>
The ring class to use when a call is to be automatically answered using the auto-answer feature. If set to a ring class with a type other than <code>answer</code> or <code>ring-answer</code> , the setting will be overridden such that a ringtone of <code>visual</code> (no ringer) applies.		
<b>call.autoOffHook.x.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>Enable or disable the feature</b>		
<b>call.autoOffHook.x.contact<sup>1</sup></b>	<b>a SIP URL</b>	<b>Null</b>
<b>The contact address to where the call is placed</b>		
<b>call.autoOffHook.x.protocol<sup>1</sup></b>	<b>SIP</b>	<b>Null</b>
<b>The calling protocol to use</b>		
If <code>enabled</code> is set to 0, no call is placed automatically when the system goes off hook, and the other parameters are ignored. If <code>enabled</code> is set to 1, a call is automatically placed to the <code>contact</code> using the calling <code>protocol</code> , when the system goes off hook.		
The <code>contact</code> must be an ASCII-encoded string containing digits, either the user part of a SIP URL (for example, 6416), or a full SIP URL (for example, 6416@polycom.com).		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>call.callsPerLineKey</b>	<b>1-4, 1-8, 1-24</b>	<b>4, 8, 24</b>
Set the maximum number of concurrent calls per line key. This parameter applies to all registered lines. The permitted range is 1 to 8 and the default is 8. Note that this parameter may be overridden by the per-registration parameter of <code>reg.x.callsPerLineKey</code> .		
<b>call.callWaiting.enable</b>	<b>0 or 1</b>	<b>1</b>
If 1, the system alerts you to an incoming call while you are in an active call. If 0, you are not alerted to incoming calls while in an active call and the incoming call is treated as if you did not answer it. If 1, and you end the active call during a second incoming call, you are alerted to the second incoming call.		
<b>call.callWaiting.ring<sup>1</sup></b>	<b>beep, ring, silent</b>	<b>beep</b>
Specifies the ringtone of incoming calls when another call is active. If set to Null, the default value is beep.		
<b>call.dialtoneTimeOut<sup>1</sup></b>	<b>positive integer</b>	<b>60</b>
The time is seconds that a dial tone will play before a call is dropped. If set to 0, the call is not dropped.		
<b>call.directedCallPickupString<sup>1</sup></b>	<b>star code</b>	<b>*97</b>
The star code to initiate a directed call pickup. Note: The default value supports the BroadWorks calls server only. You must change the value if your organization uses a different call server.		
<b>call.donotdisturb.perReg<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
This parameter determines if the Do-Not-Disturb feature will apply to all registrations on the system (globally), or apply on a per-registration basis. If 0, DND will apply to all registrations on the system when it is active. If 1, the user can activate DND on a per-registration basis. Note: If <code>voIpProt.SIP.serverFeatureControl.dnd</code> is set to 1 (enabled), this parameter is ignored.		
<b>call.enableOnNotRegistered<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 1, users can make calls when the system is not registered. If 0, calls are not permitted without registration.		
<b>call.hold.localReminder.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 1, users are reminded of calls that have been on hold for an extended period of time. If 0, there is no hold reminder.		
<b>call.hold.localReminder.period<sup>1</sup></b>	<b>non-negative integer</b>	<b>60</b>
Specify the time in seconds between subsequent hold reminders.		
<b>call.hold.localReminder.startDelay<sup>1</sup></b>	<b>non-negative integer</b>	<b>90</b>
Specify a time in seconds to wait before the initial hold reminder.		
<b>call.internationalDialing.enabled</b>	<b>0 or 1</b>	<b>1</b>
Use this parameter to enable or disable the key tap timer that converts a double tap of the asterisk "*" symbol to the "+" symbol used to indicate an international call. By default, this parameter is enabled so that a quick double tap of "*" converts immediately to "+". To enter a double asterisk "**", tap "*" once and wait for the key tap timer to expire to enter a second "*". When you disable this parameter, you cannot dial "+" and you must enter the international exit code of the country you are calling from to make international calls. Changes you make to this parameter cause a restart or reboot. Note that this parameter applies to all numeric dial pads on the system, including for example, the contact directory.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>call.lastCallReturnString<sup>1</sup></b>	<b>string of maximum length 32</b>	<b>*69</b>
The string sent to the server when the user selects the last call return action. The string is usually a star code.		
<b>call.localConferenceCallHold<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 0, a hold will happen for all legs when conference is put on hold. If set to 1, only the host is out of the conference, all other parties in conference continue to talk.		
<b>call.localConferenceEnabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 0, the Conference and Join soft keys do not display during an active call and you cannot establish conferences on the system. If set to 1, the Conference and Join soft keys display during an active call and you can establish conferences on the system.		
<b>call.missedCallTracking.x.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, missed call tracking is enabled. If <code>call.missedCallTracking.x.enabled</code> is set to 0, then missedCall counter is not updated regardless of what <code>call.serverMissedCalls.x.enabled</code> is set to (and regardless of how the server is configured). There is no Missed Call List provided under <b>Settings &gt; Features</b> of the system. If <code>call.missedCallTracking.x.enabled</code> is set to 1 and <code>call.serverMissedCalls.x.enabled</code> is set to 0, then the number of missedCall counter is incremented regardless of how the server is configured. If <code>call.missedCallTracking.x.enabled</code> is set to 1 and <code>call.serverMissedCalls.x.enabled</code> is set to 1, then the handling of missedCalls depends on how the server is configured.		
<b>call.offeringTimeOut<sup>1</sup></b>	<b>positive integer</b>	<b>60</b>
Specify a time in seconds that an incoming call will ring before the call is dropped, 0=infinite. Note: The call diversion, no answer feature will take precedence over this feature if enabled.		
<b>call.parkedCallRetrieveString<sup>1</sup></b>	<b>star code</b>	<b>Null</b>
The star code used to initiate retrieval of a parked call.		
<b>call.rejectBusyOnDnd<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 1, and DND is turned on, the system rejects incoming calls with a busy signal. If set to 0, and DND is turned on, the system gives a visual alert of incoming calls and no audio ringtone alert. Note: This parameter does not apply to shared lines since not all users may want DND enabled.		
<b>call.ringBackTimeOut<sup>1</sup></b>	<b>positive integer</b>	<b>60</b>
Specify a time in seconds to allow an outgoing call to remain in the ringback state before dropping the call, 0=infinite.		
<b>call.serverMissedCall.x.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, all missed-call events will increment the counter. If set to 1, only missed-call events sent by the server will increment the counter. Note: This feature is supported with the BroadSoft® Synergy call server only (previously known as Sylanro).		
<b>call.shared.disableDivert<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, the diversion feature for shared lines is disabled. Note: This feature is disabled on most call servers.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>call.shared.exposeAutoHolds<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 1, a re-INVITE will be sent to the server when setting up a conference on a shared line. If 0, no re-INVITE will be sent to the server.		
<b>call.shared.oneTouchResume<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, all users on a shared line can resume held calls by pressing the shared line key. If more than one call is on hold, the first held call is selected and resumed. If set to 0, selecting the shared line opens all current calls that the user can choose from.		
<b>call.shared.seizeFailReorder<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, play re-order tone locally on shared line seize failure.		
<b>call.singleKeyPressConference<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the conference will be setup after a user presses the <b>Conference</b> soft key or <b>Conference</b> key the first time. Also, all sound effects (dial tone, DTMF tone while dialing and ringing back) are heard by all existing participants in the conference. If set to 0, sound effects are only heard by conference initiator (original behavior).		
<b>call.stickyAutoLineSeize<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the system uses sticky line seize behavior. This will help with features that need a second call object to work with. The system will attempt to initiate a new outgoing call on the same SIP line that is currently in focus on the LCD (this was the behavior in SIP 1.6.5). Dialing through the call list when there is no active call will use the line index for the previous call. Dialing through the call list when there is an active call will use the current active call line index. Dialing through the contact directory will use the current active call line index. If set to 0, the feature is disabled (this was the behavior in SIP 1.6.6). Dialing through the call list will use the line index for the previous call. Dialing through the contact directory will use a random line index. Note: This may fail due to glare issues in which case the system may select a different available line for the call.		
<b>call.stickyAutoLineSeize.onHookDialing<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If <code>call.stickyAutoLineSeize</code> is set to 1, this parameter has no effect. The regular <code>stickyAutoLineSeize</code> behavior is followed. If <code>call.stickyAutoLineSeize</code> is set to 0 and this parameter is set to 1, this overrides the <code>stickyAutoLineSeize</code> behavior for hot dial only. (Any new call scenario seizes the next available line.) If <code>call.stickyAutoLineSeize</code> is set to 0 and this parameter is set to 0, there is no difference between hot dial and new call scenarios. Note: A hot dial occurs on the line which is currently in the call appearance. Any new call scenario seizes the next available line.		
<b>call.transferOnConferenceEnd<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
The behavior when the conference host exits a conference. If 0, all parties are disconnected when the conference host exits the conference. If 1, the other parties are left connected when the host exits the conference (the host performs an attended transfer to the other parties).		
<b>call.urlModeDialing<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, URL dialing is disabled. If 1, URL dialing is enabled.		

<sup>1</sup> Change causes system to restart or reboot.



## <callLists/>

The call lists (or call log) parameters are listed in the following table.

### Call List Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>callLists.collapseDuplicates</b>	<b>0 or 1</b>	<b>1</b>
If 0, all calls are archived and presented in the call lists. If 1, consecutive incomplete between the same party in the same direction (outgoing/incoming) are collapsed into one record with the most recent call displaying.		
<b>callLists.logConsulationCalls</b>	<b>0 or 1</b>	<b>0</b>
If 1, all consultation calls are logged. (Calls made to a third party—while the original party is on hold—when settings up a conference call are called consultation calls.) If 0, consultation calls are not logged.		
<b>callLists.size</b>	<b>10 to 99</b>	<b>99</b>
The maximum number of retained records of each type (incoming, outgoing, and missed). When the maximum number is reached, new records will overwrite existing records. You can clear the list using the system's menu system. If you want to prevent the records from uploading to the provisioning server, enter a false URL in the CALL_LISTS_DIRECTORY field in the master configuration file.		
<b>callLists.writeDelay.journal</b>	<b>1 to 600</b>	<b>5</b>
The delay (in seconds) before changes due to an in-progress call are flushed to the file system as a journal.		
<b>callLists.writeDelay.terminated</b>	<b>10 to 600</b>	<b>60</b>
The minimum period between writing out the complete XML file to the local file system and, optionally, to the provisioning server.		

## <device/>

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



### Web Info: Default Device Parameter Values

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 Shipping Configuration Notice at [Polycom Engineering Advisories and Technical Notifications](#).

Polycom provides a global `device.set` parameter that you can enable for software installation and changes to device parameters. Once you have completed the software installation or made configuration changes to device parameters, remove `device.set`. Disabling the parameter after the initial software installation prevents the systems from rebooting and triggering a reset of device parameters that users may have changed after the initial installation.

Each `<device/>` parameter has a corresponding `.set` parameter that enables or disables the value for that device parameter. Enable the corresponding `.set` parameter for each parameter you want to apply.



**Settings: Each `<device/>` Parameter has a Corresponding `.set` Parameter with One Exception**

Note that 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 both `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 will display 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.

## Type of Device Parameters

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

### Device Parameter Types

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.set<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 0, do not use any <code>device.xxx</code> fields to set any parameters. Set this to 0 after the initial software installation. If set to 1, use the <code>device.xxx</code> fields that have <code>device.xxx.set=1</code> . Set this to 1 only for the initial software installation.		
<b>device.xxx<sup>1</sup></b>	<b>string</b>	<b>Null</b>
Configuration parameter.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.xxx.set<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>

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`.

<sup>1</sup> Change causes system to restart or reboot

## Device Parameters

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

### Device Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.auth.localAdminPassword</b>	<b>string (32 character max)</b>	<b>Null</b>
The system's local administrative password. The minimum length is defined by <a href="#">sec.pwd.length.admin</a> .		
<b>device.auth.localUserPassword</b>	<b>string (32 character max)</b>	<b>Null</b>
The system user's local password. The minimum length is defined by <a href="#">sec.pwd.length.user</a> .		
<b>device.baseProfile</b>	<b>Generic, Lync</b>	<b>Null</b>
Choose the Base Profile that the system will operate with.		
<b>device.dhcp.bootSrvOpt<sup>1</sup></b>	<b>Null, 128 to 254</b>	<b>Null</b>
When the boot server is set to Custom or Custom+Option66, specify the numeric DHCP option that the system will look for.		
<b>device.dhcp.bootSrvOptType<sup>1</sup></b>	<b>IP or String</b>	<b>Null</b>
The type of DHCP option in which the system will look for its provisioning server (if <code>device.dhcp.bootSrvUseOpt</code> 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 <code>device.prov.serverName</code> .		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.dhcp.bootSrvUseOpt<sup>1</sup></b>	<b>Default, Custom, Static, CustomAndDefault</b>	<b>Null</b>
<p><b>Default</b> The system will look 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 <code>device.prov.serverName</code>.</p> <p><b>Custom</b> The system will look for the option number specified by <code>device.dhcp.bootSrvOpt</code>, and the type specified by <code>device.dhcp.bootSrvOptType</code> in the response received from the DHCP server.</p> <p><b>Static</b> The system will use the boot server configured through the provisioning server <code>device.prov.*</code> parameters.</p> <p><b>Custom and Default</b> The system will use the custom option first or use Option 66 if the custom option is not present.</p>		
<b>device.dhcp.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>Null</b>
If 0, DHCP is disabled. If 1, DHCP is enabled.		
<b>device.dhcp.option60Type<sup>1</sup></b>	<b>Binary, ASCII</b>	<b>Null</b>
The DHCP option 60 type. <b>Binary</b> : vendor-identifying information is in the format defined in <a href="#">RFC 3925</a> . <b>ASCII</b> : vendor-identifying information is in ASCII format.		
<b>device.dhcp.dhcpVlanDiscUseOpt<sup>1</sup></b>	<b>Disabled, Fixed, Custom</b>	<b>Null</b>
VLAN Discovery. <b>Disabled</b> , no VLAN discovery through DHCP. <b>Fixed</b> , use predefined DHCP vendor-specific option values of 128, 144, 157 and 191 ( <code>device.dhcp.dhcpVlanDiscOpt</code> will be ignored). <b>Custom</b> , use the number specified by <code>device.dhcp.dhcpVlanDiscOpt</code> .		
<b>device.dhcp.dhcpVlanDiscOpt<sup>1</sup></b>	<b>128 to 254</b>	<b>Null</b>
The DHCP private option to use when <code>device.dhcp.dhcpVlanDiscUseOpt</code> is set to <b>Custom</b> .		
<b>device.dns.altSrvAddress<sup>1</sup></b>	<b>server address</b>	<b>Null</b>
The secondary server to which the system directs Domain Name System (DNS) queries.		
<b>device.dns.domain<sup>1</sup></b>	<b>string</b>	<b>Null</b>
The system's DNS domain.		
<b>device.dns.serverAddress<sup>1</sup></b>	<b>string</b>	<b>Null</b>
The primary server to which the system directs Domain Name System queries.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.host.hostname<sup>1</sup></b>	<b>string</b>	<b>Null</b>
<p>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 <code>device.host.hostname.set=1</code>, and <code>device.host.hostname=Null</code>, the DHCP client uses Option 12 to send a predefined hostname to the DHCP registration server using <code>Polycom_&lt;MACaddress&gt;</code>. Note that the maximum length of the hostname string is &lt;=255 bytes. The valid character set is defined in RFC1035.</p>		
<b>device.local.usbConnectionResetInterval</b>	<b>-1 or 86400 to 72800</b>	<b>-1</b>
<p>The intervals (in seconds) when the system will reboot to resolve any USB connection issues.</p>		
<b>device.local.usbConnectionResetTime</b>	<b>0 to 2400hrs</b>	<b>0</b>
<p>The set time when the system will reboot to resolve any USB connection issues.</p>		
<b>device.local.panoviewEnable</b>	<b>0 or 1</b>	<b>1</b>
<p>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.</p>		
<b>device.local.usb3Optimize</b>	<b>0 or 1</b>	<b>0</b>
<p>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.</p>		
<b>device.local.enableMacSupport</b>	<b>0 or 1</b>	<b>1</b>
<p>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.</p>		
<b>device.local.fishEyeEnable</b>	<b>0 or 1</b>	<b>1</b>
<p>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 0, Fisheye Correction is disabled, and Active Speaker video appears distorted.</p>		
<b>device.local.ntpEnabled</b>	<b>0 or 1</b>	<b>0</b>
<p>Enables Network Time Protocol (NTP). If set to 1, NTP is enabled. If set to 0, NTP is disabled.</p>		
<b>device.local.ntpServer</b>	<b>String</b>	<b>Null</b>
<p>Sets the NTP server that is used when the parameter <code>device.local.ntpEnable</code> is enabled.</p>		
<b>device.local.deviceName</b>	<b>String</b>	<b>Null</b>
<p>Sets the device name for each system.</p>		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.local.updateServer</b>	<b>String</b>	<b>http://download s.polycom.com/ voice/millenniu m_cx_series</b>
Sets the server URL the system uses to retrieve software updates.		
<b>device.local.autoUpdateEnabled</b>	<b>0 or 1</b>	<b>0</b>
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.		
<b>device.local.updateInterval</b>	<b>-1 or a number greater than or equal to 0.</b>	<b>-1 = never</b>
Sets the frequency for how often the system checks for software updates on the server.		
<b>device.local.updateTime</b>	<b>A number greater than or equal to 0</b>	<b>0</b>
Sets the time when the system checks for software updates.		
<b>device.local.muteType</b>	<b>0 = Audio only 1 = Audio and Video</b>	<b>0</b>
Sets the function of the Mute button on the system.		
<b>device.local.lightingFrequency</b>	<b>0, 1, or 2 0 = 50Hz 1 = 60HZ 2 = 50HZ at 30fps</b>	<b>0</b>
Sets the power frequency of the system.		
<b>device.logincred.password</b>	<b>string</b>	<b>Null</b>
The user password that the system uses to connect to the provisioning server.		
<b>device.logincred.user</b>	<b>string</b>	<b>Null</b>
The user name that the system uses to connect to the provisioning server.		
<b>device.net.cdpEnabled<sup>1</sup></b>	<b>0 or 1</b>	<b>Null</b>
If set to 1, the system will attempt to determine its VLAN ID and negotiate power through CDP.		
<b>device.net.dot1x.anonid<sup>1</sup></b>	<b>string</b>	<b>Null</b>
EAP-TTLS and EAP-FAST only. The anonymous identity (user name) for 802.1X authentication.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.net.dot1x.eapFastInBandProv<sup>1</sup></b>	<b>0 or 1</b>	<b>Null</b>
EAP-FAST only, optional. Choose 1 to enable EAP In-Band Provisioning by server unauthenticated PAC provisioning using anonymous Diffie-Hellman key exchange. Choose 0 to disable EAP In-Band Provisioning. Reserved for Future Use—Choose 2 to enable EAP In-band provisioning by server authenticated PAC provisioning using certificate based server authentication.		
<b>device.net.dot1x.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>Null</b>
If 0, 802.1X authentication is disabled. If 1, 802.1X authentication is enabled.		
<b>device.net.dot1x.identity<sup>1</sup></b>	<b>string</b>	<b>Null</b>
The identity (user name) for 802.1X authentication.		
<b>device.net.dot1x.method</b>	<b>EAP-None, EAP-TLS, EAP-PEAPv0- MSCHAPv2, EAP-PEAPv0- GTC, EAP-TTLS- MSCHAPv2, EAP-TTLS- GTC, EAP- FAST, EAP- MD5</b>	<b>Null</b>
Specify the 802.1X authentication method, where <code>EAP-NONE</code> means no authentication.		
<b>device.net.dot1x.password<sup>1</sup></b>	<b>string</b>	<b>Null</b>
The password for 802.1X authentication. This parameter is required for all methods except EAP-TLS.		
<b>device.net.ether1000BTClockLAN<sup>1</sup></b>	<b>Auto, Slave, Master</b>	<b>Null</b>
The mode of the LAN clock. Polycom recommends that you do not change this value unless you have Ethernet connectivity issues.		
<b>device.net.ether1000BTClockPC<sup>1</sup></b>	<b>Auto, Slave, Master</b>	<b>Null</b>
The mode of the PC clock. Polycom recommends that you do not change this value unless you have Ethernet connectivity issues.		
<b>device.net.etherModeLAN<sup>1</sup></b>	<b>Auto, 10HD, 10FD, 100HD, 100FD, 100FD</b>	<b>Null</b>
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.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.net.etherModePC<sup>1</sup></b>	<b>Disabled, Auto, 10HD, 10FD, 100HD, 100FD, 100FD</b>	<b>Auto</b>
The PC port mode that sets the network speed over Ethernet. If set to <code>Disabled</code> , the PC port is disabled. HD means half duplex and FD means full duplex.		
<b>device.net.etherStormFilter<sup>1</sup></b>	<b>0 or 1</b>	<b>Null</b>
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.		
<b>device.net.ipAddress<sup>1</sup></b>	<b>string</b>	<b>Null</b>
The system's IP address. Note: This parameter is disabled when DHCP is enabled ( <code>device.dhcp.enabled</code> is set to 1).		
<b>device.net.IPgateway<sup>1</sup></b>	<b>dotted-decimal IP address</b>	<b>Null</b>
The system's default router.		
<b>device.net.lldpEnabled<sup>1</sup></b>	<b>0 or 1</b>	<b>Null</b>
If set to 1, the system will attempt to determine its VLAN ID and negotiate power through LLDP.		
<b>device.net.subnetMask<sup>1</sup></b>	<b>dotted-decimal subnet mask</b>	<b>Null</b>
The system's subnet mask. Note: This parameter is disabled when DHCP is enabled ( <code>device.dhcp.enabled</code> is set to 1).		
<b>device.net.vlanId<sup>1</sup></b>	<b>Null, 0-4094</b>	<b>Null</b>
The system's 802.1Q VLAN identifier. If Null, no VLAN tagging.		
<b>device.pacfile.data<sup>1</sup></b>	<b>String</b>	<b>Null</b>
EAP-FAST only, optional. The PAC file (base 64 encoded). To generate a base 64-encoded PAC file, generate the PAC file using your authentication server and then convert it to base 64. You can convert the file to base 64 using the following openssl commands: <pre>\$ openssl enc -base64 -in myfile -out myfile.b64</pre>		
<b>device.pacfile.password<sup>1</sup></b>	<b>String</b>	<b>Null</b>
EAP-FAST only, optional. The password for the PAC file.		
<b>device.prov.maxRedunServers<sup>1</sup></b>	<b>1 to 8</b>	<b>Null</b>
The maximum number of IP addresses that will be used from the DNS.		
<b>device.prov.lyncDeviceUpdateEnabled.set</b>	<b>0 or 1</b>	<b>1</b>
If set to 1, the system will attempt to check for the latest version available on update server.		



<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.prov.password<sup>1</sup></b>	<b>string</b>	<b>Null</b>
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 will re-provision. The system may also reboot if the configuration on the provisioning server has changed.		
<b>device.prov.redunAttemptLimit<sup>1</sup></b>	<b>1 to 10</b>	<b>Null</b>
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.		
<b>device.prov.redunInterAttemptDelay<sup>1</sup></b>	<b>0 to 300</b>	<b>Null</b>
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.		
<b>device.prov.serverName</b>	<b>dotted-decimal IP address, domain name string, or URL</b>	<b>Null</b>
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 ( <code>device.dhcp.enabled</code> is 0), if the DHCP server does not send a boot server option, or if the boot server option is static ( <code>device.dhcp.bootSrvUseOpt</code> is <code>static</code> ). Note: If you modify this parameter, the system will re-provision. The system may also reboot if the configuration on the provisioning server has changed.		
<b>device.prov.serverType<sup>1</sup></b>	<b>FTP, TFTP, HTTP, HTTPS, FTPS</b>	<b>Null</b>
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.		
<b>device.prov.upgradeServer</b>	<b>string</b>	<b>Null</b>
The server used by the Polycom Web Configuration Utility's software upgrade feature. The server checks this URL for new software files.		
<b>device.prov.tagSerialNo</b>	<b>0 or 1</b>	<b>Null</b>
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.		
<b>device.prov.user</b>	<b>string</b>	<b>Null</b>
The user name required for the system to log in to the provisioning server (if required). Note: If you modify this parameter, the system will re-provision. The system may also reboot if the configuration on the provisioning server has changed.		
<b>device.prov.ztpEnabled</b>	<b>0 or 1</b>	<b>Null</b>
If 0, Disable the ZTP feature. If 1, enable the ZTP feature.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.sec.configEncryption.key<sup>1</sup></b>	<b>string</b>	<b>Null</b>
The configuration encryption key used to encrypt configuration files. For more information, see Encrypt Configuration Files.		
<b>device.sec.TLS.customCaCert1 (TLS Platform Profile 1)</b> <b>device.sec.TLS.customCaCert2 (TLS Platform Profile 2)</b>	<b>string, PEM format</b>	<b>Null</b>
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.		
<b>device.sec.TLS.customDeviceCert1.publicCert</b> <b>device.sec.TLS.customDeviceCert2.publicCert</b>	<b>Enter the signed custom device certificate in PEM format (X.509)</b>	<b>Null</b>
<b>device.sec.TLS.customDeviceCert1.privateKey</b> <b>device.sec.TLS.customDeviceCert2.privateKey</b>	<b>Enter the corresponding signed private key in PEM format (X.509)</b>	<b>Null</b>
<b>device.sec.TLS.customDeviceCert1.set</b> <b>device.sec.TLS.customDeviceCert2.set</b>	<b>0 or 1</b>	<b>0</b>
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 will enable or disable that parameter. Size constraints are: 4096 bytes for the private key, 8192 bytes for the device certificate.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.sec.TLS.profile.caCertList1 (TLS Platform Profile 1)</b> <b>device.sec.TLS.profile.caCertList2 (TLS Platform Profile 2)</b>	<b>Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1AndPlatform2</b>	<b>Null</b>
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		
<b>device.sec.TLS.profile.cipherSuite1 (TLS Platform Profile 1)</b> <b>device.sec.TLS.profile.cipherSuite2 (TLS Platform Profile 2)</b>	<b>string</b>	<b>Null</b>
The cipher suites to use for TLS Platform Profile 1 and TLS Platform Profile 2)		
<b>device.sec.TLS.profile.cipherSuiteDefault1 (TLS Platform Profile 1)</b> <b>device.sec.TLS.profile.cipherSuiteDefault2 (TLS Platform Profile 2)</b>	<b>0 or 1</b>	<b>Null</b>
The cipher suite to use for TLS Platform Profile 1 and TLS Platform profile 2. If set to 0, the custom cipher suite will be used. If set to 1, the default cipher suite will be used.		
<b>device.sec.TLS.profile.deviceCert1 (TLS Platform Profile 1)</b> <b>device.sec.TLS.profile.deviceCert2 (TLS Platform Profile 2)</b>	<b>Builtin, Platform1, Platform2</b>	<b>Null</b>
Choose the device certificate(s) for TLS Platform Profile 1 and TLS Platform Profile 2 to use for authentication.		
<b>device.sec.TLS.profile.profileSelection.dot1x</b>	<b>PlatformProfile1, PlatformProfile2</b>	<b>Null</b>
Choose the TLS Platform Profile to use for 802.1X, either TLS Platform Profile 1 or TLS Platform Profile 2.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.sec.TLS.profileSelection.provisioning<sup>1</sup></b>	<b>PlatformProfile1, PlatformProfile2</b>	<b>Null</b>
The TLS Platform Profile to use for provisioning, either TLS Platform Profile 1 or TLS Platform Profile 2.		
<b>device.sec.TLS.profileSelection.syslog<sup>1</sup></b>	<b>PlatformProfile1, PlatformProfile2</b>	<b>Null</b>
The TLS Platform Profile to use for syslog, either TLS Platform Profile 1 or TLS Platform Profile 2.		
<b>device.sec.TLS.prov.strictCertificateValidation</b>	<b>0 or 1</b>	<b>1</b>
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.		
<b>device.sec.TLS.syslog.strictCertificateValidation</b>	<b>0 or 1</b>	<b>1</b>
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.		
<b>device.snmp.gmtOffset</b>	<b>-43200 to 46800</b>	<b>Null</b>
The GMT offset—in seconds—to use for daylight savings time, corresponding to -12 to +13 hours.		
<b>device.snmp.serverName</b>	<b>dotted- decimal IP address or domain name string</b>	<b>Null</b>
The SNMP server from which the system will obtain the current time.		
<b>device.syslog.facility</b>	<b>0 to 23</b>	<b>Null</b>
A description of what generated the log message. For more information, see section 4.1.1 or <a href="#">RFC 3164</a> .		
<b>device.syslog.prependMac<sup>1</sup></b>	<b>0 or 1</b>	<b>Null</b>
If 1, the system's MAC address is pre-pended to the log message sent to the syslog server.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>device.syslog.renderLevel<sup>1</sup></b>	<b>0 to 6</b>	<b>Null</b>
Specify the logging level that will display 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 that will be logged. <b>0</b> or <b>1</b> : SeverityDebug(7). <b>2</b> or <b>3</b> : SeverityInformational(6). <b>4</b> : SeverityError(3). <b>5</b> : SeverityCritical(2). <b>6</b> : SeverityEmergency(0).		
<b>device.syslog.serverName</b>	<b>dotted-decimal IP address OR domain name string</b>	<b>Null</b>
The syslog server IP address or domain name string.		
<b>device.syslog.transport</b>	<b>None, UDP, TCP, TLS</b>	<b>Null</b>
The transport protocol that the system will use to write to the syslog server. If set to None, transmission is turned off but the server address is preserved.		

<sup>1</sup> Change causes system to restart or reboot.

## <diags/>

Use these parameters to enable and setup the remote packet capture.

### Remote Packet Capture Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>diags.pcap.enabled</b>	<b>0 or 1</b>	<b>0</b>
Enable or disable all on-board packet capture features.		
<b>diags.telnetd.enabled</b>	<b>0 or 1</b>	<b>0</b>
Enable or disable all on-board packet capture features using telnet.		

## <dialplan/>

The parameters listed in the following table enable you to create a specific routing path for outgoing SIP calls independent of other *default* configurations.

The dial plan (or digit map) is not applied against Placed Call List, Voicemail, last call return, remote control dialed numbers, or on-hook dialing.

### Dial Plan (Digit Map) Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>dialplan.applyToCallListDial<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the dial plan does not apply to numbers dialed from the Received Call List or Missed Call List. If 1, the dial plan is applied to numbers dialed from the received call and missed call lists, including sub-menus.		
<b>dialplan.applyToDirectoryDial<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the dial plan is not applied to numbers dialed from the directory or speed dial list. If 1, the dial plan is applied to numbers dialed from the directory or speed dial, including auto-call contact numbers.		
<b>dialplan.applyToForward<sup>1</sup></b>		
If 0, the dial plan does not apply to forwarded calls. If 1, the dial plan applies to forwarded calls.		
<b>dialplan.applyToTelUriDial<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the dial plan does not apply to URI dialing. If 1, the dial plan applies to URI dialing.		
<b>dialplan.applyToUserDial<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the dial plan does not apply to calls made when the user presses the <b>Dial</b> soft key to place a call. If 1, the dial plan applies to calls placed using the <b>Dial</b> soft key.		
<b>dialplan.applyToUserSend<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the dial plan does not apply to calls placed when the user presses the <b>Send</b> soft key to place a call. If 1, the dial plan applies to calls placed using the <b>Send</b> soft key.		
<b>dialplan.digitmap<sup>1</sup></b>	<b>string compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435</b>	<b>[2-9]11 0T  +011xxx.T  0[2-9]xxxxxxxx  +1[2-9]xxxxxxxx  [2-9]xxxxxxxx  [2-9]xxxT</b>
The digit map used for the dial plan. The string is limited to 2560 bytes and 100 segments of 64 bytes; a comma is also allowed; a comma will turn dial tone back on; '+' is allowed as a valid digit; extension letter 'R' is used as defined above. This parameter enables the system to automatically initiate calls to numbers that match a digit map pattern.		
<b>dialplan.digitmap.timeOut<sup>1</sup></b>	<b>string of positive integers separated by ' '</b>	<b>3   3   3   3   3   3</b>
Specify a timeout in seconds for each segment of digit map. After you press a key, the system will wait this many seconds before matching the digits to a dial plan and dialing the call. Note: If there are more digit maps than timeout values, the default value of 3 will be used. If there are more timeout values than digit maps, the extra timeout values are ignored.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>dialplan.filterNonDigitUriUsers<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, allow do not filter out (+) in the dial plan. If 1, filter out (+) from the dial plan (this is the previous behavior).		
<b>dialplan.impossibleMatchHandling<sup>1</sup></b>	<b>0, 1 or 2</b>	<b>0</b>
This parameter applies to digits you enter in dial mode, the dial mode when you tap the New Call softkey. The system is not in dial mode when you are hot dialing, contact dialing, or call list dialing. If set to 0, the digits entered up to and including the point an impossible match occurred are sent to the server immediately. If set to 1, give reorder tone. If set to 2, allow user to accumulate digits and dispatch call manually with the <b>Send</b> soft key. Note that if a call orbit number begins with '#' or '*', you need to set this parameter to 2 to retrieve the call using off-hook dialing.		
<b>dialplan.removeEndOfDial<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, strip trailing # digit from digits sent out.		
<b>dialplan.routing.emergency.outboundIdentity</b>	<b>10-25 digits, or a SIP, or TEL URI</b>	<b>Null</b>
The identity used to identify your system when you place an emergency call from your system. Format should be a 10-25 digit number or a valid SIP, or TEL URI. If using a URI, the full uri will be included verbatim in the P-A-I header.		
<b>dialplan.routing.emergency.x.description<sup>1FV</sup></b> <b>Emergency contact description</b>	<b>string</b>	<b>x=1:Emergency, Others: Null</b>
<b>dialplan.routing.emergency.x.server.y<sup>1</sup></b> <b>Emergency server</b>	<b>positive integer</b>	<b>x=1: 1, others: Null</b>
<b>dialplan.routing.emergency.x.value</b> <b>Emergency URL values</b>	<b>SIP URL (single entry)</b>	<b>x=1: 911, others: Null</b>
x is the index of the emergency entry description and y is the index of the server associated with emergency entry x. For each emergency entry (index x), one or more server entries (indexes (x,y)) can be configured. x and y must both use sequential numbering starting at 1. description: The label or description for the emergency address server.y: The index representing the server to use for emergency routing (dialplan.routing.server.x.address where x is the index). value: The URLs that should be watched for. When the user dials one of the URLs, the call will be directed to the emergency server defined by address. <b>Note:</b> Blind transfer for 911 (or other emergency calls) may not work if registration and emergency servers are different entities.		
<b>dialplan.routing.server.x.address<sup>1</sup></b>	<b>dotted-decimal IP address or hostname</b>	<b>Null</b>
The IP address or hostname of a SIP server that will be used for routing calls. Multiple servers can be listed starting with x=1 to 3 for fault tolerance. <b>Note:</b> Blind transfer for 911 (or other emergency calls) may not work if registration and emergency servers are different entities.		
<b>dialplan.routing.server.x.port<sup>1</sup></b>	<b>1 to 65535</b>	<b>5060</b>
The port of a SIP server that will be used for routing calls		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>dialplan.routing.server.x.transport<sup>1</sup></b>	<b>DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly</b>	<b>DNSnaptr</b>
<p>The dns lookup of the first server to be dialed will be used, if there is a conflict with the others.            For example, if <code>dialplan.routing.server.1.transport="UDPOnly"</code> and <code>dialplan.routing.server.2.transport = "TLS"</code>, then UDPOnly is used.</p>		
<b>dialplan.userDial.timeOut</b>	<b>0 – 99 seconds</b>	<b>Generic Profile=0</b>
<p>This parameter specifies the time in seconds that the system waits before dialing a number you enter while the system is on hook. You can apply <code>dialplan.userDial.timeOut</code> only when its value is lower than <code>up.IdleTimeOut</code>. Note that you need to restart or reboot to apply changes to this parameter.</p>		
<b>dialplan.x.conflictMatchHandling</b>	<b>0 or 1</b>	<b>Generic Profile=0</b>
<p>This is the per-registration parameter of <code>dialplan.conflictMatchHandling</code>. This parameter takes priority over the general parameter, <code>dialplan.conflictMatchHandling</code>.</p>		

<sup>1</sup> Change causes system to restart or reboot.

Per-registration dial plan configuration is also supported and parameters are listed in the table [Per Registration Dial Plan \(Digit Map\) Parameters](#). The descriptions for these per-registration parameters are provided in the table [Dial Plan \(Digit Map\) Parameters](#). Note that the per-registration parameters override the general parameters where x is the registration number (for example, `dialplan.x.applyToTelUriDial` overrides `dialplan.applyToTelUriDial` for registration x).

For the CX500 system, x=1-16.

#### Per-Registration Dial Plan (Digit Map) Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<code>dialplan.conflictMatchHandling</code>	<b>0 or 1</b>	<b>Generic Profile=0 Lync Profile=1</b>
<code>dialplan.x.applyToCallListDial<sup>1</sup></code>	<b>0 or 1</b>	<b>1</b>
<code>dialplan.x.applyToDirectoryDial<sup>1</sup></code>	<b>0 or 1</b>	<b>0</b>
<code>dialplan.x.applyToForward</code>	<b>0 or 1</b>	<b>0</b>
<code>dialplan.x.applyToTelUriDial<sup>1</sup></code>	<b>0 or 1</b>	<b>1</b>
<code>dialplan.x.applyToUserDial<sup>1</sup></code>	<b>0 or 1</b>	<b>1</b>
<code>dialplan.x.applyToUserSend<sup>1</sup></code>	<b>0 or 1</b>	<b>1</b>
<code>dialplan.x.digitmap<sup>1</sup></code>	<b>string - max number of characters 2560</b>	<b>Null</b>
<code>dialplan.x.digitmap.timeOut<sup>1</sup></code>	<b>string - max number of characters 100</b>	<b>Null</b>



<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
dialplan.x.e911dialmask	<b>string - max number of characters 256</b>	<b>Null</b>
dialplan.x.e911dialstring	<b>string - max number of characters 256</b>	<b>Null</b>
dialplan.x.applyToForward	<b>0 or 1</b>	<b>0</b>
dialplan.x.impossibleMatchHandling <sup>1</sup>	<b>0 to 2</b>	<b>0</b>
dialpan.x.lyncDigitmap.timeOut	<b>0-99 seconds</b>	<b>3 seconds</b>
dialplan.x.originaldigitmap	<b>string - max number of characters 2560</b>	<b>Null</b>
dialplan.x.removeEndOfDial <sup>1</sup>	<b>0 or 1</b>	<b>1</b>
dialplan.x.routing.emergency.y.value <sup>1</sup>	<b>string - max number of characters 64</b>	<b>Null</b>
dialplan.x.routing.emergency.y.server.z <sup>1</sup>	<b>0 to 3</b>	<b>0 For all x, y, and z = 1 to 3</b>
dialplan.x.routing.server.y.address <sup>1</sup>	<b>string - max number of characters 256</b>	<b>Null</b>
dialplan.x.routing.server.y.port <sup>1</sup>	<b>1 to 65535</b>	<b>5060</b>
dialplan.x.routing.server.y.transport <sup>1</sup>	<b>DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly</b>	<b>DNSnaptr</b>
dialplan.userDial.timeOut	<b>0 – 99 seconds</b>	<b>Generic Profile=0 Lync Profile=3</b>

<sup>1</sup> Change causes system to restart or reboot.

## <dir>

This parameter definition includes:

- **<broadsoft/>** Polycom BroadSoft UC-One directory definitions
- **<local/>** The local directory definition
- **<corp/>** The corporate directory definition

## <broadsoft/>

Use the parameters listed in the following table with the Polycom BroadSoft UC-One directory.

### Polycom BroadSoft UC-One Feature Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>dir.broadsoft.xsp.address</b>	<b>dotted-decimal IP address, hostname or FQDN</b>	<b>Null</b>
Set the IP address or hostname of the Broadsoft directory XSP home address. For example, <code>host.domain.com</code> or <a href="http://xxx.xxx.xxx.xxx">http://xxx.xxx.xxx.xxx</a> .		
<b>dir.broadsoft.xsp.username</b>	<b>UTF-8 encoding string</b>	<b>Null</b>
Set the username used to authenticate to the BroadSoft Directory XSP server.		
<b>dir.broadsoft.xsp.password</b>	<b>UTF-8 encoding string</b>	<b>Null</b>
Set the password used to authenticate to the BroadSoft Directory XSP server.		

## <local/>

The following table lists parameters you can configure for your local contact directory. The local directory is stored in either device settings or RAM on the system. The local directory size is limited based on the amount of flash memory in the system. (Different system models have variable flash memory.)

When the volatile storage option is enabled, ensure that a properly configured provisioning server that allows uploads is available to store a back-up copy of the directory or its contents will be lost when the system reboots or loses power.

### Local Contact Directory Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>dir.local.contacts.maxNum<sup>1</sup></b>	<b>1 to 9999</b>	<b>99 9999</b>
Maximum number of contacts allowed in the local contact directory.		
<b>dir.local.readonly<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the local contact directory can be edited. If 1, the local contact directory is read-only.		
<b>dir.search.field</b>	<b>0 or 1</b>	<b>0</b>
If 0, contact directory searches are sorted by contact's last name. If 1, contact directory searches are sorted by first name.		

<sup>1</sup> Change causes system to restart or reboot.

**<corp/>**

Use the parameters in the following table to configure a corporate directory. A portion of the corporate directory is stored in flash memory on the system. The size is based on the amount of flash memory in the system. Different system models have variable flash memory.

**Corporate Directory Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>dir.corp.address<sup>1</sup></b>	<b>dotted-decimal IP address or hostname or FQDN</b>	<b>Null</b>
The IP address or hostname of the LDAP server interface to the corporate directory. For example, host.domain.com.		
<b>dir.corp.attribute.x.filter<sup>1</sup></b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The filter string for this parameter, which is edited when searching.		
<b>dir.corp.attribute.x.label<sup>1</sup></b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The label when data is displayed.		
<b>dir.corp.attribute.x.name<sup>1</sup></b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The name of the parameter to match on the server. Each name must be unique; however, an LDAP entry can have multiple parameters with the same name. Up to eight parameters can be configured (x = 1 to 8).		
<b>dir.corp.attribute.x.searchable<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, quick search on parameter x (if x is 2 or more) is disabled. If 1, quick search on x (if x is 2 or more) is enabled.		
<b>dir.corp.attribute.x.sticky<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the filter criteria for attribute x is reset after a reboot. If 1, the filter criteria are retained through a reboot. If you set an attribute to be sticky (set this parameter to 1), a '*' will display before the label of the attribute on the system.		
<b>dir.corp.attribute.x.type<sup>1</sup></b>	<b>first_name, last_name, system_number SIP_address, other</b>	<b>last_name</b>
Defines how parameter x is interpreted by the system. Entries can have multiple parameters of the same type. The value other is used for display purposes only. If the user saves the entry to the local contact directory on the system, <code>first_name</code> , <code>last_name</code> , and <code>system_number</code> are copied. The user can place a call to the <code>system_number</code> and <code>SIP_address</code> from the corporate directory.		
<b>dir.corp.autoQuerySubmitTimeout<sup>1</sup></b>	<b>0 to 60 seconds</b>	<b>0</b>
The timeout (in seconds) between when the user stops entering characters in the quick search and when the search query is automatically submitted. If 0, there is no timeout (automatic submit is disabled).		
<b>dir.corp.backGroundSync<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, background downloading from the LDAP server is disabled. If 1, background downloading is enabled.		
<b>dir.corp.backGroundSync.period<sup>1</sup></b>	<b>3600 to 604800</b>	<b>86400</b>
The corporate directory cache is refreshed after the corporate directory feature has not been used for this period of time seconds. The default period is 24 hours (86400 seconds). The minimum is 1 hour and the maximum is 7 days.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>dir.corp.baseDN<sup>1</sup></b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The base domain name. This is the starting point for making queries on the LDAP server.		
<b>dir.corp.bindOnInit<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, do not use bind authentication on initialization. If 1, use bind authentication on initialization.		
<b>dir.corp.cacheSize<sup>1</sup></b>	<b>8 to 256</b>	<b>128</b>
The maximum number of entries that can be cached locally on the system.		
<b>dir.corp.filterPrefix<sup>1</sup></b>	<b>UTF-8 encoded string</b>	<b>(objectclass=person)</b>
Predefined filter string for search queries.		
<b>dir.corp.pageSize<sup>1</sup></b>	<b>8 to 64</b>	<b>32</b>
The maximum number of entries requested from the corporate directory server with each query.		
<b>dir.corp.password<sup>1</sup></b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The password used to authenticate to the LDAP server.		
<b>dir.corp.port<sup>1</sup></b>	<b>0, Null, 1 to 65535</b>	<b>389 (TCP) 636 (TLS)</b>
The port that connects to the server if a full URL is not provided.		
<b>dir.corp.scope<sup>1</sup></b>	<b>one, sub, base</b>	<b>sub</b>
The type of search that is performed. If <b>one</b> , a search of one level below the base domain name (DN). If <b>sub</b> , a recursive search of all levels below the base DN. If <b>base</b> , a search at the base DN level.		
<b>dir.corp.sortControl<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
Control how a client can make queries and sorts entries locally. If 0, leave sorting as negotiated between the client and server. If 1, force sorting of queries (this causes excessive LDAP queries and should only be used to diagnose LDAP servers with sorting problems).		
<b>dir.corp.transport<sup>1</sup></b>	<b>TCP, TLS, Null</b>	<b>TCP</b>
Specify whether a TCP or TLS connection is made with the server, if a full URL is not provided.		
<b>dir.corp.user<sup>1</sup></b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The user name used to authenticate to the LDAP server.		
<b>dir.corp.viewPersistence<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the corporate directory search filters and browsing position are reset each time the user accesses the corporate directory. If 1, the search filters and browsing position from the previous session are displayed each time the user accesses the corporate directory.		
<b>dir.corp.vlv.allow<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, virtual view list (VLV) queries are disabled. If 1, VLV queries are enabled and can be made if the LDAP server supports VLV.		
<b>dir.corp.vlv.sortOrder<sup>1</sup></b>	<b>list of parameters</b>	<b>Null</b>
The list of parameters—in exact order—for the LDAP server to use when indexing. For example: <code>sn, givenName, telephoneNumber</code> .		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
------------------	-------------------------	----------------

<sup>1</sup> Change causes system to restart or reboot.

## <divert/>

The system has a flexible call forward/diversion feature for each registration. In all cases, a call will only be diverted if a non-Null contact has been configured.

In the following table, x is the registration number. For CX5500, x=1-16.

### Call Diversion (Call Forwarding) Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>divert.x.contact<sup>1</sup></b>	<b>contact address: ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)</b>	<b>Null</b>
The forward-to contact used for all automatic call diversion features. All automatically forwarded calls will be directed to this contact. The contact can be overridden by a busy contact, DND contact, or no-answer contact as specified by the <code>busy</code> , <code>dnd</code> , and <code>noAnswer</code> parameters that follow.		
<b>divert.x.sharedDisabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, call diversion features can be used on shared lines. If 1, call diversion features are disabled on shared lines.		
<b>divert.x.autoOnSpecificCaller<sup>2</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the Auto Divert feature of the contact directory is disabled for registration x. If 1, calls on registration x may be diverted using Auto Divert, you may specify to divert individual calls or divert all calls.		
<b>divert.busy.x.enabled<sup>2</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>divert.busy.x.contact<sup>1</sup></b>	<b>contact address</b>	<b>Null</b>
Divert incoming calls that reach a busy signal. If <code>enabled</code> is set to 1, calls will be diverted when registration x is busy. Calls will be sent to the busy contact's address if it is specified; otherwise calls will be sent to the default contact specified by <code>divert.x.contact</code> . If <code>enabled</code> is set to 0, calls will not be diverted if the line is busy.		
<b>divert.dnd.x.enabled<sup>2</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>divert.dnd.x.contact<sup>1</sup></b>	<b>contact address</b>	<b>Null</b>
Divert calls when Do Not Disturb is enabled. If <code>enabled</code> is set to 1, calls will be diverted when DND is enabled on registration x. Calls will be sent to the DND contact's address if it is specified; otherwise calls will be sent to the default contact specified by <code>divert.x.contact</code> .		
<b>divert.fwd.x.enabled<sup>2</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the user cannot enable universal call forwarding (automatic forwarding for all calls on registration x). If 1, a Forward soft key displays on the system's Home screen that you can use to enable universal call forwarding.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>divert.noanswer.x.enabled<sup>2</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>divert.noanswer.x.contact<sup>1</sup></b>	<b>contact address</b>	<b>Null</b>
<b>divert.noanswer.x.timeout<sup>1</sup></b>	<b>positive integer</b>	<b>55</b>

If no-answer call diversion is *enabled*, calls that are not answered after the number of seconds specified by *timeout* will be sent to the *no-answer contact*. If the *no-answer contact* is set to *Null*, the call will be sent to the default contact specified by *divert.x.contact*. If *enabled* is set to 0, calls will not be diverted if they are not answered.

<sup>1</sup> Change causes system to restart or reboot.

<sup>2</sup> Change causes system to restart or reboot. If server-based call forwarding is enabled, this parameter is disabled.

## <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

<i>Parameter</i>	<i>Permitted values</i>	<i>Default</i>
<b>dns.cache.A.x.address</b>	<b>dotted-decimal IP version 4 address</b>	<b>Null</b>
IP address.		
<b>dns.cache.A.x.name</b>	<b>valid hostname</b>	<b>Null</b>
Hostname		
<b>dns.cache.A.x.ttl</b>	<b>300 to 536870912 (2<sup>29</sup>), seconds</b>	<b>300</b>

The TTL describes the time period the system will use 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 will retry 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

<i>Parameter</i>	<i>Permitted values</i>	<i>Default</i>
<b>dns.cache.NAPTR.x.flags</b>	<b>A single character from [A-Z, 0-9]</b>	<b>Null</b>
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 <a href="#">RFC 2915</a> for details of the permitted flags.		
<b>dns.cache.NAPTR.x.name</b>	<b>domain name string</b>	<b>Null</b>
The domain name to which this resource record refers.		
<b>dns.cache.NAPTR.x.order</b>	<b>0 to 65535</b>	<b>0</b>
An integer specifying the order in which the NAPTR records must be processed to ensure the correct ordering of rules.		
<b>dns.cache.NAPTR.x.preference</b>	<b>0 to 65535</b>	<b>0</b>
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.		
<b>dns.cache.NAPTR.x.regexp</b>	<b>string containing a substitution expression</b>	<b>Null</b>
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 that will be looked up. The grammar of the substitution expression is given in <a href="#">RFC 2915</a> .		
<b>dns.cache.NAPTR.x.replacement</b>	<b>domain name string with SRV prefix</b>	<b>Null</b>
The next name to query for NAPTR records depending on the value of the flags field. It must be a fully qualified domain-name.		
<b>dns.cache.NAPTR.x.service</b>	<b>string</b>	<b>Null</b>
Specifies the service(s) available down this rewrite path. For more information, see <a href="#">RFC 2915</a> .		
<b>dns.cache.NAPTR.x.ttl</b>	<b>300 to 536870912 (2^29), seconds</b>	<b>300</b>
The TTL describes the time period the system will use 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 will retry 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

<i>Parameter</i>	<i>Permitted values</i>	<i>Default</i>
<b>dns.cache.SRV.x.name</b>	<b>domain name string with SRV prefix</b>	<b>Null</b>
The domain name string with SRV prefix.		
<b>dns.cache.SRV.x.port</b>	<b>0 to 65535</b>	<b>0</b>
The port on this target host of this service. For more information, see <a href="#">RFC 2782</a> .		
<b>dns.cache.SRV.x.priority</b>	<b>0 to 65535</b>	<b>0</b>
The priority of this target host. For more information, see <a href="#">RFC 2782</a> .		
<b>dns.cache.SRV.x.target</b>	<b>domain name string</b>	<b>Null</b>
The domain name of the target host. For more information, see <a href="#">RFC 2782</a> .		
<b>dns.cache.SRV.x.ttl</b>	<b>300 to 536870912 (2<sup>29</sup>), seconds</b>	<b>300</b>
The TTL describes the time period the system will use 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 will retry a dynamic network request before falling back on the static entry and its reset TTL timer again.		
<b>dns.cache.SRV.x.weight</b>	<b>0 to 65535</b>	<b>0</b>
A server selection mechanism. For more information, see <a href="#">RFC 2782</a> .		

## <efk/>

Use the three tables to configure the Enhanced Feature Key (EFK) feature on your system:

- [Enhanced Feature Key Version Parameters](#)
- [Enhanced Feature Key List Parameters](#)
- [Enhanced Feature Key Prompt Parameters](#)

### Enhanced Feature Key (EFK) Version Parameters

<i>Parameter Name</i>	<i>Permitted Values</i>	<i>Default</i>
<b>efk.version</b>	<b>2 (1 for SIP 3.0 and earlier)</b>	<b>2</b>
The version of the EFK elements. For SIP 3.0.x or earlier, 1 is the only supported version. For SIP 3.1 and later, 2 is the only supported version. If this parameter is Null, the EFK feature is disabled. This parameter is not required if there are no <code>efk.efklist</code> entries.		



**Enhanced Feature Key (EFK) List Parameters**

<i>Parameter Name</i>	<i>Permitted Values</i>	<i>Default</i>
<b>efk.efklist.x.action.string</b>		
<p>The action string contains a macro definition of the action that the feature key will perform. If EFK is enabled, this parameter must have a value (it cannot be Null). For a list of macro definitions and example macro strings, see <a href="#">Understanding Macro Definitions</a>.</p>		
<b>efk.efklist.x.label</b>	<b>string</b>	<b>Null</b>
<p>The text string that will be used as a label on any user text entry screens during EFK operation. If Null, the Null string is used. Note: If the label does not fit on the screen, the text will be shortened and '...' will be appended.</p>		
<b>efk.efklist.x.mname</b>		<b>expanded_macro</b>
<p>The unique identifier used by the speed dial configuration to reference the enhanced feature key entry. Cannot start with a digit. Note that this parameter must have a value, it cannot be Null.</p>		
<b>efk.efklist.x.status</b>	<b>0 or 1</b>	<b>0</b>
<p>If 0 or Null, key x is disabled. If 1, the key is enabled.</p>		
<b>efk.efklist.x.type</b>		<b>invite</b>
<p>The SIP method to be performed. If set to <code>invite</code>, the action required is performed using the SIP INVITE method. Note: This parameter is included for backwards compatibility. Do not use if possible. If <code>efk.x.action.string</code> contains types, this parameter is ignored. If Null, the default of INVITE is used.</p>		

**Enhanced Feature Key (EFK) Prompt Parameters**

<i>Parameter Name</i>	<i>Permitted Values</i>	<i>Default</i>
<b>efk.efkprompt.x.label<sup>1</sup></b>	<b>string</b>	<b>Null</b>
The prompt text that is presented to the user on the user prompt screen. If Null, no prompt displays. Note: If the label does not fit on the screen, the label will be shortened and '...' will be appended.		
<b>efk.efkprompt.x.status<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, key x is disabled. If 1, the key is enabled. This parameter must have a value, it cannot be Null. Note: If a macro attempts to use a prompt that is disabled or invalid, the macro execution will fail.		
<b>efk.efkprompt.x.type<sup>1</sup></b>	<b>numeric or text</b>	<b>text</b>
The type of characters entered by the user. If set to <code>numeric</code> , the characters are interpreted as numbers. If set to <code>text</code> , the characters are interpreted as letters. If Null, <code>numeric</code> is used. If this parameter has an invalid value, this prompt, and all parameters depending on this prompt, are invalid. Note: A mix of <code>numeric</code> and <code>text</code> is not supported.		
<b>efk.efkprompt.x.userfeedback<sup>1</sup></b>	<b>visible or masked</b>	<b>visible</b>
The user input feedback method. If set to <code>visible</code> , the text is visible. If set to <code>masked</code> , the text displays as asterisk characters (*), this can be used to mask password fields. If Null, <code>visible</code> is used. If this parameter has an invalid value, this prompt, and all parameters depending on this prompt, are invalid.		

<sup>1</sup> Change causes system to restart or reboot.

**<exchange/>**

Set the connection parameters for the Microsoft Exchange application to configure the Calendaring feature. Use the following table which lists available parameters.

**Microsoft Exchange Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>exchange.meeting.systemPattern</b>	<b>String</b>	<b>Null</b>
The pattern used to identify system numbers in meeting descriptions, where "x" denotes any digit and " " separates alternative patterns (for example, xxx-xxx-xxxx 604.xxx.xxxx).		
<b>exchange.meeting.reminderEnabled</b>	<b>0 or 1</b>	<b>1</b>
If 0, meeting reminders are disabled. If 1, they are enabled.		
<b>exchange.server.url<sup>1</sup></b>	<b>String</b>	<b>Null</b>
The Microsoft Exchange server address.		

<sup>1</sup> Change causes system to restart or reboot.

## <feature/>

The feature parameters listed in the following table control the activation or deactivation of a feature at run time.

### Feature Activation/Deactivation Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>feature.acdAgentAvailable.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the ACD agent available/unavailable feature is disabled. If 1, the feature is enabled.		
<b>feature.acdLoginLogout.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the ACD login/logout feature is disabled. If 1, the feature is enabled.		
<b>feature.acdPremiumUnavailability.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the premium ACD unavailability feature is disabled. If 1, premium ACD unavailability feature is enabled, and unavailability reason codes can be used (if the other ACD feature parameters are also be enabled).		
<b>feature.acdServiceControlUri.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the ACD service control URI feature is disabled. If 1, the feature is enabled.		
<b>feature.broadsoftdir.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 1, the BroadSoft Enterprise directory is enabled. If 0, the directory is disabled		
<b>feature.broadsoftUcOne.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 1, the BroadSoft UC-One feature is enabled. If 0, the feature is disabled.		
<b>Feature.btoe.enabled</b>		
If 0, the Better Together over Ethernet feature is disabled. If 1, the feature is enabled.		
<b>feature.callCenterStatus.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the Status Event Threshold capability is disabled. If 1, the Status Event Threshold capability is enabled.		
<b>feature.callList.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>All locally controlled call lists.</b>		
<b>feature.callListMissed.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>The missed calls list.</b>		
<b>feature.callListPlaced.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>The placed calls list.</b>		
<b>feature.callListReceived.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>The received calls list.</b>		
If 0, the call list is disabled. If 1, the call list is enabled. To enable the Missed, Placed, or Received call lists, <code>feature.callList.enabled</code> must be enabled.		
<b>feature.callPark.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the call park and call retrieve features are disabled. If 1, the features are enabled.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>feature.corporateDirectory.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the corporate directory feature is disabled. If 1, the feature is enabled.		
<b>feature.directedCallPickup.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the directed call pickup feature is disabled. If 1, the feature is enabled.		
<b>feature.directory.enabled</b>	<b>0 or 1</b>	<b>1</b>
If 0, the local contact directory is disabled. If 1, the directory is enabled.		
<b>feature.enhancedCallDisplay.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the system may display the protocol at the end of the called party identification (for example, 1234567 [SIP]). If 1, the system will display the number only (for example, 1234567).		
<b>feature.enhancedFeatureKeys.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the enhanced feature keys feature is disabled. If 1, the feature is enabled.		
<b>feature.exchangeCalendar.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the calendaring feature is disabled. If 1, the feature is enabled.		
<b>feature.groupCallPickup.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the group call pickup feature is disabled.		
<b>feature.lastCallReturn.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the last call return feature is disabled. If 1, the feature is enabled.		
<b>feature.lync.abs.enabled</b>	<b>0 or 1</b>	<b>1</b>
Set to 1 to enable comprehensive contact search in the Lync Server address book service. Set to 0 to disable comprehensive contact search in the Lync Server address book service.		
<b>feature.lync.abs.maxResult</b>	<b>5 to 50</b>	<b>20</b>
The value for this parameter defines the maximum number of contacts to display in a Lync Server address book service contact search.		
<b>Feature.lyncbtoe.auto.signin.signoff.enabled</b>		
Enables or disables the system to signout of Lync automatically when BToE enabled. If 1, the system signs out of Lync automatically when BTOE is disabled or the system is unpaired with the computer. If 0, the system does not signout of Lync when BToE is disabled or the system is unpaired with the computer.		
<b>feature.messaging.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the instant messaging feature is disabled. If 1, the feature is enabled.		
<b>feature.nonVolatileRingerVolume.enabled</b>	<b>0 or 1</b>	<b>1</b>
If 0, user changes to the ringer volume are reset to default when the system reboots. If 1, user changes to the ringer volume are saved and maintained when the system reboots.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>feature.nWayConference.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the n-way conferencing managing feature is disabled and while three-way conferencing can exist, there is no manage conference page. If 1, n-way conferencing is enabled, conferences with the maximum number of parties are allowed, and the manage conference page is shown.		
<b>feature.presence.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the presence feature—including buddy managements and user status—is disabled. If 1, the presence feature is enabled with the buddy and status options.		
<b>feature.qml.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 1, the QML viewer is enabled on system. If 0, the viewer is disabled. The viewer is used to load the QML applications.		
<b>feature.ringDownload.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the system will not download ringtones when it starts up. If 1, the system will download ringtones when it starts up.		
<b>feature.urlDialing.enabled</b>	<b>0 or 1</b>	<b>1</b>
If 0, URL/name dialing is not available. If 1, URL/name dialing is available from private lines. Note: If enabled, unknown callers will be identified on the display by their system's IP address.		

<sup>1</sup> Change causes system to restart or reboot.

## <httpd/>

The system contains a local Web Configuration Utility server for user and administrator features. You can disable it for applications when it is not needed or where it poses a security threat. The Web server supports both basic and digest authentication. The authentication user name and password are not configurable for this release. You can configure the parameters listed in the following table.

### HTTPD (Web Server) Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>httpd.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the HTTP server is disabled (the Web Configuration Utility will also be disabled). If 1, the server will be enabled. Note: This parameter must be enabled to take screen captures of the system's screen.		
<b>httpd.cfg.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the Web Configuration Utility is disabled. If 1, the Web Configuration Utility is enabled.		
<b>httpd.cfg.port<sup>1</sup></b>	<b>1 to 65535</b>	<b>80</b>
Port is 80 for HTTP servers. Care should be taken when choosing an alternate port.		
<b>httpd.cfg.secureTunnelEnabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the Web does not use a secure tunnel. If 1, the server connects through a secure tunnel.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>httpd.cfg.secureTunnelPort<sup>1</sup></b>	<b>1 to 65535</b>	<b>443</b>
The port to use for communications when the secure tunnel is used.		
<b>httpd.cfg.secureTunnelRequired<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, communications to the Web server do not require a secure tunnel. If 1, communications do require a secure tunnel.		

<sup>1</sup> Change causes system to restart or reboot.

## <keyboard/>

The parameters listed in the following table are for use with Lync Server. Use these parameters to set options for the system screen virtual keyboard layout and encoding options.

### Keyboard for Lync Server

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>keyboard.layout.type</b>	<b>0 or 1</b>	<b>0</b>
Use this parameter to change the system's virtual keyboard for character and numeric input from the English language QWERTY layout to French language AZERTY layout. The default value 0 sets the virtual keyboard to QWERTY. Set to 1 to use the French-language AZERTY layout.		
<b>keyboard.encoding.all</b>	<b>0 or 1</b>	<b>1</b>
When set to 1, the default, the system display default character encoding options for the system menus. Set to 0 to display only ASCII and Latin encoding options for the system menus.		

## <lcl/>

You can configure the language you want the Polycom system user interface to operate and display in. The systems support both North American and international time and date formats.



### Caution: Use a Multilingual XML Editor

Edit the language parameters using a multilingual XML editor. If you do not use an XML editor, some of the language labels in the configuration file, and in the language menu on the system, will display incorrectly. To confirm whether your editor properly supports these characters, view the language parameter for languages such as Chinese, Japanese, Korean, Russian— for example `lcl.ml.lang.menu.1.label`.

This parameter definition includes:

- `<ml/>` The multilingual definitions
- `<datetime/>` The date and time definitions

## `<ml/>`

The multilingual parameters listed in the following table is based on string dictionary files downloaded from the provisioning server. These files are encoded in standalone XML format and include several eastern European and Asian languages. The files include space for user-defined languages.

### Multilingual Parameters

<i>Parameter</i>	<i>Permitted Values</i>
<b>lcl.ml.lang</b>	<b>Null or an exact match for one of the label names stored in lcl.ml.lang.menu.x.label</b>
If Null, the default internal language (US English) will be used, otherwise, the language to be used may be specified in the format of <code>lcl.ml.lang.menu.x.label</code> . For example, to get the system to boot up in German, set this parameter to <code>Deutsch (de-de)</code> .	
<b>lcl.ml.lang.charset<sup>1</sup></b>	<b>string</b>
The language character set.	
<b>lcl.ml.lang.clock.x.24HourClock</b>	<b>0 or 1</b>
If parameter present, overrides <code>lcl.datetime.time.24HourClock</code> If 1, display time in 24-hour clock mode rather than am/pm.	
<b>lcl.ml.lang.clock.x.dateTop</b>	<b>0 or 1</b>
If parameter present, overrides <code>lcl.datetime.date.dateTop</code> . If 1, display date above time, otherwise display time above date.	
<b>lcl.ml.lang.clock.x.format</b>	<b>string which includes 'D', 'd' and 'M' and two optional commas</b>
If parameter present, overrides <code>lcl.datetime.date.format</code> ; D = day of week d = day M = month. Up to two commas may be included. For example: D,dM = Thursday, 3 July or Md,D = July 3, Thursday The field may contain 0, 1 or 2 commas which can occur only between characters and only one at a time. For example: "D,,dM" is illegal.	
<b>lcl.ml.lang.clock.x.longFormat</b>	<b>0 or 1</b>
If parameter present, overrides <code>lcl.datetime.date.longFormat</code> . If 1, display the day and month in long format (Friday/November), otherwise use abbreviations (Fri/Nov).	
<b>lcl.ml.lang.font.x<sup>1</sup></b>	<b>string</b>
The language font.	
<b>lcl.ml.lang.list<sup>1</sup></b>	<b>a comma-separated list</b>
A list of the languages supported on the systems.	

<i>Parameter</i>	<i>Permitted Values</i>
<b>lcl.ml.lang.menu.x</b> <b>Dictionary file</b>	<b>String in the format language_region</b>
<b>lcl.ml.lang.menu.x.label<sup>1</sup></b> <b>System language menu label</b>	<b>String in the format nativeLanguageName (abbreviation)</b>

The system supports multiple languages. Dictionary files and labels must be sequential (for example, lcl.ml.lang.menu.1, lcl.ml.lang.menu.2, lcl.ml.lang.menu.3... lcl.ml.lang.menu.N) The dictionary file cannot have caps, and the strings must exactly match a folder name of a dictionary file (you can find the names in the **SoundPointIPLocalization** folder of your software distribution). If you edit these parameters, you need to use a multilingual XML editor that supports Unicode, such as XML Notepad 2007.

For example, a dictionary file and label for German would be: lcl.ml.lang.menu.8="German\_Germany"  
lcl.ml.lang.menu.8.label="Deutsch (de-de)"

<sup>1</sup> Change causes system to restart or reboot.

### To add a new language:

- 1 Create a new dictionary file based on an existing one.
- 2 Change the strings making sure to encode the XML file in UTF-8 but also ensuring the UTF-8 characters chosen are within the Unicode character ranges indicated in the tables below.
- 3 Place the file in an appropriately named folder according to the format `language_region` parallel to the other dictionary files under the `SoundPointIPLocalization` folder on the provisioning server.
- 4 Add an `lcl.ml.lang.clock.menu.x` parameter to the configuration file.
- 5 Add `lcl.ml.lang.clock.x.24HourClock`, `lcl.ml.lang.clock.x.format`, `lcl.ml.lang.clock.x.longFormat`, and `lcl.ml.lang.clock.x.dateTop` parameters and set them according to the regional preferences.
- 6 (Optional) Set `lcl.ml.lang` to be the new `language_region` string.

The basic character support includes the Unicode character ranges listed in the table [Unicode Ranges for Basic Character Support](#).

#### Unicode Ranges for Basic Character Support

<i>Name</i>	<i>Range</i>
C0 Controls and Basic Latin	U+0000 - U+007F
C1 Controls and Latin-1 Supplement	U+0080 - U+00FF
Cyrillic (partial)	U+0400 - U+045F

## <datetime/>

The parameters listed in the following table configure the date and time display on the system.



## Date and Time Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>lcl.datetime.date.dateTop</b>	<b>0 or 1</b>	
If set to 1, display date above time else display time above date.		
<b>lcl.datetime.date.format</b>	<b>string which includes 'D', 'd' and 'M' and two optional commas</b>	
Controls format of date string. D = day of week, d = day, M = month. Up to two commas may be included. For example: D, dM = Thursday, 3 July or Md, D = July 3, Thursday The field may contain 0, 1 or 2 commas which can occur only between characters and only one at a time. For example: "D,,dM" is illegal.		
<b>lcl.datetime.date.longFormat</b>	<b>0 or 1</b>	
If set to 1, display the day and month in long format (Friday/November), otherwise, use abbreviations (Fri/Nov).		
<b>lcl.datetime.time.24HourClock</b>	<b>0 or 1</b>	
If set to 1, display time in 24-hour clock mode rather than a.m./p.m.		

## <loc/>

The values you enter for the Lync Server-only parameters listed in the following table are used by E.911 services.

### E.911 Services Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>locInfo.source</b>	<b>LLDP=1</b> <b>MS_E911_LIS=2</b> <b>CONFIG=3</b>	<b>Generic Profile=1</b> <b>Lync Profile=2</b>
This parameter specifies the source of location information for the system and is useful for locating a system in environments that have multiple sources of location information. When set to LLDP, location information sent from the network switch is used as the current location. When set to MS_E911_LIS, location information sent from Lync Server is used as current location. When set to CONFIG, you can manually configure location information as current location. If location information is not available from a specified default or configured source, the fall back priority is as follows: Generic profile: LLDP > CONFIG > MS_E911_LIS Lync profile : MS_E911_LIS > CONFIG > LLDP		
<b>locInfo.x.label</b>	<b>String</b>	<b>Null</b>
Enter a label for your location.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>locInfo.x.country</b> Enter the country the system is located in.	<b>String</b>	<b>Null</b>
<b>locInfo.x.A1</b> Enter the national subdivision the system is located in, for example, a state or province.	<b>String</b>	<b>Null</b>
<b>locInfo.x.A3</b> Enter the city the system is located in.	<b>String</b>	<b>Null</b>
<b>locInfo.x.PRD</b> Enter the leading direction of the street location.	<b>String</b>	<b>Null</b>
<b>locInfo.x.RD</b> The name of the road or street the system is located on.	<b>String</b>	<b>Null</b>
<b>locInfo.x.STS</b> Enter the suffix of the name used in locInfo.x.RD, for example, Street, Avenue.	<b>String</b>	<b>Null</b>
<b>locInfo.x.POD</b> Enter the trailing street direction, for example SW.	<b>String</b>	<b>Null</b>
<b>locInfo.x.HNO</b> Enter the street address number of the system's location.	<b>String</b>	<b>Null</b>
<b>locInfo.x.HNS</b> Enter a suffix for the street address used in locInfo.x.HNS, for example, <sup>A</sup> or ½.	<b>String</b>	<b>Null</b>
<b>locInfo.x.LOC</b> Enter any additional information that identifies the location.	<b>String</b>	<b>Null</b>
<b>locInfo.x.NAM</b> Enter a name for the location, for example, a business name, an occupant, a resident.	<b>String</b>	<b>Null</b>
<b>locInfo.x.PC</b> Enter the postal code of the location.	<b>String</b>	<b>Null</b>

## <lldp/>

The parameters listed in the following table enable you to configure settings for LLDP discovery.

**LLDP Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>lldpFastStartCount</b>	<b>3 to 10</b>	<b>5</b>

Specifies the number of consecutive LLDP packets the system sends at the time of LLDP discovery. Note that LLDP packets are sent every one second.

**<license/>**

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

**Feature License Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>license.polling.time<sup>1</sup></b>	<b>00:00 – 23:59</b>	<b>02:00</b>

The time (using the 24-hour clock) to check if the license has expired.

<sup>1</sup> 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**

<i>Logging Level</i>	<i>Interpretation</i>
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 following table.

**Event Timestamp Formats**

<i>Type</i>	<i>Example</i>
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

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>log.level.change.xxx</b>	<b>0 to 6</b>	<b>4</b>
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, cap, cdp, cert, cfg, cipher, clink, clist, cmp, cmr, copy, curl, daa, dbs, dbuf, dhcpc, dis, dock, dot1x, dns, drvtbt, ec, efk, ethf, hset, httpa, httpd, hw, ht, ib, ldap, lic, lldp, loc, log, mb, mobil, net, niche, oaip, oosp, osd, pcd, pdc, peer, pgui, pmt, pnetm, poll, pps, pres, pstn, push, pwrsv, rdisk, res, rtos, rtls, sec, sig, sip, slog, so, soem, srtp, sshc, ssps, style, sync, sys, ta, task, tls, trace, trs, usb, usbio, util, utilm, wdog, wlan, wmgr, and xmpp.		
<b>log.render.file</b>	<b>0 or 1</b>	<b>1</b>
Set to 1. Polycom recommends that you do not change this value.		
<b>log.render.file.size</b>	<b>positive integer, 1 to 180</b>	<b>32</b>
Maximum size of flash memory for logs in Kbytes. When this size is about to be exceeded, the system will upload 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.		
<b>log.render.file.upload.append</b>	<b>0 or 1</b>	<b>1</b>
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.		
<b>log.render.file.upload.append.limitMode</b>	<b>delete, stop</b>	<b>delete</b>
Behavior when server log file has reached its limit. delete=delete file and start over stop=stop appending to file		
<b>log.render.file.upload.append.sizeLimit</b>	<b>positive integer</b>	<b>512</b>
Maximum log file size that can be stored on provisioning server in Kbytes.		
<b>log.render.file.upload.period</b>	<b>positive integer</b>	<b>172800</b>
Time in seconds between log file uploads to the provisioning server. Note: The log file will not be uploaded if no new events have been logged since the last upload.		
<b>log.render.level</b>	<b>0 to 6</b>	<b>1</b>
Specifies the lowest class of event that will be 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) For more information, refer to <a href="#">Syslog Menu</a> .		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>log.render.realtime</b>	<b>0 or 1</b>	<b>1</b>
Set to 1. Polycom recommends that you do not change this value.		
<b>log.render.stdout</b>	<b>0 or 1</b>	<b>1</b>
Set to 1. Polycom recommends that you do not change this value.		
<b>log.render.type</b>	<b>0 to 2</b>	<b>2</b>
Refer to 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 following 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

<i>Parameter</i>	<i>Permitted Values</i>
<b>log.sched.x.level</b>	<b>0 to 5, default 3</b>
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.	
<b>log.sched.x.name</b>	<b>alphanumeric string</b>
Name of an internal system command to be periodically executed. To be supplied by Polycom.	
<b>log.sched.x.period</b>	<b>positive integer, default 15</b>
Seconds between each command execution. 0=run once	
<b>log.sched.x.startDay</b>	<b>0 to 7</b>
When startMode is abs, specifies the day of the week to start command execution. 1=Sun, 2=Mon, ..., 7=Sat	
<b>log.sched.x.startMode</b>	<b>abs, rel</b>
Start at an absolute time or relative to boot.	
<b>log.sched.x.startTime</b>	<b>positive integer OR hh:mm</b>
Seconds since boot when startMode is rel or the start time in 24-hour clock format when startMode is abs.	

## <msg/>

The following table lists parameters you can use to configure message-waiting which is supported on a per-registration basis.

In the following table, x is the registration number. For the CX5500, x=1-16.

### Message Waiting Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>msg.bypassInstantMessage<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
This parameter determines what is shown on the system menu when you press the <b>Messages</b> key. If 0, the system shows Message Center and Instant Messages. If 1, the system bypasses these menus and goes directly to voicemail.		
<b>msg.mwi.x.subscribe</b>	<b>ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)</b>	<b>Null</b>
If non-Null, the system will send a SUBSCRIBE request to this contact after boot-up.		
<b>msg.mwi.x.callBackMode</b>	<b>contact, registration, disabled</b>	<b>registration</b>
The message retrieval mode and notification for registration x. <i>contact</i> : a call is placed to the contact specified by <i>msg.mwi.x.callback</i> . <i>registration</i> : the registration places a call to itself (the system calls itself). <i>disabled</i> : message retrieval and message notification are disabled.		
<b>msg.mwi.x.callBack</b>	<b>ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)</b>	<b>Null</b>
The contact to call when retrieving messages for this registration if <i>msg.mwi.x.callBackMode</i> is set to <i>contact</i> .		
<b>msg.mwi.x.led</b>	<b>0, 1</b>	<b>1</b>
Where x is an integer referring to the registration indexed by reg.x. If set to 0, the red MWI LED will <b>not</b> flash when there are new unread messages for the selected line. When set to 1, the LED will flash as long as there are new unread voicemail messages <i>for any line</i> in which this is parameter is enabled.		

<sup>1</sup> Change causes system to restart or reboot.

## <mwi/>

The parameters listed in the following table enable and disable a back light on the system screen to illuminate when you receive a new voicemail message.

### Message Waiting Indicator Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>mwi.backLight.disable</b>	<b>0 or 1</b>	<b>0</b>
<p>A back light on the system screen illuminates when you receive a new voicemail. Set to 0 to disable the back light message alert. Set to 1 to enable. The default is disabled.</p> <p>If mwi.backLight.disable is set to true then backLight will not be illuminated on new voice message arrival. By default it will be set to false and does not have any impact on existing functionality.</p>		

## <nat/>

The parameters listed in the following table define port and IP address changes used in NAT traversal. The port changes will change 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

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>nat.ip<sup>1</sup></b>	<b>dotted- decimal IP address</b>	<b>Null</b>
<p>IP address to advertise within SIP signaling - should match the external IP address used by the NAT device.</p>		
<b>nat.keepalive.interval</b>	<b>0 to 3600</b>	<b>0</b>
<p>The keep-alive interval in seconds. Sets the interval at which systems will send a keep-alive 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 will not send out keep-alive messages.</p>		
<b>nat.mediaPortStart<sup>1</sup></b>	<b>0 to 65440</b>	<b>0</b>
<p>The initially allocated RTP port. Overrides the value set for <code>tcIpApp.port.rtp.mediaPortRangeStart</code>.</p>		
<b>nat.signalPort<sup>1</sup></b>	<b>1024 to 65535</b>	<b>0</b>
<p>The port used for SIP signaling. Overrides <code>voIpProt.local.port</code>.</p>		

<sup>1</sup> Change causes system to restart or reboot.



## <systemLock/>

The parameters listed in the following table. The Enhanced Feature Key feature must be enabled if you want to use the **Lock** soft key.

### System Lock Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>systemLock.authorized.x.description</b> The name or description of an authorized number	<b>String</b>	
<b>systemLock.authorized.x.value</b> The number or address for an authorized contact	<b>string</b>	
Up to five (x=1 to 5) authorized contacts that a user can call while their system is locked. Each contact needs a description to display on the screen, and a system number or address value for the system to dial.		
<b>systemLock.browserEnabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the microbrowser or browser is not displayed while the system is locked. If 1, the microbrowser or browser is displayed while the system is locked.		
<b>systemLock.dndWhenLocked</b>	<b>0 or 1</b>	<b>0</b>
If 0, the system can receive calls while it is locked. If 1, the system enters Do-Not-Disturb mode while it is locked. Note: The user can change this setting from the system user interface.		
<b>systemLock.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the system lock feature is disabled. If 1, the system lock feature is enabled. Note: To 'unlock' the system remotely (in conjunction with deleting/modifying the overrides files), disable and re-enable this parameter.		
<b>systemLock.idleTimeout</b>	<b>0 to 65535</b>	<b>0</b>
The amount of time (in seconds) the system can be idle before it automatically locks. If 0, automatic locking is disabled.		
<b>systemLock.lockState</b>	<b>0 or 1</b>	<b>0</b>
The value for this parameter indicates whether the system is locked or unlocked and changes each time you lock or unlock the system. If 0, the system is unlocked. If 1, the system is locked. Note that the system stores and uploads the value each time it changes via the <code>MAC-system.cfg</code> . You can set this parameter remotely using the Web Configuration Utility.		
<b>systemLock.powerUpUnlocked</b>	<b>0 or 1</b>	<b>0</b>
Use this parameter to override <code>systemLock.lockState</code> . If 0, the system retains the value in <code>systemLock.lockState</code> . If 1, you can restart, reboot, or power cycle the system to override the value for <code>systemLock.lockState</code> in the <code>MAC-system.cfg</code> and start the system in an unlocked state. You can then lock or unlock the system locally. Polycom recommends that you do not leave this parameter enabled.		

<sup>1</sup> Change causes system to restart or reboot.

## <powerSaving/>

The power saving feature automatically turns off the system's LCD display when not in use.

---

**Power Saving Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>powerSaving.enable</b>	<b>0 or 1</b>	<b>1</b>
If 0, the LCD power saving feature is disabled. If 1, the feature is enabled. The power-saving feature is enabled by default.		
<b>powerSaving.idleTimeout.offHours</b>	<b>1 to 10</b>	<b>1</b>
The number of minutes to wait while the system is idle during off hours before activating power saving.		
<b>powerSaving.idleTimeout.officeHours</b>	<b>1 to 600 minutes</b>	<b>480</b>
The number of minutes to wait while the system is idle during office hours before activating power saving. Note that the default time is 480 minutes.		
<b>powerSaving.idleTimeout.userInputExtension</b>	<b>1 to 20</b>	<b>10</b>
The minimum number of minutes to wait while the system is idle—after using the system—before activating power saving.		
<b>powerSaving.officeHours.duration.monday</b>	<b>0 to 24</b>	<b>12</b>
<b>powerSaving.officeHours.duration.tuesday</b>	<b>0 to 24</b>	<b>12</b>
<b>powerSaving.officeHours.duration.wednesday</b>	<b>0 to 24</b>	<b>12</b>
<b>powerSaving.officeHours.duration.thursday</b>	<b>0 to 24</b>	<b>12</b>
<b>powerSaving.officeHours.duration.friday</b>	<b>0 to 24</b>	<b>12</b>
<b>powerSaving.officeHours.duration.saturday</b>	<b>0 to 24</b>	<b>0</b>
<b>powerSaving.officeHours.duration.sunday</b>	<b>0 to 24</b>	<b>0</b>
The duration of the day's office hours.		
<b>powerSaving.officeHours.startHour.xxx</b>	<b>0 to 23</b>	<b>7</b>
The starting hour for the day's office hours, where xxx is one of monday, tuesday <sup>n</sup> , wednesday, thursday, friday, saturday, and sunday (refer to <code>powerSaving.officeHours.duration</code> for an example).		
<b>powerSaving.userDetectionSensitivity.offHours</b>	<b>0 to 10</b>	<b>2</b>
The sensitivity of the algorithm used to detect the presence of the system's user during off hours. 10 is the most sensitive. If set to 0, this feature is disabled. The default value was chosen for good performance in a typical office environment and is biased for difficult detection during off hours.		
<b>powerSaving.userDetectionSensitivity.officeHours</b>	<b>0 to 10</b>	<b>7</b>
The sensitivity of the algorithm used to detect the presence of the system's user during office hours. 10 is the most sensitive. If set to 0, this feature is disabled. The default value was chosen for good performance in a typical office environment and is biased for easy detection during office hours.		

---

## <pres/>

The following table lists parameters you can configure for the presence feature. Note that the parameter `pres.reg` is the line number used to send SUBSCRIBE. If this parameter is missing, the system will use the primary line to send SUBSCRIBE.

### Presence Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>pres.idleSoftkeys</b>	<b>0 or 1</b>	<b>1</b>
If 0, the <b>MyStat</b> and <b>Buddies</b> presence idle soft keys do not display. If 1, the soft keys display.		
<b>pres.idleTimeout.offHours.enabled</b>	<b>0 or 1</b>	<b>1</b>
If 0, the off hours idle timeout feature is disabled. If 1, the feature is enabled.		
<b>pres.idleTimeout.offHours.period</b>	<b>1 to 600</b>	<b>15</b>
The number of minutes to wait while the system is idle during off hours before showing the Away presence status.		
<b>pres.idleTimeout.officeHours.enabled</b>	<b>0 or 1</b>	<b>1</b>
If 0, the office hours idle timeout feature is disabled. If 1, the feature is enabled.		
<b>pres.idleTimeout.officeHours.period</b>	<b>1 to 600</b>	<b>15</b>
The number of minutes to wait while the system is idle during office hours before showing the Away presence status.		
<b>pres.reg</b>	<b>1 to 34</b>	<b>1</b>
The valid line/registration number that is used for presence. This registration sends a SUBSCRIBE for presence. If the value is not a valid registration, this parameter is ignored.		

## <prov/>

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

### Provisioning Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>prov.autoConfigUpload.enabled</b>	<b>string</b>	<b>Null</b>
Enable or disable the automatic upload of system and Web Configuration Utility override configuration files to the provisioning server. By default, per-system MAC-system.cfg and MAC-web.cfg files are automatically uploaded to the provisioning server when a configuration change is made from the system's interface or Web Configuration Utility respectively. When disabled, per-system override files are not uploaded to the provisioning server.		
<b>prov.configUploadPath</b>	<b>string</b>	<b>Null</b>
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.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>prov.login.automaticLogout</b>	<b>0 to 46000</b>	<b>0</b>
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.		
<b>prov.login.defaultPassword</b>	<b>String</b>	<b>Null</b>
The login password for the default user.		
<b>prov.login.defaultOnly</b>	<b>0 or 1</b>	<b>0</b>
If 1, the default user is the only user who can log in. If 0, other users can log in.		
<b>prov.login.defaultUser</b>	<b>String</b>	<b>Null</b>
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.		
<b>prov.login.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the user profile feature is disabled. If 1, the user profile feature is enabled.		
<b>prov.login.lcCache.domain</b>	<b>0 to 64</b>	<b>Null</b>
The user's sign-in domain name.		
<b>prov.login.lcCache.user</b>	<b>0 to 64</b>	<b>Null</b>
The user's sign-in user name.		
<b>prov.login.localPassword</b>	<b>String</b>	<b>123</b>
The password used to validate the user login. It is stored either as plain text or encrypted (an SHA1 hash).		
<b>prov.login.persistent</b>	<b>0 or 1</b>	<b>0</b>
If 0, users are logged out if the handset reboots. If 1, users remain logged in when the system reboots.		
<b>prov.login.required</b>	<b>0 or 1</b>	<b>0</b>
If 1, a user must log in when the login feature is enabled. If 0, the user does not have to log in.		
<b>prov.loginCredPwdFlushed.enabled</b>	<b>0 or 1</b>	<b>1</b>
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.		
<b>prov.polling.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the provisioning server is not automatically polled for upgrades. If 1, the provisioning server is polled.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>prov.polling.mode</b>	<b>abs, rel, random</b>	<b>abs</b>
<p>The polling mode.</p> <p><b>abs</b> The system polls every day at the time specified by <code>prov.polling.time</code>.</p> <p><b>rel</b> The system polls after the number of seconds specified by <code>prov.polling.period</code>.</p> <p><b>random</b> The system polls at random between a starting time set in <code>prov.polling.time</code> and an end time set in <code>prov.polling.timeRandomEnd</code>.</p> <p>Note that if you set the polling period in <code>prov.polling.period</code> 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 will not change with a reboot whereas the time within the start and end is calculated again with every reboot.</p>		
<b>prov.polling.period</b>	<b>integer &gt; 3600</b>	<b>86400</b>
<p>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.</p>		
<b>prov.polling.time</b>	<b>hh:mm</b>	<b>03:00</b>
<p>The polling start time. Used in absolute and random modes.</p>		
<b>prov.polling.timeRandomEnd</b>	<b>hh:mm</b>	<b>Null</b>
<p>The polling stop time. Only used in random mode.</p>		
<b>prov.quickSetup.enabled</b>	<b>0 or 1</b>	<b>0</b>
<p>If 0, the quick setup feature is disabled. If 1, the quick setup feature is enabled.</p>		
<b>prov.startupCheck.enabled</b>	<b>0 or 1</b>	<b>1</b>
<p>If 0, the system is not provisioned at startup. If 1, the system is provisioned at start up. All configuration files, licenses, and overrides are downloaded even if the software changes. (The previous behavior was to reboot as soon as the system determined that software changed.)</p>		

<sup>1</sup> Change causes system to restart or reboot.

## <ptt/>

The parameters in the following table apply to page mode.

### Group Paging Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>ptt.address</b>	<b>multicast IP address</b>	<b>224.0.1.116</b>
<p>The multicast IP address to send page audio to and receive page audio from.</p>		
<b>ptt.pageMode.enable</b>	<b>0 or 1</b>	<b>0</b>
<p>If 0, group paging is disabled. If 1, group paging is enabled.</p>		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>ptt.pageMode.displayName</b>	<b>up to 64 octet UTF-8 string</b>	<b>PTT</b>
This display name is shown in the caller ID field of outgoing group pages. If Null, the value from <code>reg.1.displayName</code> will be used.		
<b>ptt.pageMode.group.x.available</b> <b>Make the group available to the user</b>	<b>0 or 1</b>	<b>1</b>
<b>ptt.pageMode.group.x.allowTransmit</b> <b>Allow outgoing announcements to the group</b>	<b>0 or 1</b>	<b>1</b>
<b>ptt.pageMode.group.x.label</b> <b>The label to identify the group</b>	<b>string</b>	<b>ch24: Priority, ch25: Emergency, others: Null</b>
<b>ptt.pageMode.group.x.subscribed</b> <b>Subscribe the system to the group</b>	<b>0 or 1</b>	<b>ch1, 24, 25: 1, others: 0</b>
A page mode group <code>x</code> , where <code>x</code> = 1 to 25. The <code>label</code> is the name used to identify the group during pages. If <code>available</code> is disabled (0), the user cannot access the group or subscribe and the other page mode group parameters will be ignored. If enabled, the user can access the group and choose to subscribe. If <code>allowTransmit</code> is disabled (0), the user cannot send outgoing pages to the group. If enabled, the user may send outgoing pages. If <code>subscribed</code> is disabled, the system will not be subscribed to the group. If enabled, the system will subscribe to the group.		

## <qos/>

These parameters listed in the following table control 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

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>qos.ethernet.callControl.user_priority<sup>1</sup></b>	<b>0 to 7</b>	<b>5</b>
User-priority used for call control packets.		
<b>qos.ethernet.other.user_priority<sup>1</sup></b>	<b>0 to 7</b>	<b>2</b>
User-priority used for packets that do not have a per-protocol setting.		
<b>qos.ethernet.rtp.user_priority<sup>1</sup></b>	<b>0 to 7</b>	<b>5</b>
Choose the priority of voice Real-Time Protocol (RTP) packets. The default priority level is 5.		
<b>qos.ethernet.rtp.video.user_priority<sup>1</sup></b>	<b>0 to 7</b>	<b>5</b>
User-priority used for Video RTP packets.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>qos.ip.callControl.dscp<sup>1</sup></b>	<b>0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43</b>	<b>Null</b>
Specify the DSCP of packets. If the value is not null, this parameter will override the other <code>qos.ip.callControl.*</code> parameters. The default value is Null, so the other <code>qos.ip.callControl.*</code> parameters will be used if no value is entered.		
<b>qos.ip.callControl.max_reliability<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>qos.ip.callControl.max_throughput<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>qos.ip.callControl.min_cost<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>qos.ip.callControl.min_delay<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>qos.ip.callControl.precedence<sup>1</sup></b>	<b>0 -7</b>	<b>5</b>
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.		
<b>qos.ip.rtp.dscp<sup>1</sup></b>	<b>0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43</b>	<b>Null</b>
Specify the DSCP of packets. If the value is not null, this parameter will override the other <code>qos.ip.rtp.*</code> parameters. The default value is Null, so the other <code>quality.ip.rtp.*</code> parameters will be used.		
<b>qos.ip.rtp.max_reliability<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>qos.ip.rtp.max_throughput<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>qos.ip.rtp.min_cost<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>qos.ip.rtp.min_delay<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>qos.ip.rtp.precedence<sup>1</sup></b>	<b>0 -7</b>	<b>5</b>
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.		
<b>qos.ip.rtp.video.dscp<sup>1</sup></b>	<b>0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43</b>	<b>Null</b>
Allows the DSCP of packets to be specified. If the value is non-null, this parameter will override the other <code>qos.ip.rtp.video.*</code> parameters. The default value is Null, so the other <code>qos.ip.rtp.video.*</code> parameters will be used.		
<b>qos.ip.rtp.video.max_reliability<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>qos.ip.rtp.video.max_throughput<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>qos.ip.rtp.video.min_cost<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<b>qos.ip.rtp.video.min_delay<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
<b>qos.ip.rtp.video.precedence<sup>1</sup></b>	<b>0 -7</b>	<b>5</b>
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.		

<sup>1</sup> Change causes system to restart or reboot.

## <reg/>

Each registration can optionally be associated with a private array of servers for completely segregated signaling. The CX5500 system supports a total of 16 registrations.

In the following tables, x is the registration number. For the CX5500, x=1-16.

The tables [Registration Parameters](#) and [Registration Server Parameters](#) list all line registration and server registration parameters.

### Registration Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>reg.x.acd-login-logout</b>	<b>0 or 1</b>	<b>0</b>
<b>reg.x.acd-agent-available</b>	<b>0 or 1</b>	<b>0</b>
If both ACD login/logout and agent available are set to 1 for registration x, the ACD feature will be enabled for that registration.		
<b>reg.x.address</b>	<b>string address</b>	<b>Null</b>
The user part (for example, 1002) or the user and the host part (for example, 1002@polycom.com) of the registration SIP URI extension.		
<b>reg.x.applyServerDigitMapLocally</b>	<b>0 or 1</b>	<b>0</b>
If 1 and <code>reg.x.server.y.specialInterop</code> is set to <code>lync2010</code> , the system uses the dialplan from the Microsoft Lync Server. Any dialed number will apply the dial plan locally. If 0, the dialplan from the Microsoft Lync Server is not used.		
<b>reg.x.auth.domain</b>	<b>string</b>	<b>Null</b>
The domain of the authorization server that is used to check the user names and passwords.		
<b>reg.x.auth.optimizedInFailover</b>	<b>0 or 1</b>	<b>0</b>
The destination of the first new SIP request when failover occurs. If 0, the SIP request is sent to the server with the highest priority in the server list. If 1, the SIP request is sent to the server which sent the proxy authentication request.		
<b>reg.x.auth.password</b>	<b>string</b>	<b>Null</b>
The password to be used for authentication challenges for this registration. If the password is non-Null, it will override the password entered into the Authentication submenu on the Settings menu of the system.		
<b>reg.x.auth.userId</b>	<b>string</b>	<b>Null</b>
User ID to be used for authentication challenges for this registration. If the User ID is non-Null, it will override the user parameter entered into the Authentication submenu on the Settings menu of the system.		
<b>reg.x.auth.useLoginCredentials</b>	<b>0 or 1</b>	<b>0</b>
If 0, login credentials are not used for authentication to the server on registration x. If 1, login credentials are used for authentication to the server.		
<b>reg.x.bargeInEnabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, barge-in is disabled for line x. If 1, barge-in is enabled (remote users of shared call appearances can interrupt or barge in to active calls).		



<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>reg.x.callsPerLineKey<sup>1</sup></b>	<b>1-24</b>	<b>24</b>
Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all systems sharing that registration. This parameter overrides <code>call.callsPerLineKey</code> .		
<b>reg.x.csta</b>	<b>0 or 1</b>	<b>0</b>
If 0, the uaCSTA (User Agent Computer Supported Telecommunications Applications) feature is disabled. If 1, uaCSTA is enabled (overrides the global parameter <code>voIpProt.SIP.csta</code> ).		
<b>reg.x.dialPlanName</b>	<b>String</b>	<b>Null</b>
If <code>reg.x.server.y.specialInterop</code> is set to <code>lync2010</code> , the dialplan name from the Microsoft Lync Server is stored here. Each registration has its own name for this dialplan. Note: Do not change this parameter if set by Microsoft Lync.		
<b>reg.x.displayName</b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The display name used in SIP signaling or as the default caller ID.		
<b>reg.x.filterReflectedBlaDialogs</b>	<b>0 or 1</b>	<b>1</b>
If 0, bridged line appearance NOTIFY messages (dialog state change) will not be ignored. If 1, the messages will be ignored.		
<b>reg.x.fwd.busy.contact</b>	<b>string</b>	<b>Null</b>
The forward-to contact for calls forwarded due to busy status. If Null, the contact specified by <code>divert.x.contact</code> will be used.		
<b>reg.x.fwd.busy.status</b>	<b>0 or 1</b>	<b>0</b>
If 0, incoming calls that receive a busy signal will not be forwarded. If 1, busy calls are forwarded to the contact specified by <code>reg.x.fwd.busy.contact</code> .		
<b>reg.x.fwd.noanswer.contact</b>	<b>string</b>	<b>Null</b>
The forward-to contact used for calls forwarded due to no answer. If Null, the contact specified by <code>divert.x.contact</code> will be used.		
<b>reg.x.fwd.noanswer.ringCount</b>	<b>0 to 65535</b>	<b>0</b>
The number of seconds the system should ring for before the call is forwarded because of no answer. Note: The maximum value accepted by some call servers is 20.		
<b>reg.x.fwd.noanswer.status</b>	<b>0 or 1</b>	<b>0</b>
If 0, calls are not forwarded if there is no answer. If 1, calls are forwarded to the contact specified by <code>reg.x.noanswer.contact</code> after ringing for the length of time specified by <code>reg.x.fwd.noanswer.ringCount</code> .		
<b>reg.x.ice.turn.callAdmissionControl.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, call admission control is disabled. If 1, call admission control is enabled for calls using the Microsoft Lync 2010 Server.		
<b>reg.x.label</b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The text label that displays next to the line key for registration x. If Null, the user part of <code>reg.x.address</code> is used.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>reg.x.lcs</b>	<b>0 or 1</b>	<b>0</b>
If 0, the Microsoft Live Communications Server (LSC) is not supported for registration x. If 1, LSC is supported.		
<b>reg.x.lineKeys</b>	<b>1 to max</b>	<b>1</b>
Specify the number of line keys to use for a single registration. The maximum number of line keys you can use per registration depends on your system model. To find out the maximum number for your system, see <b>Error! Reference source not found.</b>		
<b>reg.x.lisdisclaimer</b>	<b>string, 0 to 256 characters</b>	<b>Null</b>
This parameter sets the value of the location policy disclaimer. For example, the disclaimer may be "Warning: If you do not provide a location, emergency services may be delayed in reaching your location should you need to call for help." This parameter is set by in-band provisioning when the system is registered to Microsoft Lync Server 2010.		
<b>reg.x.lync.autoProvisionCertLocation</b>	<b>0 to 6</b>	<b>6</b>
If 0, the certificate download is disabled. If non-0, the certificate corresponding to the index of the appropriate <code>sec.TLS.customCaCert.X</code> is downloaded.		
<b>reg.x.musicOnHold.uri</b>	<b>a SIP URI</b>	<b>Null</b>
A URI that provides the media stream to play for the remote party on hold. If present and not Null, this parameter overrides <code>voIpProt.SIP.musicOnHold.uri</code> .		
<b>reg.x.outboundProxy.address</b>	<b>dotted-decimal IP address or hostname</b>	<b>Null</b>
The IP address or hostname of the SIP server to which the system sends all requests.		
<b>reg.x.outboundProxy.failOver.failBack.mode</b>	<b>newRequests DNSTTL registration duration</b>	<b>newRequests</b>
<p>The mode for failover failback (overrides <code>reg.x.server.y.failOver.failBack.mode</code>).</p> <p><b>newRequests</b> all new requests are forwarded first to the primary server regardless of the last used server.</p> <p><b>DNSTTL</b> the system tries the primary server again after a timeout equal to the DNS TTL configured for the server that the system is registered to.</p> <p><b>registration</b> the system tries the primary server again when the registration renewal signaling begins.</p> <p><b>duration</b> the system tries the primary server again after the time specified by <code>reg.x.outboundProxy.failOver.failBack.timeout</code> expires.</p>		
<b>reg.x.outboundProxy.failOver.failBack.timeout</b>	<b>0, 60 to 65535</b>	<b>3600</b>
The time to wait (in seconds) before failback occurs (overrides <code>reg.x.server.y.failOver.failBack.timeout</code> ). If the fail back mode is set to Duration, the system waits this long after connecting to the current working server before selecting the primary server again. If 0, the system will not fail-back until a fail-over event occurs with the current server.		
<b>reg.x.outboundProxy.failOver.failRegistrationOn</b>	<b>0 or 1</b>	<b>0</b>
When set to 1, and the <code>reRegisterOn</code> parameter is enabled, the system will silently invalidate an existing registration (if it exists), at the point of failing over. When set to 0, and the <code>reRegisterOn</code> parameter is enabled, existing registrations will remain active. This means that the system will attempt failback without first attempting to register with the primary server to determine if it has recovered.		
Note that <code>reg.x.outboundProxy.failOver.RegisterOn</code> must be enabled.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>reg.x.outboundProxy.failOver.onlySignalWithRegistered</b>	<b>0 or 1</b>	<b>1</b>
<p>When set to 1, and the reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the system attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call will end. No SIP messages will be sent to the unregistered server. When set to 0, and the reRegisterOn and failRegistrationOn parameters are enabled, signaling will be accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).</p>		
<b>reg.x.outboundProxy.failOver.reRegisterOn</b>	<b>0 or 1</b>	<b>0</b>
<p>This parameters overrides reg.x.server.y.failOver.failBack.RegisterOn. When set to 1, the system will attempt to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling will proceed with the secondary server. When set to 0, the system won't attempt to register with the secondary server, since the system will assume that the primary and secondary servers share registration information.</p>		
<b>reg.x.outboundProxy.port</b>	<b>1 to 65535</b>	<b>0</b>
<p>The port of the SIP server to which the system sends all requests.</p>		
<b>reg.x.outboundProxy.transport</b>	<b>DNSNaptr, TCPpreferred, UDPOnly, TLS, TCPOnly</b>	<b>DNSNaptr</b>
<p>The transport method the system uses to communicate with the SIP server.</p> <p><b>Null or DNSNaptr</b> if reg.x.outboundProxy.address is a hostname and reg.x.outboundProxy.port is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If reg.x.outboundProxy.address is an IP address, or a port is given, then UDP is used.</p> <p><b>TCPpreferred</b> TCP is the preferred transport, UDP is used if TCP fails.</p> <p><b>UDPOnly</b> only UDP will be used.</p> <p><b>TLS</b> if TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061.</p> <p><b>TCPOnly</b> only TCP will be used.</p>		
<b>reg.x.proxyRequire</b>	<b>string</b>	<b>Null</b>
<p>The string that needs to be entered in the Proxy-Require header. If Null, no Proxy-Require will be sent.</p>		
<b>reg.x.ringType</b>	<b>default, ringer1 to ringer24</b>	<b>ringer2</b>
<p>The ringer to be used for calls received by this registration. The default is the first non-silent ringer.</p> <p>The configuration parameter reg.x.ringtype correctly uses the ringtones ringer13 or ringer14 only if np.normal.ringing.calls.tonePattern is set to default or if reg.x.ringtype is used by multiple line registrations. If you use the configuration parameters ringer13 and ringer14 on a single registered line, the system plays SystemRing.wav. When setting reg.x.ringType to ringer13 or to ringer14. Using the Web Configuration Utility, the correct ringtone is played using the override parameter np.normal.ringing.calls.tonePattern=ringer13.</p>		
<b>reg.x.ringType.privateLine</b>	<b>default, ringer1 to ringer24</b>	<b>default</b>
<p>The ringer to be used for calls received by a private line connected to Microsoft Lync Server 2010.</p>		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>reg.x.serverAutoDiscovery</b>	<b>0 or 1</b>	<b>1</b>
Determines whether or not to discover the server address automatically. This parameter is used with Microsoft Lync Server 2010.		
<b>reg.x.serverFeatureControl.cf<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, server-based call forwarding is not enabled. If 1, server based call forwarding is enabled. This parameter overrides <code>voIpProt.SIP.serverFeatureControl.cf</code> .		
<b>reg.x.serverFeatureControl.dnd<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, server-based do-not-disturb (DND) is not enabled. If 1, server-based DND is enabled and the call server has control of DND. This parameter overrides <code>voIpProt.SIP.serverFeatureControl.dnd</code> .		
<b>reg.x.serverFeatureControl.localProcessing.cf</b>	<b>0 or 1</b>	<b>1</b>
If 0 and <code>reg.x.serverFeatureControl.cf</code> is set to 1, the system will not perform local Call Forward behavior. If set to 1, the system will perform local Call Forward behavior on all calls received. This parameter overrides <code>voIpProt.SIP.serverFeatureControl.localProcessing.cf</code> .		
<b>reg.x.serverFeatureControl.localProcessing.dnd</b>	<b>0 or 1</b>	<b>1</b>
If 0 and <code>reg.x.serverFeatureControl.dnd</code> is set to 1, the system will not perform local DND call behavior. If set to 1, the system will perform local DND call behavior on all calls received. This parameter overrides <code>voIpProt.SIP.serverFeatureControl.localProcessing.dnd</code> .		
<b>reg.x.serverFeatureControl.signalingMethod</b>	<b>string</b>	<b>serviceMsForwardContact</b>
Controls the method used to perform call forwarding requests to the server.		
<b>reg.x.server.y.registerRetry.maxTimeout</b>		<b>180 seconds</b>
Set the maximum period of time in seconds that you want the system to try registering with the server.		
<b>reg.x.srtp.enable<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the registration always declines SRTP offers. If 1, the registration accepts SRTP offers.		
<b>reg.x.srtp.offer<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 1, the registration includes a secure media stream description along with the usual non-secure media description in the SDP of a SIP INVITE. This parameter applies to the registration initiating (offering) a system call. If 0, no secure media stream is included in SDP of a SIP invite.		
<b>reg.x.srtp.require<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, secure media streams are not required. If 1, the registration is only allowed to use secure media streams. Any offered SIP INVITEs must include a secure media description in the SDP or the call will be 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, <code>reg.x.srtp.offer</code> will also be set to 1, regardless of the value in the configuration file.		
<b>reg.x.srtp.simplifiedBestEffort</b>	<b>0 or 1</b>	<b>0</b>
If 0, no SRTP is supported. If 1, negotiation of SRTP compliant with Microsoft Session Description Protocol Version 2.0 Extensions is supported. This parameter overrides <code>sec.srtp.simplifiedBestEffort</code> .		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>reg.x.strictLineSeize</b>	<b>0 or 1</b>	<b>0</b>
If 1, the system is forced to wait for 200 OK on registration x when receiving a TRYING notify. If set to 0, dial prompt is provided immediately when you attempt to seize a shared line without waiting for a successful OK from the call server. This parameter overrides <code>voIpProt.SIP.strictLineSeize</code> for registration x.		
<b>reg.x.tcpFastFailover</b>	<b>0 or 1</b>	<b>0</b>
If 1, failover occurs based on the values of <code>reg.x.server.y.retryMaxCount</code> and <code>voIpProt.server.x.retryTimeOut</code> . If 0, a full 32 second RFC compliant timeout is used.		
<b>reg.x.telephony</b>	<b>0 or 1</b>	<b>1</b>
If 0, telephony calls are not enabled on this registration (use this value if the registration is used with Microsoft Office Communications Server 2007 R2 or Microsoft Lync 2010). If 1, telephony calls are enabled on this registration.		
<b>reg.x.thirdPartyName</b>	<b>string address</b>	<b>Null</b>
This field must match the <code>reg.x.address</code> value of the registration which makes up the part of a bridged line appearance (BLA). It must be Null in all other cases.		
<b>reg.x.type</b>	<b>private or shared</b>	<b>private</b>
If set to private, use standard call signaling. If set to shared, augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.		

<sup>1</sup> Change causes system to restart or reboot.

You can list multiple registration servers for fault tolerance. In the table [Registration Server Parameters](#), you can list four servers by using `y=1` to 4. If the `reg.x.server.y.address` is not null, all of the parameters in the following table will override the parameters specified in `voIpProt.server.*`. The server registration parameters are listed in the following table:

#### Registration Server Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>Desired registration period.</b>		
<code>reg.x.server.y.address</code>	dotted-decimal IP address or hostname	Null
<b>The IP address or host name of a SIP server that accepts registrations. If not Null, all of the parameters in this table will override the parameters specified in <code>voIpProt.server.*</code>. Notes: If this parameter is set, it will take precedence even if the DHCP server is available.</b>		
<code>reg.x.server.y.expires</code>	positive integer, minimum 10	3600
<b>The system's requested registration period in seconds. Note: The period negotiated with the server may be different. The system will attempt to re-register at the beginning of the overlap period. For example, if <code>expires="300"</code> and <code>overlap="5"</code>, the system will re-register after 295 seconds (300-5).</b>		
<code>reg.x.server.y.expires.lineSeize</code>	0 to 65535	30

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>Requested line-seize subscription period.</b>		
reg.x.server.y.expires.overlap	5 to 65535	60
<b>The number of seconds before the expiration time returned by server x at which the system should try to re-register. The system will try to re-register at half the expiration time returned by the server if the server value is less than the configured overlap value.</b>		
reg.x.server.y.failOver.failBack.mode	newRequests DNSTTL registration duration	newRequests
<b>The mode for failover failback (this parameter overrides voIpProt.server.x.failOver.failBack.mode):</b>		
<b>newRequests</b> – all new requests are forwarded first to the primary server regardless of the last used server.		
<b>DNSTTL</b> – the system tries the primary server again after a timeout equal to the DNS TTL configured for the server that the system is registered to.		
<b>registration</b> – the system tries the primary server again when the registration renewal signaling begins.		
<b>duration</b> – the system tries the primary server again after the time specified by reg.x.server.y.failOver.failBack.timeout.		
reg.x.server.y.failOver.failBack.timeout	0, 60 to 65535	3600
<b>The time to wait (in seconds) before failback occurs (overrides voIpProt.server.x.failOver.failBack.timeout).If the fail back mode is set to Duration, the system waits this long after connecting to the current working server before selecting the primary server again. If 0, the system will not fail-back until a fail-over event occurs with the current server.</b>		
reg.x.server.y.failOver.failRegistrationOn	0 or 1	0
<b>When set to 1, and the reRegisterOn parameter is enabled, the system will silently invalidate an existing registration (if it exists), at the point of failing over. When set to 0, and the reRegisterOn parameter is enabled, existing registrations will remain active. This means that the system will attempt failback without first attempting to register with the primary server to determine if it has recovered.</b>		
reg.x.server.y.failOver.onlySignalWithRegistered	0 or 1	1
<b>When set to 1, and the reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the system attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call will end. No SIP messages will be sent to the unregistered server. When set to 0, and the reRegisterOn and failRegistrationOn parameters are enabled, signaling will be accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).</b>		
reg.x.server.y.failOver.reRegisterOn	0 or 1	0
<b>This parameter overrides the voIpProt.server.x.failOver.reRegisterOn. When set to 1, the system will attempt to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling will proceed with the secondary server. When set to 0, the system won't attempt to register with the secondary server, since the system will assume that the primary and secondary servers share registration information.</b>		
reg.x.server.y.lcs	0 or 1	0

Parameter	Permitted Values	Default
<b>If 0, the Microsoft Live Communications Server (LSC) is not supported. If 1, LCS is supported for registration x.</b>		
reg.x.server.y.useOutboundProxy	0 or 1	1
<b>Specify whether or not to use the outbound proxy specified in reg.x.outboundProxy.address for server x. This parameter overrides voIpProt.server.x.useOutboundProxy for registration x.</b>		
reg.x.server.y.port	0, 1 to 65535	Null
<b>The port of the sip server that specifies registrations. If 0, the port used depends on reg.x.server.y.transport.</b>		
reg.x.server.y.register	0 or 1	1
<b>If 0, calls can be routed to an outbound proxy without registration. See volpProt.server.x.register. For more information, see <a href="#">Technical Bulletin 5844: SIP Server Fallback Enhancements on Polycom Systems</a>.</b>		
reg.x.server.y.registerRetry.baseTimeOut	10 - 120	60
<b>The base time period to wait before a registration retry. Used in conjunction with reg.x.server.y.registerRetry.maxTimeOut to determine how long to wait. The algorithm is defined in RFC 5626.</b>		
reg.x.server.y.registerRetry.maxTimeOut	60 - 1800	60
<b>The maximum time period to wait before a registration retry. Used in conjunction with reg.x.server.y.registerRetry.baseTimeOut to determine how long to wait. The algorithm is defined in RFC 5626.</b>		
reg.x.server.y.retryMaxCount	0 to 20	3
<b>If set to 0, 3 is used. The number of retries that will be attempted before moving to the next available server.</b>		
reg.x.server.y.retryTimeOut	0 to 65535	0
<b>The amount of time (in milliseconds) to wait between retries. If 0, use standard RFC 3261 signaling retry behavior.</b>		
reg.x.server.y.specialInterop	standard, ocs2007r2, lcs2005, lync2010	standard
<b>Specify if this registration should support Microsoft Office Communications Server 2007 R2 (ocs2007r2), Microsoft Live Communications Server 2005 (lcs2005), or Microsoft Lync 2010 (lync2010).</b>		
reg.x.server.y.transport	DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly	DNSnaptr

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>The transport method the system uses to communicate with the SIP server.</b>		
<b>Null or DNSnaptr</b> – if <code>reg.x.server.y.address</code> is a hostname and <code>reg.x.server.y.port</code> is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If <code>reg.x.server.y.address</code> is an IP address, or a port is given, then UDP is used.		
<b>TCPpreferred</b> – TCP is the preferred transport; UDP is used if TCP fails.		
<b>UDPOnly</b> – only UDP will be used.		
<b>TLS</b> – if TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061.		
<b>TCPOnly</b> – only TCP will be used.		

## <request/>

The parameters listed in the following table control the system's behavior when a request for restart or reconfiguration is received.

### Configuration Request Parameter

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>request.delay.type<sup>1</sup></b>	<b>audio, call</b>	<b>call</b>

Specify when the system should process a request for a restart or reconfiguration. If set to `audio`, the request will be executed once there is no active audio on the system—regardless of the call state. If set to `call`, the request should be executed once there are no calls—in any state—on the system.

<sup>1</sup> Change causes system to restart or reboot.

## <roaming\_buddies/>

The parameters listed in the following table is used in conjunction with Microsoft Lync on most Polycom systems.

### Roaming Buddies Parameters

<i>Parameter</i>	<i>Permitted Value</i>	<i>Default</i>
<b>roaming_buddies.reg</b>	<b>1 to 34</b>	<b>Null</b>

The index of the registration which has roaming buddies support enabled. If Null, the roaming buddies feature is disabled. **Note:** This parameter must be set if the call server is Microsoft Lync.



## <roaming\_privacy/>

The parameters in the following table are used conjunction with Microsoft Lync Server on Lync-enabled Polycom systems.

### Roaming Privacy Parameters

<i>Parameter</i>	<i>Permitted Value</i>	<i>Default</i>
<b>roaming_privacy.reg</b>	<b>1 to 34</b>	<b>Null</b>

Specify the index of the registration/line that has roaming privacy support enabled. If Null, roaming privacy is disabled.

## <saf/>

The system uses built-in wave files for some sound effects. The built-in wave files can be replaced with files downloaded from the provisioning server or from the Internet. However, these are stored in volatile memory so the files will need to remain accessible should the system need to be rebooted. Files will be truncated to a maximum size of 300 kilobytes.

The following sampled audio WAVE (.wav) file formats are supported:

- mono 8 kHz G.711 u-Law
- G.711 A-Law
- L16/16000 (16-bit, 16 kHz sampling rate, mono)
- L16/32000 (16-bit, 32 kHz sampling rate, mono)
- L16/48000 (16-bit, 48 kHz sampling rate, mono)

In the following table, x is the sampled audio file number.

### Sampled Audio File Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>saf.x</b>	<b>Null or valid path name or an RFC 1738-compliant URL to a HTTP, FTP, or TFTP wave file resource.</b>	

If Null, the system will use a built-in file.

If set to a path name, the system will attempt to download this file at boot time from the provisioning server.

If set to a URL, the system will attempt to download this file at boot time from the Internet.

Note: A TFTP URL is expected to be in the format: `tftp://<host>/[pathname]<filename>`, for example: `tftp://somehost.example.com/sounds/example.wav` .

Note: See the above wave file format restrictions.

The following table defines the default usage of the sampled audio files with the system:

## Default Sample Audio File Usage

<i>Sampled Audio File Number</i>	<i>Default Use (Pattern Reference)</i>
1	Ringer 12 ( <i>se.pat.misc.welcome</i> )
2	Ringer 13 ( <i>se.pat.ringer.ringer15</i> )
3	Ringer 14 ( <i>se.pat.ringer.ringer16</i> )
4	Ringer 15 ( <i>se.pat.ringer.ringer17</i> )
5	Ringer 16 ( <i>se.pat.ringer.ringer18</i> )
6	Ringer 17 ( <i>se.pat.ringer.ringer19</i> )
7	Ringer 18 ( <i>se.pat.ringer.ringer20</i> )
8	Ringer 19 ( <i>se.pat.ringer.ringer21</i> )
9	Ringer 20 ( <i>se.pat.ringer.ringer22</i> )
10	Ringer 21 ( <i>se.pat.ringer.ringer23</i> )
11	Ringer 22 ( <i>se.pat.ringer.ringer24</i> )
12 to 24	Not Used

## <se/>

The following table lists configurable sound effect parameters. You can also configure sound effect patterns in <pat/> and ringtones in <rt/>. The system uses both synthesized (based on the chord-sets, see <chord/>) and sampled audio sound effects. Sound effects are defined by patterns: rudimentary sequences of chord-sets, silence periods, and wave files.

### Sound Effect Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>se.appLocalEnabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, local user interface sound effects such as confirmation/error tones, will be enabled.		
<b>se.destination</b>	<b>chassis, headset, handset, active</b>	<b>1</b>
The transducer or audio device that plays sound effects and alerts. Choose from the <i>chassis</i> (speakersystem), <i>headset</i> (if connected), <i>handset</i> , or the <i>active</i> destination. If <i>active</i> , alerts will play from the destination that is currently in use. For example, if you are in a call on the handset, a new incoming call will ring on the handset.		
<b>se.stutterOnVoiceMail</b>	<b>0 or 1</b>	<b>1</b>
If set to 1, a stuttered dial tone is used in place of a normal dial tone to indicate that one or more voicemail messages are waiting at the message center.		

## <pat/>

Patterns use a simple script language that allows different chord sets or wave files to be strung together with periods of silence. The script language uses the instructions shown in the following table.

### Sound Effects Pattern Types

<i>Instruction</i>	<i>Meaning</i>
<b>sampled (n)</b>	<b>Play sampled audio file n</b>
Example:	
<code>se.pat.misc.SAMPLED_1.inst.1.type = "sampled" (sampled audio file instruction type)</code>	
<code>se.pat.misc.SAMPLED_1.inst.1.value = "2" (specifies sampled audio file 2)</code>	
<b>chord (n, d)</b>	<b>Play chord set n (d is optional and allows the chord set ON duration to be overridden to d milliseconds)</b>
Example:	
<code>se.pat.callProg.busyTone.inst.2.type = "chord" (chord set instruction type)</code>	
<code>se.pat.callProg.busyTone.inst.2.value = "busyTone" (specifies sampled audio file busyTone)</code>	
<code>se.pat.callProg.busyTone.inst.2.param = "2000" (override ON duration of chord set to 2000 milliseconds)</code>	
<b>silence (d)</b>	<b>Play silence for d milliseconds (Rx audio is not muted)</b>
Example:	
<code>se.pat.callProg.bargeIn.inst.3.type = "silence" (silence instruction type)</code>	
<code>se.pat.callProg.bargeIn.inst.3.value = "300" (specifies silence is to last 300 milliseconds)</code>	
<b>branch (n)</b>	<b>Advance n instructions and execute that instruction (n must be negative and must not branch beyond the first instruction)</b>
Example:	
<code>se.pat.callProg.alerting.inst.4.type = "branch" (branch instruction type)</code>	
<code>se.pat.callProg.alerting.inst.4.value = "-2" (step back 2 instructions and execute that instruction)</code>	

In the following table, *x* is the pattern name, *y* is the instruction number. Both *x* and *y* need to be sequential. There are three categories cat of sound effect patterns: `callProg` (Call Progress Patterns), `ringer` (Ringer Patterns) and `misc` (Miscellaneous Patterns).

### Sound Effects Pattern Parameters

<i>Parameter</i>	<i>Permitted Values</i>
<b>se.pat.cat.x.name</b>	<b>UTF-8 encoded string</b>
Sound effects name, where <i>cat</i> is <code>callProg</code> , <code>ringer</code> , or <code>misc</code> .	
<b>se.pat.cat.x.inst.y.type</b>	<b>sampled, chord, silence, branch</b>
Type of sound effect, where <i>cat</i> is <code>callProg</code> , <code>ringer</code> , or <code>misc</code> .	

<i>Parameter</i>	<i>Permitted Values</i>
<b>se.pat.cat.x.inst.y.value</b>	<b>String</b>
The instruction: <code>sampled</code> – sampled audio file number, <code>chord</code> – type of sound effect, <code>silence</code> – silence duration in ms, <code>branch</code> – number of instructions to advance. <code>cat</code> is <code>callProg</code> , <code>ringer</code> , or <code>misc</code> .	

The following table shows the call progress pattern names and their descriptions:

**Call Progress Tone Pattern Names**

<i>Call Progress Pattern Name</i>	<i>Description</i>
<b>alerting</b>	Alerting
<b>bargeIn</b>	Barge-in tone
<b>busyTone</b>	Busy tone
<b>callWaiting</b>	Call waiting tone
<b>callWaitingLong</b>	Call waiting tone long (distinctive)
<b>confirmation</b>	Confirmation tone
<b>dialTone</b>	Dial tone
<b>howler</b>	Howler tone (off-hook warning)
<b>intercom</b>	Intercom announcement tone
<b>msgWaiting</b>	Message waiting tone
<b>precedenceCallWaiting</b>	Precedence call waiting tone
<b>precedenceRingback</b>	Precedence ringback tone
<b>preemption</b>	Preemption tone
<b>precedence</b>	Precedence tone
<b>recWarning</b>	Record warning
<b>reorder</b>	Reorder tone
<b>ringback</b>	Ringback tone
<b>secondaryDialTone</b>	Secondary dial tone
<b>stutter</b>	Stuttered dial tone

The following table shows the ring pattern names and their default descriptions:

### Ringtone Pattern Names

<i>Parameter Name</i>	<i>Ringtone Name</i>	<i>Description</i>
<b>ringer1</b>	Silent Ring	Silent ring
<b>ringer2</b>	Low Trill	Long single A3 Db3 major warble
<b>ringer3</b>	Low Double Trill	Short double A3 Db3 major warble
<b>ringer4</b>	Medium Trill	Long single C3 E3 major warble
<b>ringer5</b>	Medium Double Trill	Short double C3 E3 major warble
<b>ringer6</b>	High Trill	Long single warble 1
<b>ringer7</b>	High Double Trill	Short double warble 1
<b>ringer8</b>	Highest Trill	Long single Gb3 A4 major warble
<b>ringer9</b>	Highest Double Trill	Short double Gb3 A4 major warble
<b>ringer10</b>	Beeble	Short double E3 major
<b>ringer11</b>	Triplet	Short triple C3 E3 G3 major ramp
<b>ringer12</b>	Ringback-style	Short double ringback
<b>ringer13</b>	Low Trill Precedence	Long single A3 Db3 major warble Precedence
<b>ringer14</b>	Ring Splash	Splash
<b>ringer15</b>	Ring16	Sampled audio file 1
<b>ringer16</b>	Ring17	Sampled audio file 2
<b>ringer17</b>	Ring18	Sampled audio file 3
<b>ringer18</b>	Ring19	Sampled audio file 4
<b>ringer19</b>	Ring20	Sampled audio file 5
<b>ringer20</b>	Ring21	Sampled audio file 6
<b>ringer21</b>	Ring22	Sampled audio file 7
<b>ringer22</b>	Ring23	Sampled audio file 8
<b>ringer23</b>	Ring24	Sampled audio file 9
<b>ringer24</b>	Ring25	Sampled audio file 10

**Note: Silent Ring**

Silent ring will provide a visual indication of an incoming call, but no audio indication. Sampled audio files 1 to 10 all use the same built-in file unless that file has been replaced with a downloaded file. For more information, see <saf/>.

The following table shows the miscellaneous patterns and their descriptions:

**Miscellaneous Pattern Names**

<i>Miscellaneous pattern name</i>	<i>Description</i>
<b>instant message</b>	New instant message
<b>local hold notification</b>	Local hold notification
<b>message waiting</b>	New message waiting indication
<b>negative confirmation</b>	Negative confirmation
<b>positive confirmation</b>	Positive confirmation
<b>remote hold notification</b>	Remote hold notification
<b>welcome</b>	Welcome (boot up)

**<rt/>**

Ringtone is used to define a simple class of ring to be applied based on some credentials that are usually carried within the network protocol. The ring class includes parameters such as call-waiting and ringer index, if appropriate. The ring class can use one of four types of ring that are defined as follows:

- **ring** Play a specified ring pattern or call waiting indication
- **visual** Provide only a visual indication (no audio) of an incoming call, no ringer needs to be specified
- **answer** Provide auto-answer on an incoming call
- **ring-answer** Provide auto-answer on an incoming call after a certain number of rings

**Note: Using the Answer Ring Type**

The auto-answer on incoming call is currently only applied if there is no other call in progress on the system at the time.

The system supports the following ring classes: **default**, **visual**, **answerMute**, **autoAnswer**, **ringAnswerMute**, **ringAutoAnswer**, **internal**, **external**, **emergency**, **precedence**, **splash**, and **custom<y>** where y is 1 to 17.

In the following table, x is the ring class name.



**Caution: Ringtone Parameters Will Not Work After a Software Downgrade**

If a system has been upgraded to Polycom UC Software 4.0.0 and then downgraded to SIP 3.2.3 or earlier, the ringtone parameters will be unusable due to configuration parameters name changes in UC Software 4.0.0.

**Sound Effects Ringtone Parameters**

<i>Parameter</i>	<i>Permitted Values</i>
<b>se.rt.enabled</b>	<b>0 or 1 (default)</b>
If <b>0</b> , the ringtone feature is not enabled on the system. If <b>1</b> (default), the ringtone feature is enabled.	
<b>se.rt.modification.enabled</b>	<b>0 or 1 (default)</b>
A flag to determine whether or not to allow user modification (through system's user interface) of the pre-defined ringtone enabled for modification.	
<b>se.rt.&lt;ringClass&gt;.callWait</b>	<b>callWaiting, callWaitingLong, precedenceCallWaiting</b>
The call waiting tone to be used for this class of ring. The call waiting should match one defined in Call Progress Tone Pattern Names. The default call waiting tone is <code>callWaiting</code> .	
<b>se.rt.&lt;ringClass&gt;.name</b>	<b>UTF-8 encoded string</b>
The answer mode for a ringtone. Used for identification purposes in the user interface.	
<b>se.rt.&lt;ringClass&gt;.ringer</b>	<b>default, ringer1 to ringer24</b>
The ringtone to be used for this class of ring. The ringer should match one of Ringtone Pattern Names. The default ringer is <code>ringer2</code> .	
<b>se.rt.&lt;ringClass&gt;.timeout</b>	<b>1 to 60000 only relevant if the type is set to ring-answer</b>
The duration of the ring in milliseconds before the call is auto answered. The default is 2000.	
<b>se.rt.&lt;ringClass&gt;.type</b>	<b>ring, visual, answer, ring-answer</b>
The answer mode for a ringtone as defined in list earlier in this section.	

## <sec/>

The parameters listed in the following table affect the security features of the system. The configuration parameter is defined as follows:

### General Security Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>sec.tagSerialNo<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>

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.

<sup>1</sup> Change causes system to restart or reboot.

This parameter also includes:

- [<encryption/>](#)
- [<pwd/><length/>](#)
- [<srtp/>](#)
- [<dot1x/><eapollogoff/><hostmovedetect/>](#)
- [<TLS/>](#)
  - [<profile/>](#)
  - [<profileSelection/>](#)

## <encryption/>

The following table lists available encryption parameters.

### File Encryption Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>sec.encryption.upload.callLists<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<p>The encryption on the system-specific call lists that is uploaded to the provisioning server.            If 0, the call list is uploaded unencrypted regardless of how it was downloaded, the directory replaces whatever system-specific call list is on the server, even if the file on the server is encrypted.            If 1, the call list is uploaded encrypted regardless of how it was downloaded. The file replaces any existing system-specific call lists file on the server.</p>		
<b>sec.encryption.upload.config</b>	<b>0 or 1</b>	<b>0</b>
<p>The encryption on the system-specific configuration file created and uploaded to the provisioning server when the user selects <b>Upload Configuration</b> from the system menu.            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.</p>		



<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>sec.encryption.upload.dir<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<p>The encryption on the system-specific contact directory that is uploaded to the provisioning server. If 0, the directory is uploaded unencrypted regardless of how it was downloaded, the directory replaces whatever system-specific contact directory is on the server, even if the file on the server is encrypted. If 1, the directory is uploaded encrypted regardless of how it was downloaded. The file replaces any existing system-specific contact directory file on the server.</p>		
<b>sec.encryption.upload.overrides</b>	<b>0 or 1</b>	<b>0</b>
<p>The encryption on the system-specific <b>&lt;MACaddress&gt;-system.cfg</b> 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.</p>		

<sup>1</sup> Change causes system to restart or reboot.

## <pwd/><length/>

The following table lists configurable password length parameters.

### Password Length Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>sec.pwd.length.admin<sup>1</sup></b>	<b>0-32</b>	<b>1</b>
<p>The minimum length for administrator passwords changed using the system. Use 0 to allow null passwords.</p>		
<b>sec.pwd.length.user<sup>1</sup></b>	<b>0-32</b>	<b>2</b>
<p>The minimum length for user passwords changed using the system. Use 0 to allow null passwords.</p>		

<sup>1</sup> Change causes system to restart or reboot.

## <srtp/>

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

### SRTP Parameters

<i>Parameter</i>	<i>Permitted values</i>	<i>Defaults</i>
<b>sec.srtp.answerWithNewKey</b>	<b>0 or 1</b>	<b>1</b>
<p>If 0, a new key is not provided when answering a call. If 1, a new key is provided when answering a call.</p>		

<i>Parameter</i>	<i>Permitted values</i>	<i>Defaults</i>
<b>sec.srtp.enable<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the system always declines SRTP offers. If 1, the system accepts SRTP offers. Note: The defaults for SIP 3.2.0 was 0 when Null or not defined.		
<b>sec.srtp.key.lifetime<sup>1</sup></b>	<b>0, positive integer minimum 1024 or power of 2 notation</b>	<b>Null</b>
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 <sup>10</sup> ), the master key lifetime is set. When the lifetime is set, a re-invite with a new key will be 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.		
<b>sec.srtp.mki.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
The master key identifier (MKI) is an optional parameter for the cryptographic parameter in the SDP that uniquely identifies the SRTP stream within an SRTP session. MKI is expressed as a pair of decimal numbers in the form:  mki:mki_length  where mki is the MKI value and mki_length its length in bytes. If 1, a four-byte MKI parameter is sent within the SDP message of the SIP INVITE / 200 OK. If 0, the MKI parameter is not sent.		
<b>sec.srtp.mki.length<sup>1</sup></b>	<b>1 to 4</b>	<b>4</b>
The length of the master key identifier (MKI), in bytes. Microsoft Lync offers 1-byte MKIs.		
<b>sec.srtp.mki.startSessionAtOne</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, use an MKI value of 1 at the start of an SDP session. If set to 0, the MKI value will increment for each new crypto key.		
<b>sec.srtp.offer<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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 system call. If 0, no secure media stream is included in SDP of a SIP invite.		
<b>sec.srtp.offer.HMAC_SHA1_32<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 1, a crypto line with the AES_CM_128_HMAC_SHA1_32 crypto-suite will be included in offered SDP. If 0, the crypto line is not included.		
<b>sec.srtp.offer.HMAC_SHA1_80<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 1, a crypto line with the AES_CM_128_HMAC_SHA1_80 crypto-suite will be included in offered SDP. If 0, the crypto line is not included.		
<b>sec.srtp.padRtpToFourByteAlignment<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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.		
<b>sec.srtp.require<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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 will be 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 will also be set to 1, regardless of the value in the configuration file.		

<i>Parameter</i>	<i>Permitted values</i>	<i>Defaults</i>
<b>sec.srtp.requireMatchingTag<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the tag values in the crypto parameter in an SDP answer are ignored. If 1, the tag values must match.		
<b>sec.srtp.sessionParams.noAuth.offer<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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.		
<b>sec.srtp.sessionParams.noAuth.require<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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 will also be set to 1, regardless of the value in the configuration file.		
<b>sec.srtp.sessionParams.noEncryptRTCP.offer<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, encryption of RTCP is offered. If 1, no encryption of RTCP is offered; a session description that includes the UNENCRYPTED_SRTP session parameter is sent when initiating a call.		
<b>sec.srtp.sessionParams.noEncryptRTCP.require<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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_SRTP session parameter in its SDP. If this parameter is set to 1, sec.srtp.sessionParams.noEncryptRTCP.offer will also be set to 1, regardless of the value in the configuration file.		
<b>sec.srtp.sessionParams.noEncryptRTP.offer<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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.		
<b>sec.srtp.sessionParams.noEncryptRTP.require<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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 will also be set to 1, regardless of the value in the configuration file.		
<b>sec.srtp.simplifiedBestEffort</b>	<b>0 or 1</b>	<b>0</b>
If 0, no SRTP is supported. If 1, negotiation of SRTP compliant with Microsoft Session Description Protocol Version 2.0 Extensions is supported.		

<sup>1</sup> Change causes system to restart or reboot.

## <dot1x><eapollogoff/>

The following table lists configurable parameters.

### 802.1X EAP over LAN (EAPOL) Logoff Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>sec.dot1x.eapollogoff.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the system will not send an EAPOL Logoff message on behalf of the disconnected supplicant. If 1, the feature is enabled and the system will send an EAPOL Logoff message on behalf of the disconnected supplicant connected to the system's secondary (PC) port.		
<b>sec.dot1x.eapollogoff.lanlinkreset<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the system software will not reset (recycle) the LAN port link in the application initiation stage. If 1, the LAN port link will be reset in the application initiation stage.		

<sup>1</sup> Change causes system to restart or reboot.

## <hostmovedetect/>

The following table lists configurable parameters.

### Host Movement Detection Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>sec.hostmovedetect.cdp.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the system software will unconditionally send a CDP packet (to the authenticator switch port) to indicate a host has been connected or disconnected to its secondary (PC) port.		
<b>sec.hostmovedetect.cdp.sleepTime<sup>1</sup></b>	<b>0 to 60000</b>	<b>1000</b>
If <code>sec.hostmovedetect.cdp.enabled</code> is set to 1, then there will be an x microsecond time interval between two consecutive link-up state change reports. This will reduce the frequency of dispatching CDP packets.		

<sup>1</sup> Change causes system to restart or reboot.

## <TLS/>

The following table lists configurable TLS parameters. For the list of configurable ciphers, see [Configurable TLS Cipher Suites](#).

This parameter also includes [<profile/>](#) and [<profileSelection/>](#).

**TLS Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>sec.TLS.browser.cipherList</b>	<b>String</b>	<b>NoCipher</b>
The cipher list for browser. The format for the cipher list uses openssl syntax found here: <a href="#">OpenSSL Ciphers</a> .		
<b>sec.TLS.cipherList</b>	<b>String</b>	<b>“RSA:!EXP:!LOW:!NULL:!MD5:@STRENGTH”</b>
The global cipher list parameter. The format for the cipher list uses openssl syntax found here: <a href="#">OpenSSL Ciphers</a> .		
<b>sec.TLS.customCaCert.x</b>	<b>String</b>	<b>Null</b>
The custom certificate for TLS Application Profile x (x= 1 to 6).		
<b>sec.TLS.customDeviceCert.x</b>	<b>String</b>	<b>Null</b>
The custom device certificate for TLS Application Profile x (x= 1 to 6).		
<b>sec.TLS.customDeviceKey.x</b>	<b>String</b>	<b>Null</b>
The custom device certificate private key for TLS Application Profile x (x= 1 to 6).		
<b>sec.TLS.LDAP.cipherList</b>	<b>String</b>	<b>NoCipher</b>
The cipher list for the corporate directory. The format for the cipher list uses openssl syntax found here: <a href="#">OpenSSL Ciphers</a> .		
<b>sec.TLS.prov.cipherList</b>	<b>String</b>	<b>NoCipher</b>
The cipher list for provisioning. The format for the cipher list uses openssl syntax found here: <a href="#">OpenSSL Ciphers</a> .		
<b>sec.TLS.SIP.cipherList</b>	<b>String</b>	<b>NoCipher</b>
The cipher list for SIP. The format for the cipher list uses openssl syntax found here: <a href="#">OpenSSL Ciphers</a> .		
<b>sec.TLS.SIP.strictCertCommonNameValidation</b>	<b>0 or 1</b>	<b>1</b>
If 1, enable common name validation for SIP.		
<b>sec.TLS.syslog.cipherList</b>	<b>String</b>	<b>NoCipher</b>
The cipher list for syslog. The format for the cipher list uses openssl syntax found here: <a href="#">OpenSSL Ciphers</a> .		

## <profile/>

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

### TLS Profile Parameters

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

## <profileSelection/>

You can configure the parameters listed in the following 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

### TLS Profile Selection Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>sec.TLS.profileSelection.browser</b>	<b>a TLS profile</b>	<b>PlatformProfile1</b>
The TLS platform profile or TLS application profile (see preceding list) to use for the browser or microbrowser.		
<b>sec.TLS.profileSelection.LDAP</b>	<b>a TLS profile</b>	<b>PlatformProfile1</b>
The TLS platform profile or TLS application profile (see preceding list) to use for the Corporate Directory.		
<b>sec.TLS.profileSelection.SIP</b>	<b>a TLS profile</b>	<b>PlatformProfile1</b>
The TLS platform profile or TLS application profile (see preceding list) to use for SIP operations.		
<b>sec.TLS.profileSelection.syslog</b>	<b>PlatformProfile1 or PlatformProfile2</b>	<b>PlatformProfile1</b>
The TLS platform profile to use for syslog operations.		

## <softkey/>

The following table lists parameters you can use to customize soft keys on the system interface. Note that `feature.enhancedFeatureKeys.enabled` must be enabled (set to 1) to use the Configurable Soft Key feature.

The configuration parameter is defined as follows (where x=1 to a maximum number of 10 soft keys).

### Soft Key Customization Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>softkey.feature.basicCallManagement.redundant</b>	<b>0 or 1</b>	<b>1</b>
Control the display of the <b>Hold</b> , <b>Transfer</b> , and <b>Conference</b> soft keys. If set to 0 and the system has hard keys mapped for <b>Hold</b> , <b>Transfer</b> , and <b>Conference</b> functions (all must be mapped), none of the soft keys are displayed. If set to 1, all of these soft keys are displayed.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>softkey.feature.buddies</b>	<b>0 or 1</b>	<b>1</b>
If 0, the <b>Buddies</b> soft key is not displayed. If 1, the soft key is displayed (if <code>pres.idleSoftKeys</code> is set to 1).		
<b>softkey.feature.callers</b>	<b>0 or 1</b>	<b>0</b>
If 1, the <b>Callers</b> soft key displays on all platforms. If 0, the <b>Callers</b> soft key is disabled for all platforms. The default value is 0.		
<b>softkey.feature.directories</b>	<b>0 or 1</b>	<b>0</b>
If 1, the <b>Directory</b> soft key displays on all platforms. If 0, the <b>Directory</b> soft key is disabled for all platforms. The default value is 0.		
<b>softkey.feature.endcall</b>	<b>0 or 1</b>	<b>1</b>
If 0, the <b>End Call</b> soft key is not displayed. If 1, the soft key is displayed.		
<b>softkey.feature.forward</b>	<b>0 or 1</b>	<b>1</b>
If 0, the <b>Forward</b> soft key is not displayed. If 1, the soft key is displayed.		
<b>softkey.feature.join</b>	<b>0 or 1</b>	<b>1</b>
Join two individual calls to form a conference. If 0, the <b>Join</b> soft key is not displayed. If 1, the soft key is displayed.		
<b>softkey.feature.mystatus</b>	<b>0 or 1</b>	<b>1</b>
If 0, the <b>MyStatus</b> soft key is not displayed. If 1, the soft key is displayed (if <code>pres.idleSoftKeys</code> is set to 1).		
<b>softkey.feature.newcall</b>	<b>0 or 1</b>	<b>1</b>
If 0, the <b>New Call</b> soft key is not displayed when there is an alternative way to place a call. If 1, the <b>New Call</b> soft key is displayed.		
<b>softkey.feature.simplifiedSignIn</b>	<b>0 or 1</b>	<b>0</b>
If 0, the <b>SignIn</b> soft key is not displayed. If 1 and <code>voIpProt.server.x.specialInterop</code> is <code>lync2010</code> , the <b>SignIn</b> soft key is displayed.		
<b>softkey.feature.split</b>	<b>0 or 1</b>	<b>1</b>
Split up a conference into individual calls. If 0, the <b>Split</b> soft key is not displayed. If 1, the soft key is displayed.		
<b>softkey.x.action</b>	<b>macro action string, 256 characters</b>	<b>Null</b>
The action or function for custom soft key x. This value uses the same macro action string syntax as an Enhanced Feature Key. For a list of actions, see Understanding Macro Definitions.		
<b>softkey.x.enable</b>	<b>0 or 1</b>	<b>0</b>
If 0, the soft key x is disabled. If 1, the soft key is enabled.		



<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>softkey.x.insert</b>	<b>0 to 10</b>	<b>0</b>
<p>The position on the system screen for soft key x. For example, if the value is 3, the soft key will be displayed on the screen in the third position from the left. Note: If <code>softkey.x.precede</code> is configured, this value is ignored. If the insert location is greater than the number of soft keys, the key will be positioned last, after the other soft keys.</p>		
<b>softkey.x.label</b>	<b>string</b>	<b>Null</b>
<p>The text displayed on the soft key label. If Null, the label is determined as follows:            If the soft key performs an Enhanced Feature Key macro action, the label of the macro will be used.            If the soft key calls a speed dial, the label of the speed dial contact will be used.            If the soft key performs chained actions, the label of the first action is used.            If the soft key label is Null and none of the preceding criteria are matched, the label will be blank.</p>		
<b>softkey.x.precede</b>	<b>0 or 1</b>	<b>0</b>
<p>If 0, soft key x is positioned in the first empty space from the left. If 1, the soft key is displayed before (to the left of) the first default soft key.</p>		
<b>softkey.x.use.active</b> Display in the active call state	<b>0 or 1</b>	<b>0</b>
<b>softkey.x.use.alerting</b> Display in the alerting state	<b>0 or 1</b>	<b>0</b>
<b>softkey.x.use.dialtone</b> Display in the dial tone state	<b>0 or 1</b>	<b>0</b>
<b>softkey.x.use.hold</b> Display in the hold state	<b>0 or 1</b>	<b>0</b>
<b>softkey.x.use.idle</b> Display in the idle state	<b>0 or 1</b>	<b>0</b>
<b>softkey.x.use.proceeding</b> Display in the proceeding state	<b>0 or 1</b>	<b>0</b>
<b>softkey.x.use.setup</b> Display in the proceeding state	<b>0 or 1</b>	<b>0</b>
<p>If 0, the soft key is not displayed when the system is in the call state. If 1, the soft key is displayed when the system is in the call state.</p>		

## <tcplpApp/>

This parameter includes:

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

- [<fileTransfer/>](#)

## <dhcp/>

The DHCP parameters listed in the following table enable you to change how the system reacts to DHCP changes.

### DHCP Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>tcplpApp.dhcp.releaseOnLinkRecovery</b>	<b>0 or 1</b>	<b>1</b>

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

### Domain Name System (DNS) Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>tcplpApp.dns.address.overrideDHCP<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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 tcplpApp.dns.server and tcplpApp.dns.altServer.		
<b>tcplpApp.dns.server<sup>1</sup></b>	<b>Dotted-decimal IP address</b>	<b>Null</b>
The primary server to which the system directs DNS queries.		
<b>tcplpApp.dns.altServer<sup>1</sup></b>	<b>Dotted-decimal IP address</b>	<b>Null</b>
The secondary server to which the system directs DNS queries.		
<b>tcplpApp.dns.domain<sup>1</sup></b>	<b>String</b>	<b>Null</b>
The system's DNS domain.		
<b>tcplpApp.dns.domain.overrideDHCP<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
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 tcplpApp.dns.domain.		

<sup>1</sup> Change causes system to restart or reboot.

## <ice/>

The <ice/> parameters in the following table enable you to set the STUN/TURN/ICE feature.

### Ice Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>tcplpApp.ice.mode</b>	<b>Disabled, Standard, MSOCS</b>	<b>Disabled</b>
Turn SIP ICE negotiation on or off. If using Lync Server 2010, set to MSOCS to enable ICE.		
<b>tcplpApp.ice.password</b>	<b>String</b>	<b>Null</b>
Enter the password to authenticate to the TURN server.		
<b>tcplpApp.ice.stun.server</b>	<b>String</b>	<b>Null</b>
Enter the IP address of the STUN server.		
<b>tcplpApp.ice.stun.udpPort</b>	<b>1-65535</b>	<b>3478</b>
The UDP port number of the STUN server.		
<b>tcplpApp.ice.tcp.enabled</b>	<b>0 or 1</b>	<b>1</b>
If 0, TCP is disabled. If 1, TCP is enabled.		
<b>tcplpApp.ice.turn.callAdmissionControl.enabled</b>		<b>1</b>
<b>tcplpApp.ice.turn.server</b>	<b>String</b>	<b>Null</b>
Enter the IP address of the TURN server.		
<b>tcplpApp.ice.turn.tcpPort</b>	<b>1-65535</b>	<b>443</b>
The UDP port number of the TURN server.		
<b>tcplpApp.ice.turn.udpPort</b>	<b>1-65535</b>	<b>443</b>
The UDP port number of the TURN server.		
<b>tcplpApp.ice.username</b>	<b>String</b>	<b>Null</b>
Enter the user name to authenticate to the TURN server.		

## <sntp/>

The following table lists the Simple Network Time Protocol (SNTP) parameters used to set up time synchronization and daylight savings time. The default values will enable and configure daylight 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

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>tcplpApp.sntp.address</b>	<b>Valid hostname or IP address</b>	<b>Null</b>
The address of the SNTP server.		
<b>tcplpApp.sntp.AQuery</b>	<b>0 or 1</b>	<b>0</b>
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.		
<b>tcplpApp.sntp.address.overrideDHCP</b>	<b>0 or 1</b>	<b>0</b>
If 0, the DHCP values for the SNTP server address will be used. If 1, the SNTP parameters will override the DHCP values.		
<b>tcplpApp.sntp.daylightSavings.enable</b>	<b>0 or 1</b>	<b>1</b>
If 0, daylight savings time rules are not applied to the displayed time. If 1, the daylight savings rules apply.		
<b>tcplpApp.sntp.daylightSavings.fixedDayEnable</b>	<b>0 or 1</b>	<b>0</b>
If 0, <code>month</code> , <code>date</code> , and <code>dayOfWeek</code> are used in the DST calculation. If 1, only <code>month</code> and <code>date</code> are used.		
<b>tcplpApp.sntp.daylightSavings.start.date</b>	<b>1 to 31</b>	<b>8</b>
The start date for daylight savings time. If <code>fixedDayEnable</code> is set to 1, the value of this parameter is the day of the month to start DST. If <code>fixedDayEnable</code> is set to 0, this value specifies the occurrence of <code>dayOfWeek</code> when DST should start. Set 1 for the first occurrence in the month, set 8 for the second occurrence, 15 for the third occurrence, or 22 for the fourth occurrence. For example, if set to 15, DST starts on the third <code>dayOfWeek</code> of the month.		
<b>tcplpApp.sntp.daylightSavings.start.dayOfWeek</b>	<b>1 to 7</b>	<b>1</b>
The day of the week to start DST. 1=Sunday, 2=Monday, ... 7=Saturday. Note: this parameter is not used if <code>fixedDayEnable</code> is set to 1.		
<b>tcplpApp.sntp.daylightSavings.start.dayOfWeek.lastInMonth</b>	<b>0 or 1</b>	<b>0</b>
If 1, DST starts on the last <code>dayOfWeek</code> of the month and the <code>start.date</code> is ignored). Note: this parameter is not used if <code>fixedDayEnable</code> is set to 1.		
<b>tcplpApp.sntp.daylightSavings.start.month</b>	<b>1 to 12</b>	<b>3 (March)</b>
The month to start DST. 1=January, 2=February... 12=December.		
<b>tcplpApp.sntp.daylightSavings.start.time</b>	<b>0 to 23</b>	<b>2</b>
The time of day to start DST – in 24 hour clock format. 0= 12am, 1= 1am,... 12= 12pm, 13= 1pm, ... 23= 11pm.		
<b>tcplpApp.sntp.daylightSavings.stop.date</b>	<b>1 to 31</b>	<b>1</b>
The stop date for daylight savings time. If <code>fixedDayEnable</code> is set to 1, the value of this parameter is the day of the month to stop DST. If <code>fixedDayEnable</code> is set to 0, this value specifies the occurrence of <code>dayOfWeek</code> when DST should stop. Set 1 for the first occurrence in the month, set 8 for the second occurrence, 15 for the third occurrence, or 22 for the fourth occurrence. For example, if set to 22, DST stops on the fourth <code>dayOfWeek</code> of the month.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>tcplpApp.snpt.daylightSavings.stop.dayOfWeek</b>	<b>1 to 7</b>	<b>1</b>
The day of the week to stop DST. 1=Sunday, 2=Monday, ... 7=Saturday. Note: this parameter is not used if <code>fixedDayEnable</code> is set to 1.		
<b>tcplpApp.snpt.daylightSavings.stop.dayOfWeek.lastInMonth</b>	<b>0 or 1</b>	<b>0</b>
If 1, DST stops on the last <code>dayOfWeek</code> of the month and the <code>stop.date</code> is ignored). Note: this parameter is not used if <code>fixedDayEnable</code> is set to 1.		
<b>tcplpApp.snpt.daylightSavings.stop.month</b>	<b>1 to 12</b>	<b>11</b>
The month to stop DST. 1=January, 2=February... 12=December.		
<b>tcplpApp.snpt.daylightSavings.stop.time</b>	<b>0 to 23</b>	<b>2</b>
The time of day to stop DST – in 24 hour clock format. 0= 12am, 1= 1am,... 12= 12pm, 13= 1pm, ... 23= 11pm.		
<b>tcplpApp.snpt.gmtOffset</b>	<b>positive or negative integer</b>	<b>0</b>
The offset in seconds of the local time zone from GMT.3600 seconds = 1 hour, -3600 seconds = -1 hour.		
<b>tcplpApp.snpt.gmtOffset.overrideDHCP</b>	<b>0 or 1</b>	<b>0</b>
If 0, the DHCP values for the GMT offset will be used. If 1, the SNTP values for the GMT offset will be used.		
<b>tcplpApp.snpt.resyncPeriod</b>	<b>positive integer</b>	<b>86400</b>
The period of time (in seconds) that passes before the system resynchronizes with the SNTP server. Note: 86400 seconds is 24 hours.		

## <port/><rtp/>

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

### RTP Port Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>tcplpApp.port.rtp.filterByPort<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
Ports can be negotiated through the SDP protocol. If set to 1, the system will reject RTP packets arriving from (sent from) a non-negotiated port.		
<b>tcplpApp.port.rtp.forceSend<sup>1</sup></b>	<b>0 to 65535</b>	<b>0</b>
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 <code>tcpIpApp.port.rtp.filterByIp</code> and <code>tcpIpApp.port.rtp.filterByPort</code> must be set to 1 for this to work.		
<b>tcplpApp.port.rtp.mediaPortRangeStart<sup>1</sup></b>	<b>even integer 1024 to 65440</b>	<b>2222</b>
The starting port for RTP packets. Ports will be 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).		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
------------------	-------------------------	----------------

<sup>1</sup> Change causes system to restart or reboot.

## <keepalive/>

The parameters listed in the following 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

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
------------------	-------------------------	----------------

<b>tcplpApp.keepalive.tcp.idleTransmitInterval</b>	<b>10 to 7200</b>	<b>30</b>
--	-------------------	-----------

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.

<b>tcplpApp.keepalive.tcp.noResponseTransmitInterval</b>	<b>5 to 120</b>	<b>20</b>
--	-----------------	-----------

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).

<b>tcplpApp.keepalive.tcp.sip.tls.enable</b>	<b>0 or 1</b>	<b>0</b>
--	---------------	----------

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.

<b>tcplpApp.keepalive.tcp.sip.persistentConnection.enable1</b>	<b>0 or 1</b>	<b>0</b>
--	---------------	----------

If 0, the TCP socket opens a new connection when the system tries to send any new SIP message and closes after one minute. If 1, the TCP socket connection remains open indefinitely.

<sup>1</sup> Change causes system to restart or reboot.

## <fileTransfer/>

The parameters listed in the following table provide information on file transfers from the system to the Provisioning server.

### File Transfer Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
------------------	-------------------------	----------------

<b>tcplpApp.fileTransfer.waitForLinkIfDown</b>	<b>0 or 1</b>	<b>1</b>
--	---------------	----------

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.

## <tones/>

This parameter describes configuration items for the tone resources available in the system. It includes:

- <DTMF/>
- <chord/>

## <DTMF/>

The parameters listed in the following table enable you to configure Dual-tone multi-frequency (DTMF) tone signaling.

### DTMF Tone Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>tone.dtmf.chassis.masking<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, DTMF tones will be played through the speakersystem in handsfree mode. If 1 (set only if <code>tone.dtmf.viaRtp</code> is set to 0), DTMF tones will be substituted with non-DTMF pacifier tones when dialing in handsfree mode—this is to prevent the tones from broadcasting to surrounding telephony devices or being inadvertently transmitted in-band due to local acoustic echo.		
<b>tone.dtmf.level<sup>1</sup></b>	<b>-33 to 3</b>	<b>-15</b>
The level of the high frequency component of the DTMF digit measured in dBm0; the low frequency tone will be two dB lower.		
<b>tone.dtmf.offTime<sup>1</sup></b>	<b>positive integer</b>	<b>50</b>
When a sequence of DTMF tones is played out automatically, this is the length of time in milliseconds the system will pause between digits. This is also the minimum inter-digit time when dialing manually.		
<b>tone.dtmf.onTime<sup>1</sup></b>	<b>positive integer</b>	<b>50</b>
When a sequence of DTMF tones is played out automatically, this is the length of time in milliseconds the tones will be played for. This is also the minimum time the tone will be played when dialing manually (even if key press is shorter).		
<b>tone.dtmf.rfc2833Control<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, the system will indicate a preference for encoding DTMF through RFC 2833 format in its Session Description Protocol (SDP) offers by showing support for the system-event payload type. This does not affect SDP answers; these will always honor the DTMF format present in the offer since the system has native support for RFC 2833.		
<b>tone.dtmf.rfc2833Payload<sup>1</sup></b>	<b>96 to 127</b>	<b>127</b>
The system-event payload encoding in the dynamic range to be used in SDP offers.		
<b>tone.dtmf.viaRtp<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, encode DTMF in the active RTP stream. Otherwise, DTMF may be encoded within the signaling protocol only when the protocol offers the option. Note: If this parameter is set to 0, <code>tone.dtmf.chassis.masking</code> should be set to 1.		

<sup>1</sup> Change causes system to restart or reboot.

## <chord/>

Chord-sets are the building blocks of sound effects that used synthesized audio rather than sampled audio. Most call progress and ringer sound effects are synthesized. A chord-set is a multi-frequency note with an optional on/off cadence. A chord-set can contain up to four frequency components generated simultaneously, each with its own level. Chord parameters are listed in the following table.

There are three chord sets: callProg, misc, and ringer. Each chord set has different chord names, represented by x in the following table. The chord names are as follows:

For **callProg**, x can be one of the following chords:

- **dialTone, busyTone, ringback, reorder, stutter\_3, callWaiting, callWaitingLong, howler, recWarning, stutterLong, intercom, callWaitingLong, precedenceCallWaiting, preemption, precedenceRingback, or spare1 to spare6.**

For **misc**, x can be one of the following chords

- **spare1 to spare9.**

For **ringer**, x can be one of the following chords:

- **ringback, originalLow, originalHigh, or spare1 to spare19.**

### Chord Parameters

<i>Parameter</i>	<i>Permitted Values</i>
<b>tone.chord.callProg.x.freq.y</b>	<b>0-1600</b>
<b>tone.chord.misc.x.freq.y</b>	<b>0-1600</b>
<b>tone.chord.ringer.x.freq.y</b>	<b>0-1600</b>
The frequency (in Hertz) for component y. Up to six chord-set components can be specified (y=1 to 6).	
<b>tone.chord.callProg.x.level.y</b>	<b>-57 to 3</b>
<b>tone.chord.misc.x.level.y</b>	<b>-57 to 3</b>
<b>tone.chord.ringer.x.level.y</b>	<b>-57 to 3</b>
The level of component y in dBm0. Up to six chord-set components can be specified (y=1 to 6).	
<b>tone.chord.callProg.x.onDur</b>	<b>positive integer</b>
<b>tone.chord.misc.x.onDur</b>	<b>positive integer</b>
<b>tone.chord.ringer.x.onDur</b>	<b>positive integer</b>
The on duration (length of time to play each component) in milliseconds, 0=infinite.	
<b>tone.chord.callProg.x.offDur</b>	<b>positive integer</b>
<b>tone.chord.misc.x.offDur</b>	<b>positive integer</b>
<b>tone.chord.ringer.x.offDur</b>	<b>positive integer</b>
The off duration (the length of silence between each chord component) in milliseconds, 0=infinite.	
<b>tone.chord.callProg.x.repeat</b>	<b>positive integer</b>
<b>tone.chord.misc.x.repeat</b>	<b>positive integer</b>
<b>tone.chord.ringer.x.repeat</b>	<b>positive integer</b>
The number of times each ON/OFF cadence is repeated, 0=infinite.	



**<up/>**

Use the parameters listed in the following table to set user preferences on the systems.

**User Preferences Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>up.25mm</b>	<b>1 or 2</b>	<b>1</b>
Specify whether to use a mobile system or a PC to connect to the 2.5mm audio port on a conference system. Set to 1 if using a mobile system. Set to 2 if using a PC.		
<b>up.analogHeadsetOption</b>	<b>0, 1, 2, 3</b>	<b>0</b>
The Electronic Hookswitch mode for the system's analog headset jack. 0 - no EHS-compatible headset is attached. 1 - a Jabra EHS-compatible headset is attached. 2 - a Plantronics EHS-compatible headset is attached. 3 - a Sennheiser EHS-compatible headset is attached.		
<b>up.audioMode</b>	<b>0 or 1</b>	<b>0</b>
If 0, a handset is connected. If 1, a headset is connected.		
<b>up.backlight.idleIntensity</b>	<b>0, 1, 2, or 3</b>	<b>1</b>
The brightness of the LCD backlight when the system is idle. 0 – off, 1 – low, 2 – medium, 3 – high. Note: If this is higher than the active backlight brightness ( <i>onIntensity</i> ), the active backlight brightness is used.		
<b>up.backlight.onIntensity</b>	<b>0, 1, 2, or 3</b>	<b>3</b>
The brightness of the LCD backlight when the system is active (in use). 0: off, 1 – low, 2 – medium, 3 – high		
<b>up.backlight.timeout</b>	<b>5 to 60</b>	<b>40</b>
The number of seconds to wait before the backlight dims from the active intensity to the idle intensity.		
<b>up.cfgWarningsEnabled</b>	<b>0 or 1</b>	<b>0</b>
If 1, a warning is displayed on the system if the system is configured with pre-UC software 3.3.0 parameters. If 0, the warning will not display.		
<b>up.handsfreeMode</b>	<b>0 or 1</b>	<b>1</b>
If 0, the handsfree speakersystem is disabled (cannot be used). If 1, the handsfree speakersystem is enabled.		
<b>up.headsetAlwaysUseIntrinsicRinger</b>	<b>0 or 1</b>	<b>1</b>
If 1, the USB headset will use the intrinsic ringer mixed with DSP ringer when the sound effect destination is the USB headset.		
<b>up.headsetMode</b>	<b>0 or 1</b>	<b>0</b>
If 0, handsfree mode will be used by default instead of the handset. If 1, the headset will be used as the preferred audio mode after the headset key is pressed for the first time, until the headset key is pressed again.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>up.headset.systemVolumeControl<sup>1</sup></b>	<b>disable, enable, auto</b>	<b>auto</b>
Controls the system's behavior when you adjust volume at the headset.		
<b>enable</b> – The system responds to volume up/down events from the headset by displaying the volume widget in the system's user interface and adjusting the system's internal volume.		
<b>disable</b> – The system ignores volume up/down events from the headset; pressing the headset's volume controls has no effect on the system.		
<b>auto</b> – The system automatically selects which of the above two behaviors to apply based on the type and model of headset that you attach.		
<b>up.hearingAidCompatibility.enabled</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the system audio Rx (receive) equalization is disabled for hearing aid compatibility. If 0, audio Rx equalization is enabled.		
<b>up.idleBrowser.enabled</b>	<b>0 or 1</b>	<b>0</b>
If 0, the idle browser is disabled. If 1, the idle browser is enabled (if <code>up.prioritizeBackground.enable</code> is 1, the user can choose to display the background or the idle browser through the system menu).		
<b>up.idleStateView<sup>1</sup></b>	<b>0, 1, or 2</b>	<b>0</b>
Sets the default view when the system is idle and not in use.		
<b>0</b> = Lines screen		
<b>1</b> = Home screen		
<b>2</b> = Dialpad screen		
<b>up.idleTimeout<sup>1</sup></b>	<b>0 to 65535, seconds</b>	<b>40</b>
The number of seconds that the system can be idle for before automatically leaving a menu and showing the idle display. If 0, there is no timeout and the system does not automatically exit to the idle display.		
<b>up.IdleViewPreferenceRemoteCalls1</b>	<b>0 or 1</b>	<b>0</b>
Use this parameter to determine when the system displays the idle browser.		
When set to 1, a system with only remote calls active, is treated as in the active state and the idle browser does not display.		
When set to 0, a system with only remote calls active, is treated as in the idle state and the idle browser displays.		
<b>up.lineKeyCallTerminate</b>	<b>0 or 1</b>	<b>0</b>
If 1, the user can press a line key to end an active call on that line. If 0, the user cannot end a call by pressing the line key (this is the previous behavior).		
<b>up.localClockEnabled</b>	<b>0 or 1</b>	<b>1</b>
If 0, the date and time are not shown on the idle display. If 1, the date and time and shown on the idle display.		
<b>up.mwiVisible<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set is 0, the incoming MWI notifications for lines where the MWI callback mode is disabled ( <code>msg.mwi.x.callBackMode</code> is set to 0) are ignored, and do not appear in the message retrieval menus.		
If set to 1, the MWI for lines whose MWI is disabled will display (pre-SIP 2.1 behavior), even though MWI notifications have been received for those lines.		
<b>up.numberFirstCID<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the caller ID display will show the caller's name first. If 1, the caller's system number will be shown first.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>up.numOfDisplayColumns</b>	<b>1, 2, 3, 4</b>	<b>max 4</b>
Set the maximum number of columns the CX5500 system displays. Note that systems display one column when the value is set to 0. The maximum number of columns for the CX5500 system is 4.		
<b>up.offHookAction.none<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the behavior will be as it was in SIP 2.1.2. If 1, when the user lifts the handset, the system will not seize the line and the ringer will continue until the user takes further action.		
<b>up.oneTouchVoiceMail<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the voicemail summary display is bypassed and voicemail is dialed directly (if configured).		
<b>up.screenCapture.enabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, screen captures are disabled. If 1, the user can enable screen captures from the Screen Capture menu on the system. Note: when the system reboots, screen captures are disabled from the Screen Capture menu on the system.		
<b>up.screenSaver.enabled</b>	<b>0 or 1</b>	<b>0</b>
. If 0, the screen saver feature is disabled. If 1, the screen saver feature is enabled. If a USB flash drive containing images is connected to the system, and the idle browser is not configured, a slide show will cycle through the images from the USB flash drive when the screen saver feature is enabled. The images must be stored in the directory on the flash drive specified by <code>up.pictureFrame.folder</code> . The screen saver displays when the system has been in the idle state for the amount of time specified by <code>up.screenSaver.waitTime</code> .		
<b>up.screenSaver.type</b>	<b>0, 1, 2</b>	<b>0</b>
The type of screen saver. If 0, the screen saver feature is disabled. If 1, a blank screen is used, If 2, the idle browser is used as the screen saver.		
<b>up.screenSaver.waitTime</b>	<b>1 to 9999, minutes</b>	<b>15</b>
. The number of minutes that the system waits in the idle state before the screen saver starts.		
<b>up.simplifiedSipCallInfo</b>	<b>0 or 1</b>	<b>0</b>
If 1, the displayed host name is trimmed for both incoming and outgoing calls and the protocol tag/information is not displayed for incoming and outgoing calls.		
<b>up.useDirectoryNames<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, names provided through network signaling are used for caller ID. If 1, the name field in the local contact directory will be used as the caller ID for incoming calls from contacts in the local directory. Note: Outgoing calls and corporate directory entries are not matched.		
<b>up.warningLevel<sup>1</sup></b>	<b>0 to 2</b>	<b>0</b>
If 0, the system's warning icon and a pop-up message display on the system for all warnings. If 1, the warning icon and pop-up messages are only shown for critical warnings. Note: All warnings are listed in the Warnings menu (navigate to <b>Settings &gt; Status &gt; Diagnostics &gt; Warnings</b> on the system).		
<b>up.welcomeSoundEnabled<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the welcome sound is disabled. If 1, the welcome sound is enabled and played each time the system reboots.		
<b>up.welcomeSoundOnWarmBootEnabled<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the welcome sound is played when the system powers up (cold boot), but not after it restarts or reboots (warm boot). If 1, the welcome sound plays each time the system powers up, reboots, or restarts.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
------------------	-------------------------	----------------

<sup>1</sup> Change causes system to restart or reboot.

## <upgrade/>

Use the parameters listed in the following 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

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>upgrade.custom.server.url</b>	<b>URL</b>	<b>Null</b>
The URL of a custom download server.		
<b>upgrade.plcm.server.url</b>	<b>URL</b>	<a href="http://downloads.polycom.com/voice/software/">http://downloads.polycom.com/voice/software/</a>
The URL of the Polycom UC Software download server.		

## <video/>

The parameters in the following table includes video parameters that are supported on the CX5500 system.

This parameter also includes:

- [<camera/>](#)
- [<codecs/>](#)

### General Video Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>video.autoFullScreen</b>	<b>0 or 1</b>	<b>0</b>
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)		
<b>video.autoStartVideoTx</b>	<b>0 or 1</b>	<b>1</b>
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 <b>Video &gt; Start Video</b> soft keys. This parameter controls video sent to the far side. Video from the far side will always be displayed if it is available, and far side users can control when to send video.		
<b>video.callMode.default</b>	<b>audio or video</b>	<b>audio</b>
Allows the user to select the mode to use when using SIP protocol only.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>video.callRate</b>	<b>128 to 2048</b>	<b>512</b>
The default call rate (in kbps) to use when initially negotiating bandwidth for a video call.		
<b>video.dynamicControlMethod</b>	<b>0 or 1</b>	<b>1</b>
If 1, the first I-Frame request uses the method defined by <code>video.forceRtcpVideoCodecControl</code> and subsequent requests alternate between RTCP-FB and SIP INFO. In case of network device problems, you can set the system to attempt multiple methods of I-frame requests. To set other methods for I-frame requests, refer to the parameter <code>video.forceRtcpVideoCodecControl</code> .		
<b>video.enable</b>	<b>0=Disable, 1=Enable</b>	<b>1</b>
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.		
<b>video.iFrame.delay<sup>1</sup></b>	<b>0 to 10, seconds</b>	<b>0</b>
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. Use a value of 2 seconds if you are using this parameter in a Microsoft Lync environment.		
<b>video.iFrame.minPeriod</b>	<b>1 - 60</b>	<b>2</b>
After sending an I-frame, the system will always wait at least this amount of time before sending another I-frame in response to requests from the far end.		
<b>video.iFrame.onPacketLoss</b>	<b>0 or 1</b>	<b>0</b>
If 1, an I-frame is transmitted to the far end when a received RTCP report indicates that video RTP packet loss has occurred.		
<b>video.maxCallRate<sup>1</sup></b>	<b>128 to 2048 kbps</b>	<b>768</b>
The maximum call rate allowed. This allows the administrator to limit the maximum call rate that the users can select. If <code>video.callRate</code> exceeds this value, this value will be used as the maximum.		
<b>video.quality<sup>1</sup></b>	<b>motion, sharpness</b>	<b>Null</b>
The optimal quality for video that you send in a call or a conference. Use <code>motion</code> if your outgoing video will have motion or movement. Use <code>sharpness</code> or <code>Null</code> if your outgoing video will have little or no movement. Note: If <code>motion</code> is not selected, moderate to heavy motion can cause some frames to be dropped.		
<b>video.screenMode</b>	<b>normal, full, crop</b>	<b>normal</b>
The screen mode for the video window shown in non-full screen mode. If set to <code>normal</code> or <code>Null</code> , the entire view is displayed and horizontal or vertical black bars may appear on the edges to maintain the correct aspect ratio. If set to <code>full</code> , the entire view is stretched linearly and independently to fill the video frame. If set to <code>crop</code> , black bars are not shown, the image is re-sized and enlarged to cover the entire video frame, and parts of the image that do not fit in the display are cropped (removed).		
<b>video.screenModeFS</b>	<b>normal, full, crop</b>	<b>normal</b>
The screen mode for the video window shown in full screen mode. If set to <code>normal</code> or <code>Null</code> , the entire view is displayed and horizontal or vertical black bars may appear on the edges to maintain the correct aspect ratio. If set to <code>full</code> , the entire view is stretched linearly and independently to fill the screen. If set to <code>crop</code> , black bars are not shown, the image is re-sized and enlarged to cover the entire screen, and parts of the image that do not fit in the display are cropped (removed).		

<sup>1</sup> Change causes system to restart or reboot.

## <camera/>

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

### Video Camera Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>video.camera.brightness</b>	<b>0 to 6</b>	<b>3</b>
Set brightness level. The value range is from 0 (Dimmest) to 6 (Brightest).		
<b>video.camera.contrast</b>	<b>0 to 4</b>	<b>0</b>
Set contrast level. The value range is from 0 (No contrast increase) to 3 (Most contrast increase), and 4 (Noise reduction contrast).		
<b>video.camera.flickerAvoidance</b>	<b>0 to 2</b>	<b>0</b>
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).		
<b>video.camera.frameRate</b>	<b>5 to 30</b>	<b>25</b>
Set target frame rate (frames per second). Values indicate a fixed frame rate, from 5 (least smooth) to 30 (most smooth). Note: If <code>video.camera.frameRate</code> is set to a decimal number, the value 25 is used.		
<b>video.camera.saturation</b>	<b>0 to 6</b>	<b>3</b>
Set saturation level. The value range is from 0 (Lowest) to 6 (Highest).		
<b>video.camera.sharpness</b>	<b>0 to 6</b>	<b>3</b>
Set sharpness level. The value range is from 0 (Lowest) to 6 (Highest).		

## <codecs/>

These video codecs include:

- [<profile/>](#)

## <profile/>

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

---

**Video Profile Parameters**

<i>Parameter</i>	<i>Permitted Values</i>
<b>video.profile.H261.annexD<sup>1</sup></b>	<b>0 or 1 (default)</b>
Enable or disable Annex D when negotiating video calls.	
<b>video.profile.H261.CifMpi<sup>1</sup></b>	<b>1 (default) to 32</b>
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'.	
<b>video.profile.H261.jitterBufferMax<sup>1</sup></b>	<b>(video.profile.H261.jitter BufferMin + 500ms) to 2500ms, default 2000ms</b>
The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter.	
<b>video.profile.H261.jitterBufferMin<sup>1</sup></b>	<b>33ms to 1000ms, default 150ms</b>
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 will still continue. 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.	
<b>video.profile.H261.jitterBufferShrink<sup>1</sup></b>	<b>33ms to 1000ms, default 70ms</b>
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).	
<b>video.profile.H261.payloadType<sup>1</sup></b>	<b>0 to 127, default 31</b>
RTP payload format type for H261 MIME type.	
<b>video.profile.H261.QcifMpi<sup>1</sup></b>	<b>1 (default) to 32</b>
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'.	
<b>video.profile.H263.CifMpi<sup>1</sup></b>	<b>1 (default) to 32</b>
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'.	
<b>video.profile.H263.jitterBufferMax<sup>1</sup></b>	<b>(video.profile.H263.jitter BufferMin + 500ms) to 2500ms, default 2000ms</b>
The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter.	
<b>video.profile.H263.jitterBufferMin<sup>1</sup></b>	<b>33ms to 1000ms, default 150ms</b>
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 will still continue. 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.	

---

<i>Parameter</i>	<i>Permitted Values</i>
<b>video.profile.H263.jitterBufferShrink<sup>1</sup></b>	<b>33ms to 1000ms, default 70ms</b>
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).	
<b>video.profile.H263.payloadType<sup>1</sup></b>	<b>0 to 127, default 34</b>
RTP payload format type for H263 MIME type.	
<b>video.profile.H263.QcifMpi<sup>1</sup></b>	<b>1 (default) to 32</b>
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'.	
<b>video.profile.H263.SqcifMpi<sup>1</sup></b>	<b>1 (default) to 32</b>
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'.	
<b>video.profile.H2631998.annexF<sup>1</sup></b>	<b>0 (default) or 1</b>
Enable or disable Annex F when negotiating video calls.	
<b>video.profile.H2631998.annexI<sup>1</sup></b>	<b>0 (default) or 1</b>
Enable or disable Annex I when negotiating video calls.	
<b>video.profile.H2631998.annexJ<sup>1</sup></b>	<b>0 (default) or 1</b>
Enable or disable Annex J when negotiating video calls.	
<b>video.profile.H2631998.annexK<sup>1</sup></b>	<b>0, 1 (default), 2, 3, 4</b>
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'.	
<b>video.profile.H2631998.annexN<sup>1</sup></b>	<b>0, 1 (default), 2, 3, 4</b>
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'.	
<b>video.profile.H2631998.annexT<sup>1</sup></b>	<b>0 (default) or 1</b>
Enable or disable Annex T when negotiating video calls.	
<b>video.profile.H2631998.CifMpi<sup>1</sup></b>	<b>1 (default) to 32</b>
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'.	
<b>video.profile.H2631998.jitterBufferMax<sup>1</sup></b>	<b>(video.profile.H2631998.jitterBufferMin+ 500ms) to 2500ms, default 2000ms</b>
The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter.	



<i>Parameter</i>	<i>Permitted Values</i>
<b>video.profile.H2631998.jitterBufferMin<sup>1</sup></b>	<b>33ms to 1000ms, default 150ms</b>
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 will still continue. 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.	
<b>video.profile.H2631998.jitterBufferShrink<sup>1</sup></b>	<b>33ms to 1000ms, default 70ms</b>
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).	
<b>video.profile.H2631998.payloadType<sup>1</sup></b>	<b>96 (default) to 127</b>
RTP payload format type for H263-1998/90000 MIME type.	
<b>video.profile.H2631998.QcifMpi<sup>1</sup></b>	<b>1 (default) to 32</b>
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'.	
<b>video.profile.H2631998.SqcifMpi<sup>1</sup></b>	<b>1 (default) to 32</b>
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'.	
<b>video.profile.H264.jitterBufferMax<sup>1</sup></b>	<b>(video.profile.H264.jitter BufferMin + 500ms) to 2500ms, default 2000ms</b>
The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter.	
<b>video.profile.H264.jitterBufferMin<sup>1</sup></b>	<b>33ms to 1000ms, default 150ms</b>
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 will still continue. 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.	
<b>video.profile.H264.jitterBufferShrink<sup>1</sup></b>	<b>33ms to 1000ms, default 70ms</b>
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).	
<b>video.profile.H264.payloadType<sup>1</sup></b>	<b>96 to 127, default 109</b>
RTP payload format type for H264/90000 MIME type.	
<b>video.profile.H264.profileLevel<sup>1</sup></b>	<b>1, 1b, 1.1, 1.2, and 1.3 (default)</b>
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. The default level is 1.3. For more information, refer to ITU-T H.264.	

<sup>1</sup> Change causes system to restart or reboot.

## <voice/>

The following parameters listed in the table control audio on the system.

### Voice Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.txPacketDelay<sup>1</sup></b>	<b>low, normal, Null</b>	<b>Null</b>
<p>If set to normal or Null, no audio parameters are changed.</p> <p>If set to low and there are no precedence conflicts, the following changes are made:</p> <ul style="list-style-type: none"> <li>• <code>voice.codecPref.G722="1"</code></li> <li>• <code>voice.codecPref.G711Mu="2"</code></li> <li>• <code>voice.codecPref.G711A="3"</code></li> <li>• <code>voice.codecPref.&lt;OtherCodecs&gt;=""</code></li> <li>• <code>voice.audioProfile.G722.payloadSize="10"</code></li> <li>• <code>voice.audioProfile.G711Mu.payloadSize= "10"</code></li> <li>• <code>voice.audioProfile.G711A.payloadSize= "10"</code></li> <li>• <code>voice.aec.hs.enable="0"</code></li> <li>• <code>voice.ns.hs.enable="0"</code></li> </ul>		
<b>voice.txPacketFilter<sup>1</sup></b>	<b>0 or 1</b>	<b>Null</b>
<p>If 0, no Tx filtering is performed. If 1, narrowband Tx high pass filter is enabled.</p>		

<sup>1</sup> Change causes system to restart or reboot.

This parameter includes:

- [<codecPref/>](#)
- [<volume/>](#)
- [<vad/>](#)
- [<quality monitoring/>](#)
- [<rxQoS/>](#)

## <codecPref/>

As of Polycom UC Software 3.3.0, you can configure a simplified set of codec properties for all system models to improve consistency and reduce workload on the systems. System codec preferences are listed in the following table.

If a particular system does not support a codec, the system will ignore that codec and continue to the codec next in the priority.

For more information on codecs on particular systems and priorities, see [Audio Codecs](#).

**Voice Codec Preferences Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.codecPref.G711_A</b>	<b>0 to 27</b>	<b>7</b>
<b>voice.codecPref.G711_Mu</b>		<b>6</b>
<b>voice.codecPref.G719.32kbps</b>		<b>0</b>
<b>voice.codecPref.G719.48kbps</b>		<b>0</b>
<b>voice.codecPref.G719.64kbps</b>		<b>0</b>
<b>voice.codecPref.G722</b>		<b>4</b>
<b>voice.codecPref.G7221.16kbps</b>		<b>0</b>
<b>voice.codecPref.G7221.24kbps</b>		<b>0</b>
<b>voice.codecPref.G7221.32kbps</b>		<b>5</b>
<b>voice.codecPref.G7221_C.24kbps</b>		<b>0</b>
<b>voice.codecPref.G7221_C.32kbps</b>		<b>0</b>
<b>voice.codecPref.G7221_C.48kbps</b>		<b>2</b>
<b>voice.codecPref.G729_AB</b>		<b>8</b>
<b>voice.codecPref.iLBC.13_33kbps</b>		<b>0</b>
<b>voice.codecPref.iLBC.15_2kbps</b>		<b>0</b>
<b>voice.codecPref.Lin16.8ksps</b>		<b>0</b>
<b>voice.codecPref.Lin16.16ksps</b>		<b>0</b>
<b>voice.codecPref.Lin16.32ksps</b>		<b>0</b>
<b>voice.codecPref.Lin16.44_1ksps</b>		<b>0</b>
<b>voice.codecPref.Lin16.48ksps</b>		<b>0</b>
<b>voice.codecPref.Siren14.24kbps</b>		<b>0</b>
<b>voice.codecPref.Siren14.32kbps</b>		<b>0</b>
<b>voice.codecPref.Siren14.48kbps</b>		<b>3</b>
<b>voice.codecPref.Siren22.32kbps</b>		<b>0</b>
<b>voice.codecPref.Siren22.48kbps</b>		<b>0</b>
<b>voice.codecPref.Siren22.64kbps</b>		<b>0</b>

The priority of the codec. If 0 or Null, the codec is disabled. A value of 1 is the highest priority. If a system does not support a codec, it will treat the setting as if it were 0 and not offer or accept calls with that codec.

## <volume/>

In some countries, regulations state that a system's receiver volume must be reset to a nominal level for each new call. This is the system's default behavior. Using the parameters listed in the following table, you can set the receiver volume to persist across calls each time a user makes changes to the default volume level.

### Volume Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.volume.persist.handset<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the handset receive volume will automatically reset to a nominal level after each call. If 1, the volume for each call will be the same as the previous call. If set to 1, the handset receive volume will persist across calls. If set to 0, the handset receive volume will be reset to nominal at the start of each call.		
<b>voice.volume.persist.headset<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the headset receive volume will automatically rest to a nominal level after each call. If 1, the volume for each call will be the same as the previous call.		
<b>voice.volume.persist.handsfree<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the speakersystem receive volume will automatically rest to a nominal level after each call. If 1, the volume for each call will be the same as the previous call.		
<b>voice.volume.persist.usb.handsfree<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, the USB headset will not be used. If 1, the USB headset will be used in handsfree mode.		
<b>voice.volume.persist.usbHeadset<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, the USB headset will not be used. If 1, the USB headset will be used.		

<sup>1</sup> Change causes system to restart or reboot.

## <vad/>

The following paramters listed in the table control the performance of the voice activity detection (silence suppression) feature.

### Voice Activity Detection (VAD) Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.vad.signalAnnexB<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If 0, there is no change to SDP. If 1, Annex B is used and a new line is added to SDP depending on the setting of <code>voice.vadEnable</code> . If <code>voice.vadEnable</code> is set to 1, add parameter line <code>a=fmtp:18 annexb="yes"</code> below <code>a=rtpmap...</code> parameter line (where '18' could be replaced by another payload). If <code>voice.vadEnable</code> is set to 0, add parameter line <code>a=fmtp:18 annexb="no"</code> below <code>a=rtpmap...</code> parameter line (where '18' could be replaced by another payload).		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.vadEnable<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, voice activity detection (VAD) is disabled. If 1, VAD is enabled.		
<b>voice.vadThresh<sup>1</sup></b>	<b>integer from 0 to 30</b>	<b>15</b>
The threshold for determining what is active voice and what is background noise in dB. Sounds louder than this value will be considered active voice, and sounds quieter than this threshold will be considered background noise. This does not apply to G.729AB codec operation which has its own built-in VAD function.		

<sup>1</sup> Change causes system to restart or reboot.

## <quality monitoring/>

The following table shows the Voice Quality Monitoring parameters.

### Voice Quality Monitoring Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.qualityMonitoring.collector.alert.moslq.threshold.critical<sup>1</sup></b>	<b>0 to 40</b>	<b>0</b>
The threshold value of listening MOS score (MOS-LQ) that causes system to send a critical alert quality report. Configure the desired MOS value multiplied by 10. If 0 or Null, critical alerts are not generated due to MOS-LQ. For example, a configured value of 28 corresponds to the MOS score 2.8.		
<b>voice.qualityMonitoring.collector.alert.moslq.threshold.warning<sup>1</sup></b>	<b>0 to 40</b>	<b>0</b>
Threshold value of listening MOS score (MOS-LQ) that causes system to send a warning alert quality report. Configure the desired MOS value multiplied by 10. If 0 or Null, warning alerts are not generated due to MOS-LQ. For example, a configured value of 35 corresponds to the MOS score 3.5.		
<b>voice.qualityMonitoring.collector.alert.delay.threshold.critical<sup>1</sup></b>	<b>0 to 2000</b>	<b>0</b>
Threshold value of one way delay (in ms) that causes system to send a critical alert quality report. If 0 or Null, critical alerts are not generated due to one-way delay. One-way delay includes both network delay and end system delay.		
<b>voice.qualityMonitoring.collector.alert.delay.threshold.warning<sup>1</sup></b>	<b>0 to 2000</b>	<b>0</b>
Threshold value of one way delay (in ms) that causes system to send a warning alert quality report. If 0 or Null, warning alerts are not generated due to one-way delay. One-way delay includes both network delay and end system delay.		
<b>voice.qualityMonitoring.collector.enable.periodic<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, periodic quality reports are not generated. If 1, periodic quality reports are generated throughout a call.		
<b>voice.qualityMonitoring.collector.enable.session<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, quality reports are not generated at the end of each call. If 1, reports are generated at the end of each call.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.qualityMonitoring.collector.enable.triggeredPeriodic<sup>1</sup></b>	<b>0 to 2</b>	<b>0</b>
If 0, alert states do not cause periodic reports to be generated. If 1, periodic reports are generated if an alert state is critical. If 2, period reports are generated when an alert state is either warning or critical. Note: This parameter is ignored when <code>voice.qualityMonitoring.collector.enable.periodic</code> is 1, since reports are sent throughout the duration of a call.		
<b>voice.qualityMonitoring.collector.period<sup>1</sup></b>	<b>5 to 20</b>	<b>20</b>
The time interval between successive periodic quality reports.		
<b>voice.qualityMonitoring.collector.server.x.address<sup>1</sup></b> <b>The server address</b>	<b>Dotted-decimal IP address or hostname</b>	<b>Null</b>
<b>voice.qualityMonitoring.collector.server.x.port<sup>1</sup></b> <b>The server port.</b>	<b>1 to 65535</b>	<b>5060</b>
The server address and port of a SIP server (report collector) that accepts voice quality reports contained in SIP PUBLISH messages. Set x to 1 as only one report collector is supported at this time.		
<b>voice.qualityMonitoring.rtcpxr.enable<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, RTCP-XR packets are not generated. If 1, the packets are generated.		

<sup>1</sup> Change causes system to restart or reboot.

## <rxQoS/>

The following table lists the jitter buffer parameters for wired network interface voice traffic, wireless network interface voice traffic, and push-to-talk interface voice traffic.

### Voice Jitter Buffer Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.rxQoS.avgJitter<sup>1</sup></b> <b>The typical average jitter.</b>	<b>0 to 80</b>	<b>20</b>
<b>voice.rxQoS.maxJitter<sup>1</sup></b> <b>The maximum expected jitter.</b>	<b>0 to 200</b>	<b>160</b>
The average and maximum jitter in milliseconds for wired network interface voice traffic.		
<code>avgJitter</code> – The wired interface minimum depth will be automatically configured to adaptively handle this level of continuous jitter without packet loss.		
<code>maxJitter</code> – The wired interface jitter buffer maximum depth will be automatically configured to handle this level of intermittent jitter without packet loss.		
Actual jitter above the average but below the maximum may result in delayed audio play out while the jitter buffer adapts, but no packets will be lost. Actual jitter above the maximum value will always result in packet loss. Note that if legacy <code>voice.audioProfile.x.jitterBuffer.*</code> parameters are explicitly specified, they will be used to configure the jitter buffer and these <code>voice.rxQoS</code> parameters will be ignored.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voice.rxQoS.wireless.avgJitter<sup>1</sup></b> <b>The typical average jitter.</b>	<b>0 to 200</b>	<b>70</b>
<b>voice.rxQoS.wireless.maxJitter<sup>1</sup></b> <b>The maximum expected jitter.</b>	<b>20 to 500</b>	<b>300</b>

The average and maximum jitter in milliseconds for wireless network interface voice traffic.

*avgJitter* – The wireless interface minimum depth will be automatically configured to adaptively handle this level of continuous jitter without packet loss.

*maxJitter* – The wireless interface jitter buffer maximum depth will be automatically configured to handle this level of intermittent jitter without packet loss.

Actual jitter above the average but below the maximum may result in delayed audio play out while the jitter buffer adapts, but no packets will be lost. Actual jitter above the maximum value will always result in packet loss.

Note: if legacy *voice.audioProfile.x.jitterBuffer.\** parameters are explicitly specified, they will be used to configure the jitter buffer and these *voice.rxQoS* parameters will be ignored for wireless interfaces.

<b>voice.rxQoS.ptt.avgJitter<sup>1</sup></b> <b>The typical average jitter.</b>	<b>0 to 200</b>	<b>150</b>
<b>voice.rxQoS.ptt.maxJitter<sup>1</sup></b> <b>The maximum expected jitter.</b>	<b>20 to 500</b>	<b>480</b>

The average and maximum jitter in milliseconds for IP multicast voice traffic (wired or wireless).

*avgJitter* – The Paging interface minimum depth will be automatically configured to adaptively handle this level of continuous jitter without packet loss.

*maxJitter* – The Paging interface jitter buffer maximum depth will be automatically configured to handle this level of intermittent jitter without packet loss.

Actual jitter above the average but below the maximum may result in delayed audio play out while the jitter buffer adapts, but no packets will be lost. Actual jitter above the maximum value will always result in packet loss.

Note: if legacy *voice.audioProfile.x.jitterBuffer.\** parameters are explicitly specified, they will be used to configure the jitter buffer and these *voice.rxQoS* parameters will be ignored for Paging interface interfaces.

<sup>1</sup> Change causes system to restart or reboot.

## <volpProt/>

You must set up the call server and DTMF signaling parameters.

This parameter includes:

- <server/>
- <SDP/>
- <SIP/>

**<server/>**

The configuration parameters listed in the following table are defined as follows.

**VoIP Server Parameters**

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voIpProt.server.dhcp.available<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If 0, do not check with the DHCP server for the SIP server IP address. If 1, check with the server for the IP address.		
<b>voIpProt.server.dhcp.option<sup>1</sup></b>	<b>128 to 254</b>	<b>128</b>
The option to request from the DHCP server if <code>voIpProt.server.dhcp.available=1</code> . Note: If <code>reg.x.server.y.address</code> is non-Null, it takes precedence even if the DHCP server is available.		
<b>voIpProt.server.dhcp.type<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
Type to request from the DHCP server if <code>voIpProt.server.dhcp.available</code> is set to 1. If this parameter is set to 0, IP request address. If set to 1, request string		
<b>voIpProt.server.x.address</b>	<b>dotted- decimal IP address or hostname</b>	<b>Null</b>
The IP address or hostname and port of a SIP server that accepts registrations. Multiple servers can be listed starting with x=1 to 4 for fault tolerance.		
<b>voIpProt.server.x.port</b>	<b>0, 1 to 65535</b>	<b>0</b>
The port of the server that specifies registrations. If 0, the port used depends on <code>voIpProt.server.x.transport</code> .		
<b>voIpProt.server.x.registerRetry.baseTimeOut</b>	<b>10 - 120</b>	<b>60</b>
The base time period to wait before a registration retry. Used in conjunction with <code>voIpProt.server.x.registerRetry.maxTimeOut</code> to determine how long to wait. The algorithm is defined in RFC 5626. If both parameters <code>voIpProt.server.x.registerRetry.baseTimeOut</code> and <code>reg.x.server.y.registerRetry.baseTimeOut</code> are set, the value of <code>reg.x.server.y.registerRetry.baseTimeOut</code> takes precedence.		
<b>voIpProt.server.x.registerRetry.maxTimeOut</b>	<b>60 - 1800</b>	<b>60</b>
The maximum time period to wait before a registration retry. Used in conjunction with <code>voIpProt.server.x.registerRetry.maxTimeOut</code> to determine how long to wait. The algorithm is defined in RFC 5626. If both parameters <code>voIpProt.server.x.registerRetry.maxTimeOut</code> and <code>reg.x.server.y.registerRetry.maxTimeOut</code> are set, the value of <code>reg.x.server.y.registerRetry.maxTimeOut</code> takes precedence.		



<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>voIpProt.server.x.transport</b>	<b>DNSNaptr, TCPpreferred, UDPOnly, TLS, TCPOnly</b>	<b>DNSNaptr</b>
<p>The transport method the system uses to communicate with the SIP server.</p> <p>Null or DNSNaptr – if voIpProt.server.x.address is a hostname and voIpProt.server.x.port is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If voIpProt.server.x.address is an IP address, or a port is given, then UDP is used.</p> <p>TCPpreferred – TCP is the preferred transport; UDP is used if TCP fails.</p> <p>UDPOnly: only UDP will be used.</p> <p>TLS – if TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061.</p> <p>TCPOnly – only TCP will be used.</p>		
<b>voIpProt.server.x.protocol.SIP</b>	<b>0 or 1</b>	<b>1</b>
<p>If 1, server is a SIP proxy/registrar. Note: if set to 0, and the server is confirmed to be a SIP server, then the value is assumed to be 1.</p>		
<b>voIpProt.server.x.expires</b>	<b>positive integer, minimum 10</b>	<b>3600</b>
<p>The system's requested registration period in seconds. Note: The period negotiated with the server may be different. The system will attempt to re-register at the beginning of the overlap period. For example, if expires="300" and overlap="5", the system will re-register after 295 seconds (300-5).</p>		
<b>voIpProt.server.x.expires.overlap</b>	<b>5 to 65535</b>	<b>60</b>
<p>The number of seconds before the expiration time returned by server x at which the system should try to re-register. The system will try to re-register at half the expiration time returned by the server if the server value is less than the configured overlap value.</p>		
<b>voIpProt.server.x.expires.lineSeize</b>	<b>positive integer, minimum 0 was 10</b>	<b>30</b>
<p>Requested line-seize subscription period.</p>		
<b>voIpProt.server.x.failOver.failBack.mode</b>	<b>newRequests, DNSTTL, registration, duration</b>	<b>newRequest s</b>
<p>The mode for failover failback:</p> <p>newRequests – all new requests are forwarded first to the primary server regardless of the last used server.</p> <p>DNSTTL – the system tries the primary server again after a timeout equal to the DNS TTL configured for the server that the system is registered to.</p> <p>registration – the system tries the primary server again when the registration renewal signaling begins.</p> <p>duration – the system tries the primary server again after the time specified by voIpProt.server.x.failOver.failBack.timeout.</p>		
<b>voIpProt.server.x.failOver.failBack.timeout</b>	<b>0, 60 to 65535</b>	<b>3600</b>
<p>If voIpProt.server.x.failOver.failBack.mode is set to duration, this is the time in seconds after failing over to the current working server before the primary server is again selected as the first server to forward new requests to. Values between 1 and 59 will result in a timeout of 60 and 0 means do not fail-back until a fail-over event occurs with the current server.</p>		

Parameter	Permitted Values	Default
<b>volpProt.server.x.failOver.failRegistrationOn</b>	<b>0 or 1</b>	<b>0</b>
<p>When set to 1, and the reRegisterOn parameter is enabled, the system will silently invalidate an existing registration (if it exists), at the point of failing over. When set to 0, and the reRegisterOn parameter is enabled, existing registrations will remain active. This means that the system will attempt failback without first attempting to register with the primary server to determine if it has recovered.</p>		
<b>volpProt.server.x.failOver.onlySignalWithRegistered</b>	<b>0 or 1</b>	<b>1</b>
<p>When set to 1, and the reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the system attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call will end. No SIP messages will be sent to the unregistered server. When set to 0, and the reRegisterOn and failRegistrationOn parameters are enabled, signaling will be accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).</p>		
<b>volpProt.server.x.failOver.reRegisterOn</b>	<b>0 or 1</b>	<b>0</b>
<p>When set to 1, the system will attempt to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling will proceed with the secondary server. When set to 0, the system won't attempt to register with the second.</p>		
<b>volpProt.server.x.lcs</b>	<b>0 or 1</b>	<b>0</b>
<p>If 0, the Microsoft Live Communications Server (LSC) is not supported. If 1, LCS is supported for registration x. This parameter overrides <code>voIpProt.SIP.lcs</code>.</p>		
<b>volpProt.server.x.register</b>	<b>0 or 1</b>	<b>1</b>
<p>If 0, calls can be routed to an outbound proxy without registration. See <code>reg.x.server.y.register</code>. For more information, see <a href="#">Technical Bulletin 5844: SIP Server Fallback Enhancements on Polycom Systems</a>.</p>		
<b>volpProt.server.x.retryTimeOut</b>	<b>0 to 65535</b>	<b>0</b>
<p>The amount of time (in milliseconds) to wait between retries. If 0, use standard RFC 3261 signaling retry behavior.</p>		
<b>volpProt.server.x.retryMaxCount</b>	<b>0 to 20</b>	<b>3</b>
<p>If set to 0, 3 is used. The number of retries that will be attempted before moving to the next available server.</p>		
<b>volpProt.server.x.specialInterop</b>	<b>standard, ocs2007r2, lcs2005, lync2010</b>	<b>standard</b>
<p>Specify if this registration should support Microsoft Office Communications Server 2007 R2 (ocs2007r2), Microsoft Live Communications Server 2005 (lcs2005), or Microsoft Lync 2010 (lync2010).</p>		
<b>volpProt.server.x.useOutboundProxy</b>	<b>0 or 1</b>	<b>1</b>
<p>Specify whether or not to use the outbound proxy specified in <code>voIpProt.SIP.outboundProxy.address</code> for server x.</p>		

<sup>1</sup> Change causes system to restart or reboot.

## <SDP/>

The configuration parameters in the following table is defined as follows:

### Session Description Protocol (SDP) Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SDP.answer.useLocalPreferences</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the systems uses its own preference list when deciding which codec to use rather than the preference list in the offer. If set to 0, it is disabled.		
<b>volpProt.SDP.early.answerOrOffer</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, an SDP offer or answer is generated in a provisional reliable response and PRACK request and response. If set to 0, an SDP offer or answer is not generated. Note: An SDP offer or answer is not generated if <code>reg.x.musicOnHold.uri</code> is set.		
<b>volpProt.SDP.iLBC.13_33kpbs.includeMode</b>	<b>0 or 1</b>	<b>1</b>
If set to 1, the system should include the <code>mode=30</code> FMTP parameter in SDP offers: If <code>voice.codecPref.iLBC.13_33kpbs</code> is set and <code>voice.codecPref.iLBC.15_2kpbs</code> is Null. If <code>voice.codecPref.iLBC.13_33kpbs</code> and <code>voice.codecPref.iLBC.15_2kpbs</code> are both set, the iLBC 13.33 kbps codec is set to a higher preference. If set to 0, the system should not include the <code>mode=30</code> FTMP parameter in SDP offers even if iLBC 13.33 kbps codec is being advertised. See <codecPref/>.		
<b>volpProt.SDP.useLegacyPayloadTypeNegotiation</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the system transmits and receives RTP using the payload type identified by the first codec listed in the SDP of the codec negotiation answer. If set to 0, RFC 3264 is followed for transmit and receive RTP payload type values.		

## <SIP/>

The configuration parameters in the following table is defined as follows.

### Session Initiation Protocol (SIP) Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SIP.acd.signalingMethod<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 0, the 'SIP-B' signaling is supported. (This is the older ACD functionality.) If set to 1, the feature synchronization signaling is supported. (This is the new ACD functionality.)		
<b>volpProt.SIP.alertInfo.x.class</b>	<b>see the list of ring classes in &lt;rt/&gt;</b>	<b>default</b>
Alert-Info fields from INVITE requests will be compared against as many of these parameters as are specified (x=1, 2, ..., N) and if a match is found, the behavior described in the corresponding ring class is applied.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SIP.alertInfo.x.value</b>	<b>string</b>	<b>Null</b>
A string to match the alertinfo header in the incoming INVITE.		
<b>volpProt.SIP.allowTransferOnProceeding</b>	<b>0, 1, 2</b>	<b>1</b>
If set to 0, a transfer is not allowed during the proceeding state of a consultation call. If set to 1, a transfer can be completed during the proceeding state of a consultation call. If set to 2, systems will accept an INVITE with replaces for a dialog in early state. This is needed when using transfer on proceeding with a proxying call server such as openSIPS, reSIProcate or SipXecs.		
<b>volpProt.SIP.authOptimizedInFailover</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, when failover occurs, the first new SIP request is sent to the server that sent the proxy authentication request. If set to 0, when failover occurs, the first new SIP request is sent to the server with the highest priority in the server list. If <code>reg.x.auth.optimizedInFailover</code> set to 0, this parameter is checked. If <code>voIpProt.SIP.authOptimizedInFailover</code> is 0, then this feature is disabled. If both parameters are set, the value of <code>reg.x.auth.optimizedInFailover</code> takes precedence.		
<b>volpProt.SIP.CID.sourcePreference</b>	<b>ASCII string up to 120 characters long</b>	<b>Null</b>
Specify the priority order for the sources of caller ID information. The headers can be in any order. If Null, caller ID information comes from P-Asserted-Identity, Remote-Party-ID, and From in that order. The values <code>From,P-Asserted-Identity, Remote-Party-ID</code> and <code>P-Asserted-Identity,From, Remote-Party-ID</code> are also valid.		
<b>volpProt.SIP.compliance.RFC3261.validate.contentLanguage</b>	<b>0 or 1</b>	<b>1</b>
If set to 1, validation of the SIP header content language is enabled. If set to 0, validation is disabled.		
<b>volpProt.SIP.compliance.RFC3261.validate.contentLength</b>	<b>0 or 1</b>	<b>1</b>
If set to 1, validation of the SIP header content length is enabled.		
<b>volpProt.SIP.compliance.RFC3261.validate.uriScheme</b>	<b>0 or 1</b>	<b>1</b>
If set to 1, validation of the SIP header URI scheme is enabled. If set to 0, validation is disabled.		
<b>volpProt.SIP.conference.address</b>	<b>ASCII string up to 128 characters long</b>	<b>Null</b>
If Null, conferences are set up on the system locally. If set to some value, conferences are set up by the server using the conferencing agent specified by this address. Acceptable values depend on the conferencing server implementation policy.		
<b>volpProt.SIP.conference.parallelRefer</b>	<b>0 or 1</b>	<b>0</b>
If 1, a parallel REFER is sent to the call server. <b>Note:</b> This parameter must be set for Siemens OpenScope Centralized Conferencing.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SIP.connectionReuse.useAlias</b>	<b>0 or 1</b>	<b>0</b>
If set to 0, the alias parameter is not added to the via header If set to 1, the system uses the connection reuse draft which introduces "alias".		
<b>volpProt.SIP.csta</b>	<b>0 or 1</b>	<b>0</b>
If 0, the uaCSTA (User Agent Computer Supported Telecommunications Applications) feature is disabled. If 1, uaCSTA is enabled (If <code>reg.x.csta</code> is set, it will override this parameter).		
<b>volpProt.SIP.dialog.strictXLineID</b>	<b>0 or 1</b>	<b>0</b>
If 0, the system will not look for x-line-id (call appearance indec) in a SIP INVITE message, if one is not present. Instead, when it receives INVITE, the system will generate the call appearance locally and pass that information to other parties involved in the call.		
<b>volpProt.SIP.dialog.usePvalue</b>	<b>0 or 1</b>	<b>0</b>
If set to 0, system uses a <code>pval</code> field name in Dialog. This obeys the draft-ietf-sipping-dialog-package-06.txt draft. If set to 1, the system uses a field name of <code>pvalue</code> .		
<b>volpProt.SIP.dialog.useSDP</b>	<b>0 or 1</b>	<b>0</b>
If set to 0, a new dialog event package draft is used (no SDP in dialog body). If set to 1, for backwards compatibility, use this setting to send SDP in the dialog body.		
<b>volpProt.SIP.dtmfViaSignaling.rfc2976<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, DTMF digit information is sent in RFC2976 SIP INFO packets during a call. If set to 0, no DTMF digit information is sent.		
<b>volpProt.SIP.enable<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
A flag to determine if the SIP protocol is used for call routing, dial plan, DTMF, and URL dialing. If set to 1, the SIP protocol is used.		
<b>volpProt.SIP.failoverOn503Response</b>	<b>0 or 1</b>	<b>1</b>
A flag to determine whether or not to trigger a failover if the system receives a 503 response.		
<b>volpProt.SIP.header.diversion.enable<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the diversion header is displayed if received. If set to 0, the diversion header is not displayed.		
<b>volpProt.SIP.header.diversion.list.useFirst<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, the first diversion header is displayed. If set to 0, the last diversion header is displayed.		
<b>volpProt.SIP.header.warning.codes.accept</b>	<b>comma separated list</b>	<b>Null</b>
Specify a list of accepted warning codes. If set to Null, all codes are accepted. Only codes between 300 and 399 are supported. For example, if you want to accept only codes 325 to 330: <code>voIpProt.SIP.header.warning.codes.accept=325,326,327,328,329,330</code> Text will be shown in the appropriate language. For more information, see <a href="#">lcl_ml_lang_menu_x</a> .		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SIP.header.warning.enable</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the warning header is displayed if received. If set to 0, the warning header is not displayed.		
<b>volpProt.SIP.IM.autoAnswerDelay</b>	<b>0 to 40, seconds</b>	<b>10</b>
The time interval from receipt of the instant message invitation to automatically accepting the invitation.		
<b>volpProt.SIP.keepalive.sessionTimers</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, the session timer will be enabled. If set to 0, the session timer will be disabled, and the system will not declare "timer" in "Support" header in an INVITE. The system will still respond to a re-INVITE or UPDATE. The system will not try to re-INVITE or UPDATE even if the remote endpoint asks for it.		
<b>volpProt.SIP.lcs</b>	<b>0 or 1</b>	<b>0</b>
If 0, the Microsoft Live Communications Server (LCS) is not supported. If 1, LCS is supported. This parameter can set for a specific registration using <code>reg.x.lcs</code> .		
<b>volpProt.SIP.lineSeize.retries</b>	<b>3 to 10</b>	<b>10</b>
Controls the number of times the system will retry a notify when attempting to seize a line (BLA).		
<b>volpProt.SIP.local.port<sup>1</sup></b>	<b>0 to 65535</b>	<b>5060</b>
The local port for sending and receiving SIP signaling packets. If set to 0, 5060 is used for the local port but is not advertised in the SIP signaling. If set to some other value, that value is used for the local port and it is advertised in the SIP signaling.		
<b>volpProt.SIP.ms-forking</b>	<b>0 or 1</b>	<b>0</b>
If set to 0, support for MS-forking is disabled. If set to 1, support for MS-forking is enabled and the system will reject all Instant Message INVITEs. This parameter is applies when installing Microsoft Live Communications Server. Note that if any endpoint registered to the same account has MS-forking disabled, all other endpoints default back to non-forking mode. Windows Messenger does not use MS-forking so be aware of this behavior if one of the endpoints is using Windows Messenger.		
<b>volpProt.SIP.mtls.enable</b>	<b>0 or 1</b>	<b>1</b>
If 0, Mutual TLS is disabled. If 1, Mutual TLS is enabled. Used in conjunction with Microsoft Lync 2010.		
<b>volpProt.SIP.musicOnHold.uri</b>	<b>a SIP URI</b>	<b>Null</b>
A URI that provides the media stream to play for the remote party on hold. This parameter is used if <code>reg.x.musicOnHold.uri</code> is Null. Note: The SIP URI parameter transport is supported when configured with the values of UDP, TCP, or TLS.		
<b>volpProt.SIP.outboundProxy.address</b>	<b>dotted-decimal IP address or hostname</b>	<b>Null</b>
The IP address or hostname of the SIP server to which the system sends all requests.		
<b>volpProt.SIP.outboundProxy.port</b>	<b>0 to 65535</b>	<b>0</b>
The port of the SIP server to which the system sends all requests.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SIP.outboundProxy.failOver.failBack.mode</b>	<b>newRequests, DNSTTL, registration, duration,</b>	<b>newRequests</b>
<p>The mode for failover failback (overrides <code>voIpProt.server.x.failOver.failBack.mode</code>).</p> <p><code>newRequests</code> – all new requests are forwarded first to the primary server regardless of the last used server.</p> <p><code>DNSTTL</code> – the system tries the primary server again after a timeout equal to the DNS TTL configured for the server that the system is registered to.</p> <p><code>registration</code> – the system tries the primary server again when the registration renewal signaling begins.</p> <p><code>duration</code> – the system tries the primary server again after the time specified by <code>reg.x.outboundProxy.failOver.failBack.timeout</code> expires.</p>		
<b>volpProt.SIP.outboundProxy.failOver.failBack.timeout</b>	<b>0, 60 to 65535</b>	<b>3600</b>
<p>The time to wait (in seconds) before failback occurs (overrides <code>voIpProt.server.x.failOver.failBack.timeout</code>). If the fail back mode is set to Duration, the system waits this long after connecting to the current working server before selecting the primary server again. If 0, the system will not fail-back until a fail-over event occurs with the current server.</p>		
<b>volpProt.SIP.outboundProxy.failOver.failRegistrationOn</b>	<b>0 or 1</b>	<b>0</b>
<p>When set to 1, and the <code>reRegisterOn</code> parameter is enabled, the system will silently invalidate an existing registration (if it exists), at the point of failing over. When set to 0, and the <code>reRegisterOn</code> parameter is enabled, existing registrations will remain active. This means that the system will attempt failback without first attempting to register with the primary server to determine if it has recovered.</p> <p>Note that <code>voIpProt.SIP.outboundProxy.failOver.RegisterOn</code> must be enabled.</p>		
<b>volpProt.SIP.outboundProxy.failOver.onlySignalWithRegistered</b>	<b>0 or 1</b>	<b>1</b>
<p>When set to 1, and the <code>reRegisterOn</code> and <code>failRegistrationOn</code> parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the system attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call will end. No SIP messages will be sent to the unregistered server. When set to 0, and the <code>reRegisterOn</code> and <code>failRegistrationOn</code> parameters are enabled, signaling will be accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred). This parameter overrides <code>volpProt.server.x.failOver.onlySignalWithRegistered</code>.</p>		
<b>volpProt.SIP.outboundProxy.failOver.reRegisterOn</b>	<b>0 or 1</b>	<b>0</b>
<p>This parameter overrides the <code>voIpProt.server.x.failOver.reRegisterOn</code>. When set to 1, the system will attempt to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling will proceed with the secondary server. When set to 0, the system won't attempt to register with the secondary server, since the system will assume that the primary and secondary servers share registration information.</p>		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SIP.outboundProxy.transport</b>	<b>DNSNaptr, TCPpreferred, UDPOnly, TLS, TCPOnly</b>	<b>DNSNaptr</b>
<p>The transport method the system uses to communicate with the SIP server.</p> <p>Null or DNSNaptr – if <code>reg.x.outboundProxy.address</code> is a hostname and <code>reg.x.outboundProxy.port</code> is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If <code>reg.x.outboundProxy.address</code> is an IP address, or a port is given, then UDP is used.</p> <p>TCPpreferred – TCP is the preferred transport, UDP is used if TCP fails.</p> <p>UDPOnly – only UDP will be used.</p> <p>TLS – if TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061.</p> <p>TCPOnly – only TCP will be used.</p>		
<b>volpProt.SIP.pingInterval</b>	<b>0 to 3600</b>	<b>0</b>
<p>The number in seconds to send "PING" message. This feature is disabled by default.</p>		
<b>volpProt.SIP.pingMethod</b>	<b>PING, OPTIONS</b>	<b>PING</b>
<p>The ping method to be used.</p>		
<b>volpProt.SIP.presence.nortelShortMode<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<p>Different headers sent in SUBSCRIBE when used for presence on an Avaya (Nortel) server. Support is indicated by adding a header <code>Accept-Encoding: x-nortel-short</code>. A PUBLISH is sent to indicate the status of the system.</p>		
<b>volpProt.SIP.requestValidation.digest.realm<sup>1</sup></b>	<b>A valid string</b>	<b>PolycomSPIP</b>
<p>Determines the string used for Realm.</p>		
<b>volpProt.SIP.requestValidation.x.method<sup>1</sup></b>	<b>Null, source, digest, both, all</b>	<b>Null</b>
<p>If Null, no validation is made. Otherwise this sets the type of validation performed for the request:</p> <p>source: ensure request is received from an IP address of a server belonging to the set of target registration servers;</p> <p>digest: challenge requests with digest authentication using the local credentials for the associated registration (line);</p> <p>both or all: apply both of the above methods</p>		
<b>volpProt.SIP.requestValidation.x.request<sup>1</sup></b>	<b>INVITE, ACK , BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE</b>	<b>Null</b>
<p>Sets the name of the method for which validation will be applied.</p> <p>Note: Intensive request validation may have a negative performance impact due to the additional signaling required in some cases.</p>		



<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SIP.requestValidation.x.request.y.event<sup>1</sup></b>	<b>A valid string</b>	<b>Null</b>
Determines which events specified with the Event header should be validated; only applicable when <code>voIpProt.SIP.requestValidation.x.request</code> is set to SUBSCRIBE or NOTIFY. If set to Null, all events will be validated.		
<b>volpProt.SIP.requestURI.E164.addGlobalPrefix</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, '+' global prefix is added to the E.164 user parts in sip: URIs.		
<b>volpProt.SIP.sendCompactHdrs</b>	<b>0 or 1</b>	<b>0</b>
If set to 0, SIP header names generated by the system use the long form, for example <code>From</code> . If set to 1, SIP header names generated by the system use the short form, for example <code>f</code> .		
<b>volpProt.SIP.serverFeatureControl.cf<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, server-based call forwarding is enabled. The call server has control of call forwarding. If set to 0, server-based call forwarding is not enabled.		
<b>volpProt.SIP.serverFeatureControl.dnd<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, server-based DND is enabled. The call server has control of DND. If set to 0, server-based DND is not enabled.		
<b>volpProt.SIP.serverFeatureControl.missedCalls<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, server-based missed calls is enabled. The call server has control of missed calls. If set to 0, server-based missed calls is not enabled.		
<b>volpProt.SIP.serverFeatureControl.localProcessing.cf</b>	<b>0 or 1</b>	<b>1</b>
If set to 0 and <code>voIpProt.SIP.serverFeatureControl.cf</code> is set to 1, the system will not perform local Call Forward behavior. If set to 1, the system will perform local Call Forward behavior on all calls received.		
<b>volpProt.SIP.serverFeatureControl.localProcessing.dnd</b>	<b>0 or 1</b>	<b>1</b>
If set to 0 and <code>voIpProt.SIP.serverFeatureControl.dnd</code> is set to 1, the system will not perform local DND call behavior. If set to 1, the system will perform local DND call behavior on all calls received.		
<b>volpProt.SIP.specialEvent.checkSync.alwaysReboot<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
If set to 1, always reboot when a NOTIFY message is received from the server with event equal to check-sync. If set to 0, only reboot if any of the files listed in <code>&lt;MAC-address&gt;.cfg</code> have changed on the FTP server when a NOTIFY message is received from the server with event equal to check-sync.		
<b>volpProt.SIP.specialEvent.lineSeize.nonStandard<sup>1</sup></b>	<b>0 or 1</b>	<b>1</b>
If set to 1, process a 200 OK response for a line-seize event SUBSCRIBE as though a line-seize NOTIFY with Subscription State: active header had been received. This speeds up processing.		
<b>volpProt.SIP.strictLineSeize</b>	<b>0 or 1</b>	<b>0</b>
If set to 1, The system is forced to wait for a 200 OK response when receiving a TRYING notify. If set to 0, dial prompt is provided immediately when you attempt to seize a shared line without waiting for a successful OK from the call server.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>volpProt.SIP.strictUserValidation</b>	<b>0 or 1</b>	<b>0</b>
<p>If set to 1, the system is forced to match the user portion of signaling exactly.</p> <p>If set to 0, the system will use the first registration if the user part does not match any registration.</p>		
<b>volpProt.SIP.supportFor100rel</b>	<b>0 or 1</b>	<b>1</b>
<p>If set to 1, the system advertises support for reliable provisional responses in its offers and responses.</p> <p>If set to 0, the system will not offer 100rel and will reject offers requiring 100rel.</p>		
<b>volpProt.SIP.tcpFastFailover</b>	<b>0 or 1</b>	<b>0</b>
<p>If set to 1, failover occurs based on the values of <code>reg.x.server.y.retryMaxCount</code> and <code>voIpProt.server.x.retryTimeOut</code>.</p> <p>If 0, a full 32 second RFC compliant timeout is used. See <code>reg.x.tcpFastFailover</code>.</p>		
<b>volpProt.SIP.tlsDsk.enable</b>	<b>0 or 1</b>	<b>0</b>
<p>If 0, TLS DSK is disabled. If 1, TLS DSK is enabled. For more information, see <a href="#">Session Initiation Protocol (SIP) Authentication Extensions Protocol Overview</a>.</p>		
<b>volpProt.SIP.turnOffNonSecureTransport<sup>1</sup></b>	<b>0 or 1</b>	<b>0</b>
<p>If set to 1, stop listening to port 5060 when using AS-SIP enabled.</p>		
<b>volpProt.SIP.use486forReject</b>	<b>0 or 1</b>	<b>0</b>
<p>If set to 1 and the system is indicating a ringing inbound call appearance, the system will transmit a 486 response to the received INVITE when the Reject soft key is pressed.</p> <p>If set to 0, no 486 response is transmitted.</p>		
<b>volpProt.SIP.useContactInReferTo</b>	<b>0 or 1</b>	<b>0</b>
<p>If set to 0, the "To URI" is used in the REFER.</p> <p>If set to 1, the "Contact URI" is used in the REFER.</p>		
<b>volpProt.SIP.useRFC2543hold</b>	<b>0 or 1</b>	<b>0</b>
<p>If set to 0, use SDP media direction parameters (such as <code>a=sendonly</code>) per RFC 3264 when initiating a call. Otherwise use the obsolete <code>c=0.0.0.0</code> RFC2543 technique. In either case, the system processes incoming hold signaling in either format.</p> <p>Note: <code>volpProt.SIP.useRFC2543hold</code> is effective only when the call is initiated.</p>		
<b>volpProt.SIP.useSendonlyHold</b>	<b>0 or 1</b>	<b>1</b>
<p>If set to 1, the system will send a reinvite with a stream mode parameter of "sendonly" when a call is put on hold. This is the same as the previous behavior.</p> <p>If set to 0, the system will send a reinvite with a stream mode parameter of "inactive" when a call is put on hold.</p> <p>NOTE: The system will ignore the value of this parameter if set to 1 when the parameter <code>volpProt.SIP.useRFC2543hold</code> is also set to 1 (default is 0).</p>		

<sup>1</sup> Change causes system to restart or reboot.

## <webutility/>

The parameters listed in the table [Web Configuration Utility Parameters](#) specify the download location of the translated language files for the Web Configuration Utility.

### Web Configuration Utility Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>webutility.languauge.plcm.server.url</b>	<b>URL</b>	<b>http://downloads.polycom.com/voice/software/languages/</b>
The download location of the translated language files for the Web Configuration Utility.		

## <xmpp/>

The parameters in the following table set the XML streaming protocols for instant messaging, presence, and contact list maintenance for BroadSoft features

### XML Streaming Protocol Parameters

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>xmpp.1.auth.domain</b>	<b>UTF-8 encoded string</b>	<b>Null</b>
The domain used for XMPP registration.		
<b>xmpp.1.auth.password</b>	<b>UTF-8 encoded string</b>	<b>Null</b>
Password used for XMPP registration.		
<b>xmpp.1.dialMethod</b>	<b>String min 0, max 256</b>	<b>SIP</b>
For SIP dialing, the destination XMPP URI is converted to a SIP URI, and the first available SIP line is used to place the call.		
<b>xmpp.1.enable</b>	<b>0 or 1</b>	<b>0</b>
Flag to determine if XMPP presence is enabled. If 1 XMPP presence is enabled.		
<b>xmpp.1.jid</b>	<b>String min 0, max 256</b>	<b>Null</b>
Jabber identity used to register with presence server. For example: <code>presence.test2@polycom-alpha.eu.bc.im</code> .		
<b>xmpp.1.roster.invite.accept</b>	<b>Automatic or prompt</b>	<b>Prompt</b>
Turns the BroadSoft XMPP inviter's subscription for presence. If set to prompt, system receives pending invitation successfully and can accept or reject the invitation.		
<b>xmpp.1.server</b>	<b>dotted-decimal IP address, host name, or FQDN</b>	<b>Null</b>
Sets the BroadSoft XMPP presence server to IP or FQDN. For example: <code>polycom-alpha.eu.bc.im</code> .		

---

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
<b>xmpp.1.verifyCert</b>	<b>0 or 1</b>	<b>1</b>
<p>Enables and disables the Server Certificate verification from XMPP server. Accepted Values: 0 – Disables; 1 – Enables. If 0, verification of the TLS certificate provided by the BroadSoft XMPP presence server is turned off.</p>		

---

# Session Initiation Protocol (SIP)

---

This section describes the basic Session Initiation Protocol (SIP) and the protocol extensions that the current Polycom UC Software supports.

This section contains the following information:

- **Basic Protocols** All the basic calling functionality described in the SIP specification is supported. Transfer is included in the basic SIP support.
- **Protocol Extensions** Extensions add features to SIP that are applicable to a range of applications, including reliable 1xx responses and session timers.

For information on supported RFCs and Internet drafts, see the section [RFC and Internet Draft Support](#).

You can find information on the following topics:

- [Request Support](#)
- [Header Support](#)
- [Response Support](#)
- [Hold Implementation](#)
- [Reliability of Provisional Responses](#)
- [Transfer](#)
- [Third Party Call Control](#)
- [SIP for Instant Messaging and Presence Leveraging Extensions](#)
- [Shared Call Appearance Signaling](#)
- [Bridged Line Appearance Signaling](#)

## RFC and Internet Draft Support

The following RFC's and Internet drafts are supported. For more information on any of the documents, enter the RFC number at [Request for Comments \(RFC\)](#).

- RFC 1321—The MD5 Message-Digest Algorithm
- RFC 2327—SDP: Session Description Protocol
- RFC 2387—The MIME Multipart / Related Content-type
- RFC 2976—The SIP INFO Method
- RFC 3261—SIP: Session Initiation Protocol (replacement for RFC 2543)
- RFC 3262—Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263—Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264—An Offer / Answer Model with the Session Description Protocol (SDP)
- RFC 3265—Session Initiation Protocol (SIP) - Specific Event Notification
- RFC 3311—The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3325—SIP Asserted Identity
- RFC 3420—Internet Media Type message/sipfrag

- RFC 3515—The Session Initiation Protocol (SIP) Refer Method
- RFC 3555—MIME Type of RTP Payload Formats
- RFC 3611—RTP Control Protocol Extended reports (RTCP XR)
- RFC 3665—Session Initiation Protocol (SIP) Basic Call Flow Examples
- draft-ietf-sip-cc-transfer-05.txt—SIP Call Control - Transfer
- RFC 3725—Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3842—A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3856—A Presence Event Package for Session Initiation Protocol (SIP)
- RFC 3891—The Session Initiation Protocol (SIP) “Replaces” Header
- RFC 3892—The Session Initiation Protocol (SIP) Referred-By Mechanism
- RFC 3959—The Early Session Disposition Type for the Session Initiation Protocol (SIP)
- RFC 3960—Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
- RFC 3968—The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 3969—The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- draft-levy-sip-diversion-08.txt—Diversion Indication in SIP
- draft-anil-sipping-bla-02.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-04.txt—SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
- draft-ietf-sipping-cc-conferencing-03.txt—SIP Call Control - Conferencing for User Agents
- draft-ietf-sipping-rtcp-summary-02.txt —Session Initiation Protocol Package for Voice Quality Reporting Event
- draft-ietf-sip-connect-reuse-04.txt—Connection Reuse in the Session Initiation Protocol (SIP)

## Request Support

The SIP request messages in the following table are supported:

### Supported SIP Request Messages

<i>Method</i>	<i>Supported</i>	<i>Notes</i>
REGISTER	Yes	
INVITE	Yes	
ACK	Yes	

<i>Method</i>	<i>Supported</i>	<i>Notes</i>
CANCEL	Yes	
BYE	Yes	
OPTIONS	Yes	
SUBSCRIBE	Yes	
NOTIFY	Yes	
REFER	Yes	
PRACK	Yes	
INFO	Yes	RFC 2976, the system does not generate INFO requests, but will issue a final response upon receipt. No INFO message bodies are parsed.
MESSAGE	Yes	Final response is sent upon receipt. Message bodies of type text/plain are sent and received.
UPDATE	Yes	

## Header Support

The following table lists the SIP request headers supported.



### Note: Reading the Following Table

In the following table, a Yes in the Supported column means the header is sent and properly parsed.

### Supported SIP Request Headers

<i>Header</i>	<i>Supported</i>
Accept	Yes
Accept-Encoding	Yes
Accept-Language	Yes
Accept-Resource-Priority	Yes
Access-Network-Info	No
Access-URL	Yes

<i>Header</i>	<i>Supported</i>
Alert-Info	Yes
Allow	Yes
Allow-Events	Yes
Authentication-Info	Yes
Authorization	Yes
Call-ID	Yes
Call-Info	Yes
Contact	Yes
Content-Disposition	Yes
Content-Encoding	Yes
Content-Language	Yes
Content-Length	Yes
Content-Type	Yes
CSeq	Yes
Date	Yes (for missed call, not used to adjust the time of the system)
Diversion	Yes
Error-Info	No
Event	Yes
Expires	Yes
Flow-Timer	Yes
From	Yes
In-Reply-To	No
Join	Yes
Max-Forwards	Yes
Min-Expires	Yes
Min-SE	Yes
MIME-Version	No
Missed-Calls	Yes



<i>Header</i>	<i>Supported</i>
ms-client-diagnostics	Yes
ms-keep-alive	Yes
ms-text-format	Yes
Organization	No
P-Asserted-Identity	Yes
P-Preferred-Identity	Yes
Priority	No
Privacy	No
Proxy-Authenticate	Yes
Proxy-Authorization	Yes
Proxy-Require	Yes
RAck	Yes
Reason	Yes
Record-Route	Yes
Refer-Sub	Yes
Refer-To	Yes
Referred-By	Yes
Referred-To	Yes
Remote-Party-ID	Yes
Replaces	Yes
Reply-To	No
Requested-By	No
Require	Yes
Resource-Priority	Yes
Response-Key	No
Retry-After	Yes
Route	Yes
RSeq	Yes

<i>Header</i>	<i>Supported</i>
Server	Yes
Session-Expires	Yes
SIP-Etag	Yes
SIP-If-Match	Yes
Subject	Yes
Subscription-State	Yes
Supported	Yes
Timestamp	Yes
To	Yes
Unsupported	Yes
User-Agent	Yes
Via	Yes
voice-missed-call	Yes
Warning	Yes (Only warning codes 300 to 399)
WWW-Authenticate	Yes
X-Sipx-Authidentity	Yes

## ***Response Support***

The SIP responses are listed in the following tables:

- [Supported 1xx SIP Responses](#)
- [Supported 2xx SIP Responses](#)
- [Supported 3xx SIP Responses](#)
- [Supported 4xx SIP Responses](#)
- [Supported 5xx SIP Responses](#)
- [Supported 6xx SIP Responses](#)



### **Note: Reading the Following Tables**

In the following table, a Yes in the Supported column means the header is sent and properly parsed. The system may not actually generate the response.

## 1xx Responses - Provisional

### Supported 1xx SIP Responses

<i>Response</i>	<i>Supported</i>
100 Trying	Yes
180 Ringing	Yes
181 Call Is Being Forwarded	No
182 Queued	No
183 Session Progress	Yes

## 2xx Responses - Success

### Supported 2xx SIP Responses

<i>Response</i>	<i>Supported</i>	<i>Notes</i>
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

## 3xx Responses - Redirection

### Supported 3xx SIP Responses

<i>Response</i>	<i>Supported</i>
300 Multiple Choices	Yes
301 Moved Permanently	Yes
302 Moved Temporarily	Yes
305 Use Proxy	No
380 Alternative Service	No

## 4xx Responses - Request Failure



### Note: Handling 4xx Responses

All 4xx responses for which the system does not provide specific support will be treated the same as 400 Bad Request.

### Supported 4xx SIP Responses

<i>Response</i>	<i>Supported</i>
400 Bad Request	Yes
401 Unauthorized	Yes
402 Payment Required	No
403 Forbidden	No
404 Not Found	Yes
405 Method Not Allowed	Yes
406 Not Acceptable	No
407 Proxy Authentication Required	Yes
408 Request Timeout	No
410 Gone	No
413 Request Entity Too Large	No
414 Request-URI Too Long	No
415 Unsupported Media Type	Yes
416 Unsupported URI Scheme	No
420 Bad Extension	No
421 Extension Required	No
423 Interval Too Brief	Yes
480 Temporarily Unavailable	Yes
481 Call/Transaction Does Not Exist	Yes
482 Loop Detected	Yes

<i>Response</i>	<i>Supported</i>
483 Too Many Hops	No
484 Address Incomplete	Yes
485 Ambiguous	No
486 Busy Here	Yes
487 Request Terminated	Yes
488 Not Acceptable Here	Yes
491 Request Pending	No
493 Undecipherable	No

## 5xx Responses - Server Failure

### Supported 5xx SIP Responses

<i>Response</i>	<i>Supported</i>
500 Server Internal Error	Yes
501 Not Implemented	Yes
502 Bad Gateway	No
503 Service Unavailable	No
504 Server Time-out	No
505 Version Not Supported	No
513 Message Too Large	No

## 6xx Responses - Global Failure

### Supported 6xx SIP Responses

<i>Response</i>	<i>Supported</i>
600 Busy Everywhere	No

<i>Response</i>	<i>Supported</i>
603 Decline	Yes
604 Does Not Exist Anywhere	No
606 Not Acceptable	No

## ***Hold Implementation***

The system supports two currently accepted means of signaling hold.

The first method, no longer recommended due in part to the RTCP problems associated with it, is to set the “c” destination addresses for the media streams in the SDP to zero, for example, c=0.0.0.0.

The second, and preferred, method is to signal the media directions with the “a” SDP media attributes sendonly, recvonly, inactive, or sendrecv. The hold signaling method used by the system is configurable (see [SIP](#)), but both methods are supported when signaled by the remote endpoint



### **Note: Hold Methods**

Even if the system is set to use c=0.0.0.0, it will not do so if it gets any sendrecv, sendonly, or inactive from the server. These flags will cause it to revert to the other hold method.

## ***Reliability of Provisional Responses***

The system fully supports RFC 3262 - Reliability of Provisional Responses.

## ***Transfer***

The system supports transfer using the REFER method specified in draft-ietf-sip-cc-transfer-05 and RFC 3515.

## ***Third Party Call Control***

The system supports the delayed media negotiations (INVITE without SDP) associated with third-party call-control applications.

When used with an appropriate server, the User Agent Computer Supported Telecommunications Applications (uaCSTA) feature on the system may be used for remote control of the system from computer applications such as Microsoft Office Communicator.

The system is compliant with “Using CSTA for SIP System User Agents (uaCSTA), ECMA TR/087” for the Answer Call, Hold Call, and Retrieve Call functions and “Services for Computer Supported Telecommunications Applications Phase III, ECMA – 269” for the Conference Call function.

This feature is enabled by configuration parameters described in <SIP/> and <reg/>, and needs to be activated by a feature application key.

## ***SIP for Instant Messaging and Presence Leveraging Extensions***

The system is compatible with the Presence and Instant Messaging features of Microsoft Windows Messenger 5.1. In a future release, support for the Presence and Instant Message recommendations in the SIP Instant Messaging and Presence Leveraging Extensions (SIMPLE) proposals will be provided by the following Internet drafts or their successors:

- draft-ietf-simple-cpim-mapping-01
- draft-ietf-simple-presence-07
- draft-ietf-simple-presencelist-package-00
- draft-ietf-simple-winfo-format-02
- draft-ietf-simple-winfo-package-02

## ***Shared Call Appearance Signaling***

A shared line is an address of record managed by a call server. The server allows multiple endpoints to register locations against the address of record.

The system supports shared call appearances (SCA) using the SUBSCRIBE-NOTIFY method in the “SIP Specific Event Notification” framework (RFC 3265). The events used are:

- *call-info* for call appearance state notification
- *line-seize* for the system to ask to seize the line

## ***Bridged Line Appearance Signaling***

A bridged line is an address of record managed by a server. The server allows multiple endpoints to register locations against the address of record.

The system supports bridged line appearances (BLA) using the SUBSCRIBE-NOTIFY method in the “SIP Specific Event Notification” framework (RFC 3265). The events used are:

- “dialog” for bridged line appearance subscribe and notify.